kaspersky

Kaspersky Endpoint Security 14.2 para Windows

© 2026 AO Kaspersky Lab

Contenido

Ayuda de Kaspersky Endpoint Security para Windows
- Novedades
- Problemas solucionados
- Preguntas frecuentes

Kaspersky Endpoint Security para Windows
- Modos de aplicación: Estándar, EDR Agent, Light Agent
- Kit de distribución
- Requisitos de hardware y software
- Comparación de funciones disponibles en la aplicación según el tipo de sistema operativo
- Comparación: disponibilidad de características por herramienta de administración
- Compatibilidad con otras aplicaciones

Instalación y eliminación de la aplicación
- Despliegue a través de Kaspersky Security Center
  - Instalación estándar de la aplicación
  - Creación de un paquete de instalación
  - Actualización de bases de datos en el paquete de instalación
  - Creación de una tarea de instalación remota
- Instalación de la aplicación de manera local mediante el Asistente de instalación
- Instalando remotamente la aplicación usando System Center Configuration Manager
- Descripción de la configuración de instalación del archivo setup.ini
- Procesos de Kaspersky Endpoint Security para Windows
- Cambiar componentes de la aplicación
- Actualización de una versión anterior de la aplicación
  - Actualizar la aplicación sin reiniciar
  - Actualización de SMU de la aplicación
- Eliminar la aplicación

Licencias de la aplicación
- Acerca del Contrato de licencia de usuario final
- Acerca de la licencia
- Acerca del certificado de licencia
- Acerca de la suscripción
- Sobre una clave de licencia
- Acerca del código de activación
- Acerca del archivo clave
- Comparación de la funcionalidad de la aplicación según el tipo de licencia para las estaciones de trabajo
- Comparación de la funcionalidad de la aplicación según el tipo de licencia para servidores
- Activación de la aplicación
- Eliminar una clave de licencia
- Visualización de información de la licencia
- Compra de una licencia
- Renovación de suscripciones

Primeros pasos
- Acerca del Complemento de administración de Kaspersky Endpoint Security para Windows
- Consideraciones especiales cuando se trabaja con distintas versiones de complementos de administración
- Consideraciones especiales al utilizar protocolos cifrados para interactuar con servicios externos
- Interfaz de la aplicación
  - Icono de la aplicación en el área de notificaciones de la barra de tareas
  - Interfaz simplificada de la aplicación
  - Configuración de la visualización de la interfaz de la aplicación
- Preparar la aplicación para su uso
- Gestión de directivas
  - Creación de una directiva
  - Exportar e importar una directiva
  - Indicador de nivel de seguridad
- Gestión de tareas
- Configuración de los ajustes locales de la aplicación
- Inicio y detención de Kaspersky Endpoint Security
- Suspensión y reanudación de Protección y control del equipo
- Crear y utilizar un archivo de configuración
- Restaurar las configuración predeterminada de la aplicación
- Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones
  - Activación o desactivación del modo de ahorro de energía
  - Activación o desactivación de la concesión de recursos a otras aplicaciones
  - Prácticas recomendadas para optimizar el rendimiento de Kaspersky Endpoint Security

Análisis antimalware
- Análisis del equipo
- Análisis de unidades extraíbles cuando se conectan al equipo
- Análisis en segundo plano
- Analizar desde el menú contextual
- Comprobación de integridad de la aplicación
- Edición de la cobertura del análisis
- Análisis programado en ejecución
- Ejecutar un análisis como un usuario diferente
- Optimización del análisis

Actualización de las bases de datos y módulos de la aplicación
- Escenarios de actualización de las bases de datos y los módulos de la aplicación
  - Actualización con un repositorio de servidor
  - Actualización con una carpeta compartida
  - Actualización con Kaspersky Update Utility
  - Actualización en modo móvil
- Inicio y parada de una tarea de actualización
- Inicio de una tarea de actualización con los permisos de una cuenta de usuario distinta
- Selección del modo de ejecución de la tarea de actualización
- Adición de un origen de actualizaciones
- Actualización de los módulos de la aplicación
- Actualización mediante un servidor proxy
- Reversión de la última actualización

Tecnología de desinfección avanzada
Desinfección de amenazas activas en estaciones de trabajo
Desinfección de amenazas activas en servidores
Eliminar amenazas no procesadas
Protección del equipo
Estado de la protección en tiempo real
Protección frente a amenazas en archivos
Activación y desactivación de Protección frente a amenazas en archivos
Suspensión automática de Protección frente a amenazas en archivos
Modificación de las acciones tomadas en archivos infectados por parte del componente Protección frente a amenazas en archivos
Formación la cobertura de protección del componente Protección frente a amenazas en archivos
Uso de métodos de análisis
Utilización de las tecnologías de análisis en el funcionamiento del componente Protección frente a amenazas en archivos
Optimización del análisis de archivos
Análisis de archivos compuestos
Modificación del modo de análisis
Análisis de contenedores
Prevención de intrusiones en el host
Activación y desactivación de Prevención de intrusiones en el host
Gestionar grupos de confianza de aplicaciones
Cambiar el grupo de confianza de una aplicación
Configuración de derechos del grupo de confianza
Seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security
Selección de un grupo de confianza para aplicaciones desconocidas
Seleccionar un grupo de confianza para aplicaciones firmadas digitalmente
Administración de los derechos de las aplicaciones
Protección de recursos del sistema operativo y de datos personales
Eliminación de información sobre aplicaciones sin uso
Control de prevención de intrusiones en el host
Protección del acceso a audio y vídeo
Prevención de ataques de BadUSB
Activación y desactivación de Prevención de ataques de BadUSB
Usar el teclado en pantalla para la autorización de dispositivos USB
Autorización de escáneres de códigos de barras
Protección AMSI
Activación y desactivación de la protección AMSI
Optimización del análisis de archivos mediante la protección AMSI
Protección frente a amenazas web
Activación y desactivación de Protección frente a amenazas web
Configuración de métodos de detección de direcciones web maliciosas
Anti-Phishing
Creación de la lista de direcciones web de confianza
Exportación e importación de la lista de direcciones web de confianza
Protección frente a amenazas en el correo
Activación y desactivación de Protección frente a amenazas en el correo
Modificación de las acciones que se van a realizar en mensajes de correo electrónico infectados

- Formación la cobertura de protección del componente de Protección frente a amenazas en el correo
- Analizar archivos compuestos adjuntos a mensajes de correo electrónico
- Filtro de archivos adjuntos de mensajes de correo electrónico
- Exportación e importación de extensiones para filtrado de adjuntos
- Análisis de correos electrónicos en Microsoft Office Outlook
- Análisis de correos electrónicos en Thunderbird, MyOffice, R7-Office

Protección frente a amenazas en la red

- Activación y desactivación de Protección frente a amenazas en la red
- Bloquear un equipo atacante
- Configurar direcciones de exclusiones de bloqueo
- Exportación e importación de la lista de exclusiones de bloqueo
- Configuración de Protección frente a amenazas en la red por tipo

Firewall

- Activación y desactivación de Firewall
- Modificación del tipo de conexión de red
- Gestión de las reglas de paquetes de red
  - Crear una regla de paquetes de red
  - Activación o desactivación de una regla de paquetes de red
  - Modificación de la acción de Firewall para una regla de paquetes de red
  - Modificación de la prioridad de una regla de paquetes de red
  - Exportación e importación de reglas de paquetes de red
  - Definir reglas de paquetes de red en XML
- Gestionar reglas de red de la aplicación
  - Crear una regla de red de aplicaciones
  - Activar y desactivar una regla de red de la aplicación
  - Modificación de la acción de Firewall para una regla de red de la aplicación
  - Modificación de la prioridad de una regla de red de la aplicación
- Monitor de red

Prevención de exploits

- Activación y desactivación de Prevención de vulnerabilidades
- Protección de la memoria de los procesos del sistema

Detección de comportamiento

Anti-Cryptor

- Activación y desactivación de la protección de carpetas compartidas frente al cifrado externo
- Configuración del período de bloqueo de un equipo que no es de confianza
- Edición de la cobertura de protección
- Adición de equipos de confianza para el cifrado de datos externos
- Exportar e importar una lista de exclusiones a la protección de carpetas compartidas frente a cifrado externo

Motor de reparación

Kaspersky Security Network

- Activación y desactivación del uso de Kaspersky Security Network
- Limitaciones de Kaspersky Private Security Network
- Activar y desactivar el modo Cloud para los componentes de protección
- Configuración del proxy de KSN
- Comprobar la reputación de un archivo en Kaspersky Security Network

Análisis de conexiones cifradas
Habilitar el análisis de conexiones cifradas
Instalación de certificados raíz de confianza
Análisis de conexiones cifradas con un certificado que no es de confianza
Añadir el certificado de Kaspersky a la propia tienda de certificados
Exclusión de conexiones cifradas del análisis
Bloqueo del acceso a dominios con certificados que no son de confianza
Eliminación de datos
Control del equipo
Control Web
Adición de una regla de acceso a recursos web
Filtrar por direcciones de recursos web
Filtrar por contenido de recursos web.
Comprobación de las reglas de acceso a recursos web
Exportación e importación de reglas de Control Web
Exportar e importar direcciones de recursos web de la regla de Control Web
Supervisión de las actividades de los usuarios en Internet
Edición de plantillas de mensajes de Control Web
Edición de máscaras para direcciones de recursos web
Control web para máquinas virtuales
Variables en las plantillas de mensajes de Control web:
Control de dispositivos
Sobre las reglas de acceso
Obtención de información sobre los dispositivos instalados
Administrar el acceso a dispositivos por tipo
Gestionar el acceso a dispositivos por bus de conexión
Diferenciación de los derechos de acceso de los usuarios a los dispositivos
Administrar el acceso a dispositivos móviles
Administrar el acceso a dispositivos con Bluetooth
Control de impresión
Control de conexiones wifi
Seguimiento del uso de unidades extraíbles
Cambiar la duración del almacenamiento en caché
Acciones con dispositivos de confianza
Adición de un dispositivo a la lista de confianza
Exportación e importación de la lista de dispositivos de confianza
Obtención de acceso a un dispositivo bloqueado
Modo con conexión para otorgar acceso
Modo sin conexión para otorgar acceso
Edición de plantillas de mensajes de Control de dispositivos
Anti-Bridging
Activar el componente Anti-Bridging
Cambio del estado de una regla de conexión
Cambio de la prioridad de una regla de conexión
Control de anomalías adaptativo
Autoaprendizaje del Control de anomalías adaptativo
Activación y desactivación de una regla del Control de anomalías adaptativo

- Cambio de la acción que se realiza al activarse una regla del Control de anomalías adaptativo
- Crear una exclusión de una regla del Control de anomalías adaptativo
- Importar e importar exclusiones para las reglas del Control de anomalías adaptativo
- Actualización de las reglas del Control de anomalías adaptativo
- Modificación de las plantillas de mensajes del Control de anomalías adaptativo
- Supervisión de las operaciones de Control de anomalías adaptativo

Control de aplicaciones

- Limitaciones de funcionalidad de Control de aplicaciones
- Obtener información sobre las aplicaciones instaladas
- Cómo activar el modo de aplicaciones bloqueadas
- Control de aplicaciones basado en un equipo de línea de base
- Administrar reglas de Control de aplicaciones
  - Añadir una condición de activación para la regla de Control de aplicaciones
  - Añadir archivos ejecutables desde la carpeta Archivos ejecutables a la categoría de aplicación
  - Añadir archivos ejecutables relacionados con eventos a la categoría de aplicación
  - Adición de una regla de Control de aplicaciones
  - Cambiar el estado de una regla de Control de aplicaciones mediante Kaspersky Security Center
  - Exportación e importación de reglas de Control de aplicaciones
  - Ver eventos resultantes del funcionamiento del componente Control de aplicaciones
  - Ver un informe sobre aplicaciones bloqueadas
- Probar reglas de Control de aplicaciones
  - Activación y desactivación de la prueba de reglas de Control de aplicaciones
  - Ver un informe sobre las aplicaciones bloqueadas en el modo de prueba
  - Ver eventos resultantes de la comprobación del funcionamiento del componente Control de aplicaciones
- Supervisión de la actividad de aplicaciones
- Reglas para crear máscaras de nombre para archivos o carpetas
- Edición de plantillas de mensajes de Control de aplicaciones
- Variables en las plantillas de mensajes de Control de aplicaciones
- Prácticas recomendadas para realizar un inventario de archivos ejecutables
- Mejores prácticas para implementar una lista de aplicaciones permitidas
  - Configuración del modo de lista de admitidos para aplicaciones
  - Prueba del modo de lista de admitidos
  - Soporte para el modo de lista de admitidos

Supervisión de puertos de red

- Activación de la vigilancia de todos los puertos de red
- Creación de una lista de puertos de red supervisados
- Creación de una lista de aplicaciones para las que se supervisan todos los puertos de red
- Exportación e importación de listas de puertos vigilados

Inspección de registros

- Configuración de reglas predefinidas
- Adición de reglas personalizadas

Control de integridad del sistema

- Acerca de las reglas del Control de integridad del sistema
- Control de integridad del sistema en tiempo real
- Comprobación de integridad del sistema a demanda
- Exportación e importación de reglas de Control de integridad del sistema

- Visualización de informes de Control de integridad del sistema
- Restablecimiento del estado de integridad del sistema
- Cloud Discovery

Zona de confianza
- Creación de una exclusión del análisis
- Crear una exclusión por tipo de objetos detectados
- Edición de la lista de aplicaciones de confianza
- Creación de una zona de confianza local
- Exportación e importación de la zona de confianza
- Manejo de aplicaciones con una firma digital confiable
- Apéndice. Exclusiones de análisis predefinidas y aplicaciones de confianza.
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Microsoft System Center Configuration Manager
  - Citrix
  - VMware
  - Desduplicación de datos en Microsoft Windows Server

Gestión de Copia de seguridad
- Configuración del período de almacenamiento máximo de archivos en Copia de seguridad
- Configuración del tamaño máximo de Copia de seguridad
- Restauración de archivos de Copia de seguridad
- Eliminación de las copias de seguridad de los archivos de Copia de seguridad

Servicio de notificaciones
- Configuración de los parámetros de registro de eventos
- Configuración de la visualización y entrega de notificaciones
- Configuración de la visualización de advertencias sobre el estado de la aplicación en el área de notificaciones
- Mensajes entre los usuarios y el administrador

Gestión de informes
- Ver informes
- Configuración del período máximo de almacenamiento del informe
- Configuración del tamaño máximo del archivo del informe
- Almacenamiento de informes en archivos
- Limpieza de informes

Autoprotección de Kaspersky Endpoint Security
- Activación y desactivación de Autoprotección
- Activación y desactivación de la compatibilidad con AM-PPL
- Protección de los servicios de la aplicación contra gestión externa
- Soporte de las aplicaciones de administración remota
- Protección con contraseña
  - Activar la protección con contraseña
  - Otorgarle permisos a usuarios o grupos individuales
  - Utilizar una contraseña temporal para otorgar permisos
  - Revocación de contraseña temporal
  - Aspectos especiales de los permisos de la protección con contraseña
  - Restablecimiento de la contraseña de KLAdmin
- Protección de conexión al Servidor de administración

Cifrado de datos
- Limitaciones de funcionalidad del cifrado
- Cómo cambiar la longitud de la clave de cifrado (AES56 o AES256)
- Cifrado de disco de Kaspersky
  - Características especiales del cifrado de unidades SSD
  - Comienzo del Cifrado de disco de Kaspersky
  - Creación de una lista de discos duros excluidos del cifrado
  - Exportar e importar una lista de discos duros excluidos del cifrado
  - Activación de la tecnología de inicio de sesión único (SSO)
  - Administración de cuentas del Agente de autenticación
  - Utilizar una tarjeta inteligente y un token con el Agente de autenticación
  - Descifrado de discos duros
  - Restauración del acceso a una unidad protegida por la tecnología Cifrado de disco de Kaspersky
  - Inicio de sesión con la cuenta de servicio del Agente de autenticación
  - Actualización del sistema operativo
  - Eliminación de errores al actualizar la función de cifrado
  - Seguimiento del agente de autenticación
  - Editar los textos de ayuda del Agente de autenticación
  - Eliminar los objetos y datos restantes después de probar el Agente de autenticación
- Administración de BitLocker
  - Inicio del Cifrado de unidad BitLocker
  - Descifrado de un disco duro protegido por BitLocker
  - Restauración del acceso a una unidad protegida por BitLocker
  - Pausar la protección de BitLocker para actualizar el software
- Cifrado de archivos en unidades locales del equipo
  - Cifrado de los archivos de las unidades del equipo local
  - Creación de reglas de acceso a archivos cifrados para aplicaciones
  - Cifrar archivos creados o modificados por aplicaciones específicas
  - Generación de una regla de descifrado
  - Descifrado de archivos de las unidades del equipo local
  - Creación de paquetes cifrados
  - Restauración del acceso a los archivos cifrados
  - Restauración del acceso a los datos cifrados después del error del sistema operativo
  - Modificación de plantillas de mensajes de acceso a archivos cifrados
- Cifrado de unidades extraíbles
  - Iniciar el cifrado de unidades extraíbles
  - Añadir una regla de cifrado para unidades extraíbles
  - Exportación e importación de una lista de reglas de cifrado para unidades extraíbles
  - Modo portátil para acceder a archivos cifrados de unidades extraíbles
  - Descifrado de unidades extraíbles
- Visualización de los detalles del cifrado de datos
  - Ver el estado de cifrado
  - Ver las estadísticas del cifrado en los paneles de Kaspersky Security Center
  - Ver errores de cifrado de archivos en unidades del equipo local
  - Visualización del informe del cifrado de datos

- Trabajar con dispositivos cifrados cuando no hay acceso a estos
  - Recuperación de datos mediante la Utilidad de restauración FDERT
  - Creación de un disco de rescate del sistema operativo
- Componentes de Detection and Response.
  - Licencias de MDR y EDR Optimum
  - Compatibilidad con soluciones EDR de terceros
  - Kaspersky Endpoint Agent
    - Migrar la configuración [KES + KEA] a la configuración [KES + agente incorporado]
    - Migración de directivas y tareas para Kaspersky Endpoint Agent
  - Endpoint Detection and Response Agent (EDR Agent)
    - Instalación de Instale EDR Agent
    - Integración de EDR Agent con MDR
    - Integración de EDR Agent con EDR (KATA)
    - Integración de EDR Agent con NDR (KATA)
    - Integración de EDR Agent con EDR Expert (on-premises)
    - Compatibilidad con aplicaciones EPP de terceros
  - Managed Detection and Response
    - Integración del agente integrado con MDR
    - Guía de migración de KEA a KES para MDR
  - Endpoint Detection and Response
    - Integración del agente integrado con EDR Optimum/EDR Expert
    - Analizar en busca de indicadores de compromiso (tarea estándar)
    - Telemetría ampliada para Análisis de IOC
    - Mover archivo a la cuarentena
    - Obtener archivo
    - Eliminar el archivo
    - Inicio del proceso
    - Terminar proceso
    - Prevención de ejecución
    - Aislamiento de equipos de la red
    - Sandbox en la nube
    - Guía de migración de KEA a KES para EDR Optimum
  - Kaspersky Sandbox
    - Integración del agente integrado con Kaspersky Sandbox
    - Analizar en busca de indicadores de compromiso (tarea independiente)
    - Guía de migración de KEA a KES para Kaspersky Sandbox
  - Kaspersky Anti Targeted Attack Platform
    - Integración del agente integrado con EDR / NDR (KATA)
    - Configuración de la telemetría de EDR (KATA)
    - Exclusiones de telemetría de EDR (KATA)
      - Ejemplo 1. Procesos excluidos
      - Ejemplo 2. Comunicaciones de red excluidas
      - Ejemplo 3. Operaciones de archivo excluidas
      - Ejemplo 4. Modificaciones de registro excluidas

KATA Sandbox
Integración del agente integrado con KATA Sandbox
Configuración de acciones de respuesta a amenazas
Guía de migración de KEA a KES para EDR (KATA)
Endpoint Detection and Response Expert (on-premises)
Integración del agente integrado con EDR Expert (on-premises)
Configuración de parámetros de telemetría de EDR Expert (on-premises)
Configuración de telemetría de EDR Expert (on-premises)
Exportación e importación de filtros de eventos de EDR Expert (on-premises)
Consideraciones especiales al usar perfiles de política para configurar la integración con EDR Expert (on-premises) y EDR (KATA)
Endpoint Detection and Response Expert (cloud)
Integración del agente integrado con EDR Expert (cloud)
Configuración de parámetros de telemetría de EDR Expert (cloud)
Exclusiones de telemetría de EDR Expert (cloud)
Cómo exportar o importar filtros de eventos de EDR Expert (cloud)
Administración de Cuarentena
Configuración del tamaño máximo de Cuarentena
Envío de datos sobre archivos en Cuarentena a Kaspersky Security Center
Restauración de archivos de la cuarentena
Supervisión de acciones de EDR
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Integración de Kaspersky Endpoint Security con KUMA
Preparación para la integración de KES con KUMA
Conexión de KES a KUMA
Filtrado de eventos que se enviarán a KUMA
Exportación e importación de filtros de eventos de KUMA
Guía de migración de KSWS a KES
Correspondencia de los componentes de KSWS y KES
Correspondencia de la configuración de KSWS y KES
Migración de componentes de KSWS
Migración de tareas y directivas de KSWS
Migración de la zona de confianza de KSWS
Migración de las reglas de Control de inicio de aplicaciones de KSWS
Instalación de KES en lugar de KSWS
Migrar la configuración [KSWS + KEA] a la configuración [KES + agente incorporado]
Asegurarse de que Kaspersky Security for Windows Server se eliminó con éxito
Activación de KES con una clave de KSWS
Consideraciones especiales para migrar servidores de carga alta
Administrar la aplicación en un servidor en modo Server Core
Migración de [KSWS+KEA] a [KES+agente incorporado]
Modo Light Agent para proteger máquinas virtuales
Consideraciones especiales para el modo Light Agent
Configuración preliminar de la máquina virtual
Compatibilidad con la tecnología de Citrix App Layering
Compatibilidad con la tecnología de Citrix Provisioning (Citrix Provisioning Services)
Compatibilidad con la tecnología de Omnissa App Volumes

Instalación de Instale Light Agent
Conexión de Light Agent a SVM
Detección de SVM
Configuración del algoritmo de selección de SVM para Light Agent
Distribución de las conexiones de Light Agents a SVM (etiquetas)
Protección de la conexión entre un Light Agent y SVM
Activación de Light Agent
Guía de migración de KSVLA Light Agent a KES Light Agent
Instalación de KES Light Agent en lugar de KSVLA Light Agent
Correspondencia de los componentes de KSVLA Light Agent y de KES Light Agent
Migración de tareas y directivas de KSVLA Light Agent
Migrar la configuración [KSVLA Light Agent+KEA] a la configuración [KES Light Agent+agente incorporado]
Administración de la aplicación desde la línea de comandos
Setup. Instalación de la aplicación
Setup /x. Eliminar la aplicación
msiexec /i. Recuperando la aplicación
Comandos AVP
SCAN. Análisis antimalware
UPDATE. Actualización de las bases de datos y módulos de la aplicación
ROLLBACK. Reversión de la última actualización
TRACES. Rastreo
START. Iniciar un perfil
STOP. Detener un perfil
STATUS. Estado del perfil
STATISTICS. Estadísticas sobre el funcionamiento de los perfiles
RESTORE. Restauración de archivos de Copia de seguridad
EXPORT. Exportar ajustes de la aplicación
IMPORT. Importar configuración de la aplicación
ADDKEY. Aplicar un archivo clave.
LICENSE. Administración de licencias
RENEW. Compra de una licencia
PBATESTRESET. Restablecer los resultados de la comprobación de disco antes de cifrar el disco
EXIT. Salir de la aplicación
EXITPOLICY. Desactivar una directiva
STARTPOLICY. Activar una directiva
DISABLE. Desactivar la protección
SPYWARE. Detección de spyware
KSN. Cambiar entre KSN/KPSN
SERVERBINDINGDISABLE. Desactivar la protección de conexión del servidor.
Comandos KESCLI
Scan. Análisis antimalware
GetScanState. Estado de finalización del análisis
GetLastScanTime. Especificación del tiempo para completar el análisis
GetThreats. Obtención de datos sobre amenazas detectadas
UpdateDefinitions. Actualización de las bases de datos y módulos de la aplicación
GetDefinitionState. Determinar la fecha y hora de la última actualización de las bases de datos
EnableRTP. Activación de la protección

GetRealTimeProtectionState. Estado de la Protección frente a amenazas en archivos
GetEncryptionState. Estado de cifrado del disco
Version. Identificación de la versión de la aplicación
Comandos de administración de Detection and Response
SANDBOX. Administrar Sandbox
PREVENTION. Administración de la prevención de ejecución
ISOLATION. Administrar el aislamiento de red
RESTORE. Restauración de archivos de la cuarentena
IOCSCAN. Analizar en busca de indicadores de compromiso (IOC)
MDRLICENSE. Activación MDR
EDRKATA. Integración de EDR (KATA)
EDRExpertOnPrem. Integración de EDR Expert (on-premises)
KUMA. Integración de KUMA
YARA. Ejecución de Análisis de YARA
FILTROS DE TELEMETRÍA. Filtrado de eventos que se enviarán a KUMA
Comandos de administración de Light Agent
KSVLAINFO. Determinación del modo Light Agent
VIISINFO. Estado de la conexión del Light Agent al servidor de integración
SVMINFO. Estado de la conexión del Light Agent al Servidor de protección
Códigos de error
Apéndice. Perfiles de la aplicación
Administrar la aplicación a través de la API REST
Instalar la aplicación con la API REST
Funcionamiento con la API
Fuentes de información de la aplicación
Cómo ponerse en contacto con el Soporte técnico
Contenido y almacenamiento de archivos de seguimiento
Rastreo del funcionamiento de aplicaciones
Rastreo del rendimiento de aplicaciones
Escritura de volcado
Protección de archivos de volcado y archivos de seguimiento
Obtención de datos del sistema operativo (Obtener información del sistema de Kaspersky)
Limitaciones y advertencias
Glosario
Administrador de archivos portátil
Agente de autenticación
Agente de red
Archivador
Archivo de IOC
Archivo infectable
Archivo infectado
Autenticación de Kerberos
Base de datos de direcciones web maliciosas
Base de datos de direcciones web phishing
Bases de datos antivirus
Certificado de licencia
Clave activa

Cloud Discovery
Cobertura de protección
Cobertura del análisis
Desinfección
Emisor del certificado
Falsa alarma
Forma normalizada de la dirección de un recurso web
Grupo de administración
IOC
Light Agent
Máscara
Módulo de plataforma segura
Objeto OLE
OpenIOC
Servidor de integración
SVM
Tarea
Apéndices
Apéndice 1. Configuración de la aplicación
Protección frente a amenazas en archivos
Protección frente a amenazas web
Protección frente a amenazas en el correo
Protección frente a amenazas en la red
Firewall
Prevención de ataques de BadUSB
Protección AMSI
Prevención de exploits
Detección de comportamiento
Prevención de intrusiones en el host
Motor de reparación
Kaspersky Security Network
Inspección de registros
Anti-Cryptor
Control Web
Control de dispositivos
Control de aplicaciones
Control de anomalías adaptativo
Control de integridad del sistema
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Integración de KUMA
Cifrado de disco completo
Cifrado de archivos

Cifrado de unidades extraíbles
Plantillas (cifrado de datos)
Exclusiones
Configuración de la aplicación
Informes y almacenamiento
Configuración de red
Interfaz
Administrar configuración
Actualización de las bases de datos y módulos de la aplicación
Apéndice 2. Grupos de confianza de aplicaciones
Apéndice 3. Extensiones de archivo para el análisis rápido de unidades extraíbles
Apéndice 4. Tipos de archivo para el filtrado de adjuntos Protección frente a amenazas en el correo
Apéndice 5. Configuración de red para la interacción con servicios externos
Apéndice 6. Eventos de aplicación
Crítico
Fallo operativo
Advertencia
Mensaje de información
Apéndice 7. Extensiones de archivos compatibles con la Prevención de ejecución
Apéndice 8. Intérpretes de script admitidos para la Prevención de ejecución
Apéndice 9. Cobertura de análisis de IOC en el registro (RegistryItem)
Apéndice 10. Requisitos de los archivos de IOC
Apéndice 11. API para respuesta ante amenazas de EDR
Apéndice 12. Cuentas de usuario en las reglas de los componentes de la aplicación
Información legal
Provisión de datos
Provisión de datos según el Contrato de licencia de usuario final
Provisión de datos al usar Kaspersky Security Network
Provisión de datos al usar soluciones de Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integración con Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Cumplimiento de la legislación de la Unión Europea (GDPR)
Información de marcas registradas
Información sobre el código de terceros

Ayuda de Kaspersky Endpoint Security para Windows

Novedades de la versión 14.2

Se ha añadido compatibilidad con la autenticación basada en tokens para Protección con contraseña.

Novedades de cada versión de Kaspersky Endpoint Security para Windows

Primeros pasos

Despliegue de Kaspersky Endpoint Security para Windows

Configuración inicial de Kaspersky Endpoint Security para Windows

Licencias de Kaspersky Endpoint Security para Windows

Provisión de datos

Debajo del Contrato de licencia de usuario final

Al utilizar el KSN

GDPR

Eliminando amenazas

En estaciones de trabajo

En servidores

Reaccionando a la detección de un Indicador de compromiso (Aislamiento de red → Cuarentena → Prevención de ejecución)

Prácticas recomendadas

Optimizar el rendimiento de la aplicación

Implementar el modo de denegación predeterminado en Control de aplicaciones

Migrar KEA a KES con un agente integrado

Uso de KES como parte de otras soluciones

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Novedades

Actualización 14.2

Kaspersky Endpoint Security 14.2 para Windows introduce las siguientes características y mejoras:

1. Se ha modificado el conjunto de componentes instalados de forma predeterminada. La configuración predeterminada de la aplicación ahora incluye Prevención de ataques de BadUSB, la administración de BitLocker y el agente integrado de EDR Optimum.

2. Se ha añadido compatibilidad con la autenticación basada en tokens (Protección con contraseña). Ahora, para acceder a la aplicación, puede utilizar su nombre de usuario y contraseña, una contraseña temporal proporcionada por el administrador o un token. La autenticación basada en tokens puede utilizarse, por ejemplo, para cuentas de usuario de servicio que no requieran contraseña.

3. Se ha añadido un nuevo criterio de seguridad de las contraseñas para BitLocker: la comprobación del historial de contraseñas. La aplicación impide que los usuarios establezcan una contraseña que ya hayan utilizado.

4. Se ha añadido la posibilidad de cambiar el idioma de la interfaz de Kaspersky Endpoint Security al actualizar la aplicación mediante la tarea *Instalar aplicación de forma remota*. Ahora no es necesario reinstalar la aplicación si ha elegido un idioma de interfaz incorrecto.

5. Se han añadido nuevos eventos de telemetría para los usuarios de las soluciones Kaspersky Endpoint Detection and Response: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Estos nuevos eventos mejoran las capacidades de detección de amenazas de las soluciones de EDR.

6. Se ha añadido compatibilidad con una nueva acción de respuesta a la amenaza, *Colocar archivo*, para los usuarios de Kaspersky Endpoint Detection and Response Expert (on-premises). Esta tarea permite enviar a los equipos archivos de configuración, scripts de respuesta a la amenaza, utilidades para mitigar los efectos de los ataques, etc. La tarea *Colocar archivo* está disponible en la consola OSMP si se ha implementado la versión 9.0 de la solución Kaspersky EDR Expert (on-premises).

7. Se ha mejorado el comportamiento de las acciones de respuesta a la amenaza para los usuarios de Kaspersky Endpoint Detection and Response Optimum. Ahora, antes de realizar la acción (*Eliminar archivo*, *Mover archivo a Cuarentena* o *Prevención de ejecución*), la aplicación comprueba si el objeto es crítico para el sistema (System Critical Object, SCO) y advierte sobre el posible impacto en la estabilidad del sistema. No se recomienda aplicar estas acciones a los archivos de objetos críticos del sistema (SCO).

8. Se ha añadido compatibilidad para que los usuarios de Kaspersky Security for Virtualization Light Agent utilicen la aplicación como parte de un clúster de alta disponibilidad de Servidores de integración. Un clúster de Servidores de integración de alta disponibilidad proporciona protección ininterrumpida del entorno virtual gracias a la conmutación por error de las SVM y los Light Agents a un Servidor de integración de reserva cuando falla el Servidor de integración principal.

9. Al desarrollar esta versión de Kaspersky Endpoint Security, incorporamos los cambios incluidos en los siguientes parches privados: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Actualización 14.1

Kaspersky Endpoint Security 14.1 para Windows introduce las siguientes características y mejoras:

1. Se ha añadido soporte para el sistema operativo Windows Server 2025.

2. Se ha aumentado el límite del número de reglas de filtrado de eventos de telemetría para Endpoint Detection and Response Expert (on-premises) y Kaspersky Endpoint Detection and Response Expert (cloud). Ahora, Kaspersky Endpoint Security admite hasta 10 000 reglas de filtrado de inclusión y exclusión en total.

3. Ahora puede configurar tareas para que se ejecuten solo en días concretos de la semana, en un intervalo de semanas especificado. La programación está disponible en Kaspersky Security Center 16.1 o posterior.

4. Ahora puede especificar un intervalo de tiempo durante el que la tarea *Análisis antimalware* se pausará; por ejemplo, para minimiar el impacto en el rendimiento del equipo durante periodos con una mayor carga.

5. El rendimiento del subsistema del disco duro en el equipo protegido se ha optimizado mediante la reducción del número de operaciones de E/S.

6. Al desarrollar esta versión de Kaspersky Endpoint Security, incorporamos los cambios incluidos en los siguientes parches privados: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Actualización 14.0

Kaspersky Endpoint Security 14.0 para Windows introduce las siguientes características y mejoras:

1. Ahora se admiten los equipos basados en Arm. Puede instalar la aplicación en modo estándar o en modo EDR Agent. Sin embargo, la aplicación tiene varias limitaciones (por ejemplo, entre las tecnologías de cifrado de datos, solo se admite BitLocker).

2. La auditoría de directivas ampliada es compatible con Kaspersky Security Center Web Console versión 15.0 o posterior. Ahora puede ver las revisiones de la directiva y guardarlas en un archivo. Una *revisión* es un conjunto de parámetros modificados guardados por el usuario. Las revisiones le permiten comparar y revertir los cambios en los parámetros de la directiva.

3. Ahora, los nuevos eventos de telemetría están disponibles para los usuarios de Kaspersky Endpoint Detection and Response. Estos nuevos eventos mejoran las capacidades de detección de amenazas mediante las soluciones de Kaspersky EDR.

4. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005 y PF24011.

Actualización 12.12

Kaspersky Endpoint Security 12.12 para Windows introduce las siguientes características y mejoras:

1. La protección de las carpetas compartidas contra el cifrado externo que solía ser parte del componente Detección de comportamiento ahora es un componente independiente, Anti-Cryptor.

2. Se ha añadido soporte para el protocolo Kerberos para autenticar la aplicación a través de un servidor proxy para acceso a Internet.

3. Ahora puede especificar un hash de archivo para una aplicación de confianza, y no solo una ruta completa.

4. Hay más funciones de la tarea *Análisis de IOC* disponibles para los usuarios de las soluciones de Endpoint Detection and Response (EDR). La función Análisis de IOC retrospectivo está disponible. *Análisis de IOC retrospectivo* es un modo de la tarea *Análisis de IOC* en la que Kaspersky Endpoint Security analiza en busca de indicadores de compromiso utilizando datos durante un período de tiempo determinado. Este modo está destinado a detectar indicadores de compromiso en los datos de la actividad de red del equipo. Kaspersky Endpoint Security analiza los datos en los registros del sistema operativo y del navegador en el equipo.

5. Los usuarios de Kaspersky Endpoint Detection and Response (EDR) pueden eliminar el límite de tamaño de la cuarentena. Esto puede ser necesario para el análisis de YARA, porque la aplicación puede guardar un archivo de volcado de memoria grande. Ahora puede usar todo su espacio libre de disco para la cuarentena.

6. La compresión HTTPS ahora es compatible para optimizar la exportación de eventos a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Esto ayuda a reducir el tráfico saliente.

7. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005 y PF24011.

Actualización 12.11

Kaspersky Endpoint Security 12.11 para Windows ofrece las siguientes características y mejoras:

1. La aplicación comprueba la configuración de los componentes de control antes de guardar los parámetros. Se añadió la verificación para los componentes Control de aplicaciones, Control de dispositivos y Control de la integridad del sistema. La aplicación ahora muestra una advertencia si la configuración actual del componente de control puede aumentar la carga en el equipo o causar fallos en el sistema. Por ejemplo, en el caso de Control de aplicaciones, si seleccionó el modo que bloquea todas las aplicaciones excepto las permitidas, y no añadió ninguna regla de permiso, la aplicación muestra una advertencia porque dicha configuración puede causar fallos en el sistema.

2. Se agregó soporte para el envío automático de archivos a KATA Sandbox para su revisión. *KATA Sandbox* es un componente de Kaspersky Anti Targeted Attack Platform que ejecuta archivos en imágenes virtuales de sistemas operativos. Sandbox analiza el comportamiento de los objetos para detectar la actividad maliciosa y la actividad característica de los ataques dirigidos a la infraestructura de TI de la organización. Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Sandbox). Para que KATA Sandbox funcione en modo automático, se debe implementar Kaspersky Anti Targeted Attack Platform 8.0 o posterior.

3. Envío de telemetría de EDR optimizado. Ahora puede especificar la longitud máxima del paquete.

4. Diagnósticos de conexión mejorados para Kaspersky Security Network. Detalles de errores de conexión ampliados para que Kaspersky Security Network resuelta posibles problemas.

5. Se agregó soporte para configurar listas de eventos que se enviarán a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Ahora, además de las listas de eventos predefinidos en KUMA, puede agregar eventos manualmente a la telemetría o excluir eventos por su ID en el Registro de eventos de Windows.

6. Se actualizó la interfaz de directivas en Web Console. El diseño de las secciones de la directiva se ha cambiado para permitir un acceso más rápido a las funciones esenciales.

7. Soporte para Windows 11 25H2.

8. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008 y PF22014.

Actualización 12.10

Kaspersky Endpoint Security 12.10 para Windows ofrece las siguientes características y mejoras:

1. Para el componente Prevención de ataques de BadUSB, se ha añadido la opción de autorizar escáneres de códigos de barras mediante la lectura de un código de barras en la pantalla. Ahora no necesita introducir un código con el teclado en pantalla para autorizar los escáneres de códigos de barras.

2. Las siguientes funciones y mejoras están disponibles para los usuarios de las soluciones Endpoint Detection and Response (EDR) de Kaspersky:

   - Ahora puede administrar el aislamiento de red del equipo en los detalles de la alerta. Además, en los detalles de la alerta puede especificar el período de tiempo de aislamiento de la red del equipo y añadir exclusiones.

   - Completar los detalles de la alerta con nuevos datos. Ahora, los detalles de la alerta contienen más información sobre la amenaza, incluido el comportamiento de la aplicación al responder a las amenazas de EDR.

   - Se ha mejorado el procesamiento de archivos de IOC. Ahora puede ver y editar el contenido de los archivos de IOC en la interfaz de Kaspersky Security Center Web Console. Después de cargar un archivo de IOC, la aplicación muestra un informe sobre la aplicación de términos de IOC.

   - Respuesta mejorada a los IOC detectados. Ahora puede poner en cuarentena los archivos detectados por la tarea *Análisis de IOC* directamente en los resultados de la detección de IOC en las propiedades de la tarea. También puede aislar equipos de la red en las propiedades de la tarea.

   - Ahora puede crear archivos de IOC directamente en las propiedades de la tarea *Análisis de IOC* en función de listas de hashes de archivo, direcciones IP o nombres DNS generados en un archivo TXT.

   - Alcance de análisis ampliado para la tarea *Análisis de IOC*. Ahora puede definir un alcance para el análisis de IOC del registro (**Registro de Windows - RegistryItem**). En versiones anteriores de la aplicación, solo se podía usar un alcance de análisis de IOC predefinido en el registro.

3. Se ha añadido un nuevo permiso de protección con contraseña, *Exportar configuración*. De forma predeterminada, solo el usuario de KL Admin puede crear un archivo de configuración con la configuración de Kaspersky Endpoint Security en la interfaz de la aplicación. Para otorgar acceso a otros usuarios, debe otorgarles el permiso correspondiente.

4. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Actualización 12.9

Kaspersky Endpoint Security 12.9 para Windows ofrece las siguientes características y mejoras:

1. Se ha añadido la nueva funcionalidad para *administrar contraseñas temporales*. La contraseña temporal le permite proporcionar acceso a Kaspersky Endpoint Security con la Protección con contraseña activada para un equipo diferente. La administración de contraseñas temporales permite guardar el historial de contraseñas (hasta 30 días), supervisar el estado de la contraseña temporal (*Activo*, *Caducado*, *Revocado*) y revocar contraseñas temporales.

2. Se ha añadido la opción de finalizar la conexión a recursos web prohibidos por las reglas de Control web inmediatamente después de aplicar la directiva. En versiones anteriores de la aplicación, Control web solo restringía las conexiones nuevas a los recursos web prohibidos.

3. Para los usuarios de Kaspersky Anti Targeted Attack Platform, se ha añadido una opción para ejecutar la verificación YARA localmente en el equipo. Para hacer esto, necesita descargar un archivo con reglas YARA y ejecutar el comando en CMD.

4. Se ha corregido el funcionamiento de la aplicación cuando BitLocker está habilitado en equipos en los que las unidades ya están protegidas por BitLocker con herramientas de terceros. Kaspersky Endpoint Security inicia el procedimiento de recuperación para enviar la clave de recuperación a Kaspersky Security Center. Por lo tanto, la administración de BitLocker se transfiere a la consola de Kaspersky Security Center.

5. Hay disponible una nueva sección, **Historial de respuestas**, para los usuarios de las soluciones Detection and Response de Kaspersky. Esta sección contiene información sobre las acciones de respuesta a amenazas realizadas en el equipo. Tales acciones incluyen, por ejemplo, ejecutar la tarea *Terminar proceso* o aislar el equipo de la red. El historial de respuestas solo está disponible para usuarios de las siguientes soluciones de Kaspersky: MDR, EDR, KATA.

6. Los usuarios de la Kaspersky Unified Monitoring and Analysis Platform disponen ahora de compatibilidad con las acciones de respuesta ante amenazas de EDR. Al responder a las amenazas, KUMA ejecuta scripts que crean las tareas EDR correspondientes. Para realizar tareas de EDR, debe crear una regla de respuesta para el script personalizado en la consola de KUMA y seleccionar eventos.

7. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Actualización 12.8

Kaspersky Endpoint Security 12.8 para Windows ofrece las siguientes características y mejoras:

1. La aplicación ahora es compatible con el modo Light Agent para proteger entornos virtuales. Ahora puede implementar la aplicación como Light Agent como parte de la solución Kaspersky Security for Virtualization Light Agent 6.2.

2. Ahora se admite la intercepción de operaciones de archivos en contenedores Docker en servidores. Un *contenedor* es un entorno aislado en el que se puede ejecutar una aplicación sin interactuar directamente con el sistema operativo. Kaspersky Endpoint Security analiza los archivos dentro de los contenedores a los que el usuario obtiene acceso. Cuando se detecta una amenaza, la aplicación bloquea dicha actividad e intenta desinfectar el archivo del interior del contenedor. Si el archivo no se puede desinfectar, la aplicación detiene el contenedor.

3. Ahora puede definir una cobertura de protección para la protección de carpetas compartidas contra el cifrado externo (componente Detección de comportamiento). Ahora puede especificar carpetas compartidas que la aplicación debe supervisar para detectar la actividad de los archivos. También puede excluir archivos del cobertura de protección. En versiones anteriores de la aplicación, el componente Detección de comportamiento supervisaba todas las carpetas compartidas para detectar la actividad de los archivos.

4. Ahora puede configurar diferentes conjuntos de componentes para diferentes tipos de sistemas operativos en el paquete de instalación. Es decir, puede implementar la aplicación en estaciones de trabajo y servidores usando el mismo paquete de instalación. Los componentes que no están disponibles para un determinado tipo de sistema operativo se excluyen automáticamente en las propiedades del paquete de instalación.

5. Se ha añadido la opción para seleccionar exclusiones de análisis predefinidas y aplicaciones de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas permiten configurar rápidamente la zona de confianza para la aplicación en un entorno virtual (Citrix, VMware). Estas exclusiones comprenden, por ejemplo, archivos de máquinas virtuales VHD y VHDX. Se pueden añadir exclusiones al crear un paquete de instalación de la aplicación, crear una directiva o al instalar Kaspersky Endpoint Security.

6. La telemetría EDR ahora incluye eventos para operaciones con dispositivos conectados por USB. También puede añadir estos eventos a las exclusiones de la telemetría EDR.

7. Se ha añadido la opción de bloquear las conexiones de red a través del protocolo TLS 1.0 obsoleto. TLS 1.0 tiene un nivel de seguridad bajo, por lo que se recomienda desactivar este protocolo y usar versiones más recientes de TLS 1.2 o TLS 1.3. De forma predeterminada, Kaspersky Endpoint Security bloquea las conexiones TLS 1.0. Después de actualizar la versión de la aplicación, el funcionamiento de los servicios de terceros que utilizan el protocolo TLS 1.0 puede fallar. Para evitar problemas en el funcionamiento de los servicios de terceros, puede permitir el uso del protocolo TLS 1.0 en la directiva de grupo antes de actualizar la versión de la aplicación.

8. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Actualización 12.7

Kaspersky Endpoint Security 12.7 para Windows ofrece las siguientes características y mejoras:

1. Ahora puede limitar el uso de recursos de la CPU para tareas de *análisis de malware*. Para hacerlo, en la configuración de la aplicación, especifique el porcentaje máximo de carga de la CPU para todos los núcleos que se pueden utilizar al analizar el equipo.

2. Ahora puede enviar archivos para su análisis en KATA Sandbox manualmente. *KATA Sandbox* es un componente de Kaspersky Anti Targeted Attack Platform que ejecuta archivos en imágenes virtuales de sistemas operativos. Sandbox analiza el comportamiento de los objetos para detectar la actividad maliciosa y la actividad característica de los ataques dirigidos a la infraestructura de TI de la organización. Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Sandbox). Para enviar un archivo para su análisis a KATA Sandbox, seleccione el comando correspondiente en el menú contextual del archivo.

3. Ahora puede configurar la integración con la solución que protege la LAN corporativa, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) es parte de Kaspersky Anti Targeted Attack Platform. Puede configurar la interacción con NDR en modo estándar así como en el modo EDR Agent.

4. Se ha añadido compatibilidad con el cliente de correo electrónico Microsoft Office Outlook versión 2021 a la extensión de Protección frente a amenazas en el correo. La extensión permite analizar mensajes a nivel de cliente de correo en lugar de a nivel de protocolo. Además de los mensajes, la extensión le permite analizar objetos recibidos a través de la interfaz MAPI desde los repositorios de Microsoft Exchange (por ejemplo, objetos en el Calendario). Este análisis se lleva a cabo en el cliente de correo.

5. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Actualización 12.6

Kaspersky Endpoint Security 12.6 para Windows ofrece las siguientes características y mejoras:

1. La funcionalidad para la integración con la solución Kaspersky SIEM (*Kaspersky Unified Monitoring and Analysis Platform (KUMA)*) se ha añadido. Ahora es posible enviar eventos desde los registros de eventos de Windows al recopilador de KUMA. Esto permite que KUMA reciba eventos de Windows (se admite un conjunto limitado de EventID) desde todos los equipos en los que Kaspersky Endpoint Security está instalado, sin instalar agentes de KUMA en estos equipos.

2. Se añadió un nuevo componente de *Control de integridad del sistema* para reemplazar el componente Monitor de integridad de archivos. El componente Control de integridad del sistema incluye todas las funciones de Monitor de integridad de archivos y, además, permite supervisar los cambios en el registro y la conexión de dispositivos externos. El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que pueden indicar infracciones de la seguridad del equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos correspondientes y alerta al administrador. El Monitor de integridad de archivos ya no es parte de la aplicación. La configuración del Monitor de integridad de archivos se migra automáticamente a Control de integridad del sistema cuando actualiza la aplicación. Para garantizar el correcto funcionamiento del Control de integridad del sistema, tanto la aplicación Kaspersky Endpoint Security como el complemento de administración deben actualizarse a la versión 12.6.

3. El estado del EDR Agent integrado (KATA) instalado se ha agregado a las propiedades del equipo en la consola de Kaspersky Security Center. Ahora, si tiene un EDR Agent integrado (KATA) instalado, la columna **Estado del Endpoint Sensor** muestra el estado actual del componente (por ejemplo, *En ejecución*, *Detenido*, *No admitido por la licencia*, etc.).

4. Se ha añadido la opción para seleccionar exclusiones de análisis predefinidas y aplicaciones de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente la zona de confianza cuando se usa la aplicación en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Estas exclusiones comprenden, por ejemplo, archivos de bases de datos MDF y LDF. Se pueden añadir exclusiones al crear una nueva directiva, modificar una directiva existente o instalar Kaspersky Endpoint Security.

5. La visualización de los detalles de la alerta para Kaspersky Endpoint Detection and Response Optimum se ha movido del complemento de administración de Kaspersky Endpoint Security a un complemento de administración de Kaspersky Endpoint Detection and Response independiente. El complemento de administración de EDR es un complemento único para trabajar con agentes en los sistemas operativos Windows, Mac y Linux. Ahora, al trabajar con EDR Optimum, necesitará el complemento de administración de Kaspersky Endpoint Security para crear tareas de respuesta a amenazas y el complemento de administración de EDR para ver los detalles de la alerta.

6. Soporte para Windows 11 24H2.

7. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Actualización 12.5

Kaspersky Endpoint Security 12.5 para Windows ofrece las siguientes características y mejoras:

1. Se añadió la opción de configurar exclusiones de telemetría. *Telemetría* es una lista de eventos que han ocurrido en el equipo protegido. Kaspersky Anti Targeted Attack Platform (EDR) utiliza los datos de telemetría para supervisar y proteger la infraestructura de TI de la organización. La configuración de las exclusiones de telemetría ayuda a mejorar el rendimiento del equipo y optimizar la transmisión de datos al servidor de recopilación de telemetría.

2. Se mejoró la interfaz de la zona de confianza de la aplicación. Kaspersky Endpoint Security ahora oculta los objetos de la zona de confianza al usuario si el administrador le prohibió añadir sus propias exclusiones de análisis (locales) y aplicaciones de confianza. Esto evita que un intruso acceda sin autorización a la zona de confianza, lo que aumenta el nivel de seguridad del equipo.

3. Se añadió la opción de analizar el tráfico de los clientes de correo de MyOffice Mail y R7-Office Organizer. El componente Protección frente a amenazas en el correo ahora no solo analiza los archivos adjuntos de los mensajes al descargarlos, sino también los mensajes enviados y recibidos.

4. Se añadió una nueva categoría de recursos web: *Herramientas de IA generativa*. Puede configurar el acceso a los sitios web desde la nueva categoría mediante Control web.

5. Ahora puede seleccionar la ubicación de una reglas de paquetes de red en la lista Firewall. La ubicación de una regla de paquetes de red en la lista determina su prioridad. En versiones anteriores de la aplicación, una nueva regla solo se podía añadir al final de la lista, después de lo cual tenía que mover manualmente la regla a través de la lista para priorizarla. Ahora, al añadir una regla, puede elegir si la regla se debe colocar al principio, al final de la lista o al lado de la regla seleccionada.

6. En las reglas de los componentes de Kaspersky Endpoint Security, ahora puede seleccionar usuarios de la lista de usuarios en Kaspersky Security Center, además de Active Directory. También puede introducir los datos de la cuenta de usuario de forma manual. Esta posibilidad se añadió para las reglas de los siguientes componentes: Control de aplicaciones, Control de dispositivos, Control web, Control de anomalías adaptativo e Inspección de registros.

7. El informe de detección de ataques de red ahora incluye una columna con la dirección MAC del equipo atacante (el componente de Protección frente a amenazas en la red). Ahora puede ver la dirección MAC del equipo atacante en el informe, además de su dirección IP. Esto es útil para la investigación de incidentes. Los informes, que contienen la dirección MAC del equipo atacante, también estarán disponibles en la consola de Kaspersky Security Center Linux versión 15.1 y posteriores.

8. Se ha aumentado el nivel de los requisitos de protección informática. El alto nivel de protección ahora requiere activar la Protección de los servicios de la aplicación contra la administración externa. Compruebe el indicador del nivel de seguridad en la parte superior de la ventana de la directiva. Si tiene un nivel de seguridad medio o bajo, puede activar la Protección de los servicios de la aplicación contra la administración externa en la ventana de recomendación del indicador de nivel de seguridad.

9. Se ha añadido el soporte para nuevos eventos de detección de objetos cuando la aplicación se ejecuta en la configuración de Endpoint Detection and Response Agent (EDR Agent). Estos eventos ya se admitían en la configuración de [KES+agente integrado].

10. Al desarrollar esta versión de Kaspersky Endpoint Security para Windows, incorporamos los cambios incluidos en los siguientes parches privados: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Actualización 12.4

Kaspersky Endpoint Security 12.4 para Windows ofrece las siguientes características y mejoras:

1. Se ha añadido una nueva función para proteger la conexión del equipo a Kaspersky Security Center. La nueva tarea *Protección de la conexión al servidor de administración* permite establecer una contraseña para realizar la conexión a un servidor de confianza. Esto significa que no es posible reconectar el equipo y ejecutar comandos desde otro servidor sin esta contraseña.

2. Para el componente Protección con contraseña, se ha añadido la capacidad de seleccionar usuarios manualmente y no solo de Active Directory. Es decir, puede especificar manualmente un nombre de usuario y contraseña, y asignar derechos de acceso a Kaspersky Endpoint Security para dicha cuenta. De esta forma, no necesita compartir su contraseña de administrador de KLAdmin con otros usuarios o crear nuevas cuentas de usuario de Active Directory para controlar el acceso a la aplicación.

3. Soporte para Windows 11 23H2.

Actualización 12.3

Kaspersky Endpoint Security 12.3 para Windows ofrece las siguientes características y mejoras:

1. Ahora puedes instalar la aplicación en la configuración de Endpoint Detection and Response Agent. Esta configuración permite instalar la aplicación con un conjunto de componentes requeridos por las soluciones de Detection and Response de Kaspersky: Kaspersky Managed Detection and Response y Kaspersky Anti Targeted Attack Platform (EDR). Puede instalar la aplicación en esta configuración junto con soluciones de terceros (por ejemplo, Dr.Web, Dallas Lock, ESET). Esto le permite utilizar herramientas de seguridad de infraestructura de terceros junto con Detection and Response de Kaspersky.

2. Se ha mejorado el funcionamiento de Kaspersky Endpoint Security con dispositivos con Bluetooth. Ahora puede configurar exclusiones y restringir el acceso a todos los dispositivos con Bluetooth, excepto los dispositivos de entrada (teclados inalámbricos, ratones, etc.).

3. Se ha optimizado el funcionamiento del componente Control de aplicaciones con la base de datos de archivos ejecutables. Kaspersky Endpoint Security ahora elimina automáticamente la información del archivo de la base de datos si el archivo se elimina del equipo. Esto permite mantener la base de datos actualizada y ahorrar recursos de Kaspersky Security Center.

4. Se ha aumentado el nivel de los requisitos de protección informática. Ahora, el nivel de protección alto protección requiere activar la protección con contraseña. Compruebe el indicador del nivel de seguridad en la parte superior de la ventana de la directiva. Si tiene un nivel de protección medio o bajo, puede activar la protección con contraseña en la ventana de recomendación del indicador de nivel de seguridad.

5. Se ha añadido compatibilidad con el protocolo HTTPS para permitir que la aplicación funcione con Kaspersky Security Network. Active el uso de HTTPS en las propiedades del Servidor de administración de la configuración del servidor proxy de KSN.

Actualización 12.2

Kaspersky Endpoint Security 12.2 para Windows ofrece las siguientes características y mejoras:

1. Se ha añadido compatibilidad con el protocolo WPA3 para controlar las conexiones a las redes Wi-Fi (Control de dispositivos). Ahora puede seleccionar el protocolo WPA3 en la configuración de red Wi-Fi de confianza y denegar la conexión a la red usando un protocolo menos seguro.

2. Ahora puede elegir un protocolo y puertos para las exclusiones de Protección frente a amenazas en la red. Ahora, además de especificar las direcciones IP de los dispositivos de confianza, también puede seleccionar un puerto y un protocolo. Esto le permite excluir flujos de datos individuales y evitar ataques a la red desde direcciones IP de confianza.

3. Diferente orden de fuentes de orígenes de actualizaciones para la tarea *Actualización de las bases de datos y módulos de la aplicación local* si se aplica una directiva al equipo. Ahora, el servidor de Kaspersky Security Center se usa de forma predeterminada como primer origen de actualizaciones en lugar de los servidores de Kaspersky. Esto ayuda a ahorrar tráfico cuando el usuario ejecuta la tarea *Actualización de las bases de datos y módulos de la aplicación* local.

Actualización 12.1

Kaspersky Endpoint Security 12.1 para Windows ofrece las siguientes características y mejoras:

1. Se ha añadido un agente integrado para la solución Kaspersky Anti Targeted Attack Platform. Ya no necesita Kaspersky Endpoint Agent para utilizar EDR (KATA). Kaspersky Endpoint Security realizará todas las funciones de Kaspersky Endpoint Agent. Para migrar las directivas de Kaspersky Endpoint Agent, utilice el Asistente de migración. Tras actualizar la aplicación, Kaspersky Endpoint Security pasa a utilizar el agente integrado y elimina Endpoint Agent de Kaspersky. Kaspersky Endpoint Agent se ha agregado a la lista de software incompatible. Kaspersky Endpoint Security tiene agentes integrados para todas las soluciones de Detection and Response, por lo que ya no es necesario instalar Kaspersky Endpoint Agent para integrarse con esas soluciones.

2. Ahora el modo de compatibilidad de Azure WVD es compatible. Esta función garantiza que el estado de las máquinas virtuales de Azure se muestre correctamente en la consola de Kaspersky Anti Targeted Attack Platform. El modo de compatibilidad de Azure WVD permite asignar un ID de sensor único y permanente a estas máquinas virtuales.

3. Ahora puede configurar el acceso de los usuarios a dispositivos móviles en iTunes o aplicaciones similares. Es decir, puede, por ejemplo, permitir que el dispositivo móvil se use solo en iTunes y bloquear el uso del dispositivo móvil como unidad extraíble. La aplicación también admite estas reglas para la aplicación Android Debug Bridge (ADB).

4. Kaspersky Security Center versión 11 ya no es compatible. Actualice Kaspersky Security Center a la versión más reciente.

Problemas solucionados

La siguiente tabla enumera todos los problemas detectados en versiones anteriores de Kaspersky Endpoint Security y solucionados en la versión actual.

Lista de problemas solucionados en la versión 14.2

Identificador	Descripción
10110351	El componente Control de dispositivos permite acceder a un dispositivo MTD (tarjeta SD) cuando se selecciona la acción **Bloquear** para el tipo de dispositivo **Unidades extraíbles**.
10068496	En un dispositivo protegido, se puede cambiar el modo de Protección contra el spoofing de MAC aunque la configuración de Protección frente a amenazas en la red esté bloqueada en la directiva principal.
10095087	Cuando está activado el análisis de conexiones cifradas, el acceso a cualquier sitio web a través de un Firewall de nueva generación (NGFW) con un certificado revocado genera una notificación que indica que se está redirigiendo a un dominio con un certificado que no es de confianza.
10140912	Con la aplicación instalada, el equipo no detecta el dispositivo PDA BHT1100B con Windows Mobile.
10141009	Si el componente Cifrado de archivos está instalado, es posible que la aplicación Anthropic Claude no se inicie.
10610853	Después de actualizar a la nueva versión, no se puede abrir la directiva porque la configuración de Control de dispositivos de la nueva versión incluye dispositivos que no son compatibles con la versión anterior.

Identificador	Descripción
10720516	Es posible que los archivos adjuntos de los archivos en formatos de Office no se abran cuando la aplicación está instalada.
10421967	No se puede iniciar sesión en un buzón compartido si se ha añadido como una cuenta independiente.

Lista de problemas solucionados en el complemento web 14.2.0.8289

Identificador	Descripción
9946286	Al añadir la dirección de un sitio web a una regla de Control web, no se puede utilizar una máscara que no incluya un punto entre el dominio y la zona de dominio.
10054657 10507166	Después de migrar a la nueva versión, algunos componentes (como Control de dispositivos y Control de aplicaciones) no se pueden administrar mediante la directiva.
10084390	En la configuración del componente Control de dispositivos, el tipo de dispositivo **Disco duro** aparece duplicado, lo que provoca que se bloqueen los discos duros de los usuarios.
10113718	En algunos casos, no se muestran las reglas personalizadas de Firewall.
10311613	En la configuración del componente Prevención de intrusiones en el host, no se puede añadir un recurso protegido mediante una máscara con el carácter `*`.
10391923	En Control de aplicaciones, al crear una categoría de aplicaciones basada en el hash MD5 de un archivo, no se muestra ninguna advertencia que indique que dicha categoría no es válida y no funcionará.
10571790	Se ha corregido el título de la lista de reglas de bloqueo del componente Control de aplicaciones en el modo **Permitir todo lo que no esté especificado en la lista de reglas**.
10592891 10689065	En la zona de confianza, el campo **Comentario** no se muestra para las exclusiones de la sección **Exclusiones del análisis antimalware**.
10613015 10689049 10592534	En el componente Control de dispositivos, el campo **Comentario** no se muestra para los dispositivos de confianza.
10645068 10689057	La tarea *Eliminar clave* no se ejecuta si se selecciona un archivo de clave de licencia en formato KEY.
10685370 10685422	En el componente Control de dispositivos, no se puede añadir un dispositivo nuevo a la lista de dispositivos de confianza si ya hay uno con el mismo nombre en la lista.
10721136	Las tareas de grupo no se pueden guardar si no se especifica una fecha de finalización en la configuración de la programación.
10753509	Al modificar la lista de usuarios y grupos de los dispositivos de confianza en el componente Control de dispositivos, pueden cambiar los tipos de registro, lo que hace que la configuración deje de aplicarse al dispositivo.
10773402	En algunos casos, es posible que los cambios en la configuración de la directiva no se guarden debido a perfiles dañados.
10822620	La configuración del componente Anti-Cryptor no se muestra en la directiva y los cambios en la configuración de las notificaciones no se guardan.
10817035	En una directiva secundaria, se permite añadir un dispositivo de confianza aunque esta opción esté desactivada en la directiva principal (candado cerrado). Sin embargo, el dispositivo añadido no se guarda.
10678009	En el complemento web de Kaspersky Endpoint Security, no se puede añadir una nueva regla de Firewall a una directiva si anteriormente se creó una regla con un intervalo de direcciones IP.

Lista de problemas solucionados en la versión 14.1

Identificador	Descripción
10140523	La activación de NVMe nativo en Windows 11 puede provocar un comportamiento inestable de la aplicación.
9340076	En un dispositivo con la aplicación instalada y el componente Cifrado de archivos activado, el Explorador de Windows no actualiza automáticamente el contenido de una carpeta de red después de que este se modifique desde otro dispositivo.

Identificador	Descripción
9722863	El informe de Control de dispositivos no incluye el evento de desconexión de token USB.
10006481	Después de aplicar una regla que deniega el tráfico entrante, las conexiones TCP activas a servicios externos pueden finalizar prematuramente debido a un cálculo incorrecto del tiempo de espera.
10140912	La aplicación no detecta el dispositivo PDA BHT1100B.
10157563	Es posible que Folder Redirection no funcione después de reiniciar en estaciones de trabajo VDI.
10158494	Control de dispositivos registra varios eventos de conexión y desconexión de un dispositivo extraíble sin que este se haya vuelto a conectar físicamente.

Preguntas frecuentes

GENERAL

¿En qué equipos puedo usar Kaspersky Endpoint Security?

¿Qué ha cambiado desde la última versión?

¿Con qué otras aplicaciones de Kaspersky puede funcionar Kaspersky Endpoint Security?

¿Cómo puedo reducir el impacto de Kaspersky Endpoint Security en los recursos del equipo?

INSTALACIÓN

¿Cómo puedo instalar Kaspersky Endpoint Security en todos los equipos de mi organización?

¿Qué parámetros de instalación puedo configurar en la línea de comandos?

¿Cómo puedo desinstalar Kaspersky Endpoint Security de forma remota?

ACTUALIZACIÓN

¿Cuáles son los métodos para actualizar las bases de datos?

¿Qué debo hacer si surgen problemas después de una actualización?

¿Cómo actualizo las bases de datos fuera de la red corporativa?

¿Puedo usar un servidor proxy para realizar una actualización?

SEGURIDAD

¿Cómo analiza Kaspersky Endpoint Security el correo electrónico?

¿Cómo evito que un archivo de confianza se analice?

¿Cómo protejo el equipo contra las unidades flash infectadas?

¿Cómo puedo realizar un análisis antimalware sin que el usuario lo sepa?

¿Cómo pongo en pausa la protección de Kaspersky Endpoint Security?

¿Cómo restauro un archivo que Kaspersky Endpoint Security ha eliminado por error?

¿Cómo puedo evitar que los usuarios desinstalen Kaspersky Endpoint Security?

INTERNET

¿Es posible analizar conexiones cifradas (HTTPS) con Kaspersky Endpoint Security?

¿Qué debo hacer para que los usuarios solo puedan conectarse a redes wifi de confianza?

¿Cómo bloqueo las redes sociales?

APLICACIONES

¿Cómo puedo averiguar qué aplicaciones están instaladas en el equipo de un usuario (inventario)?

¿Cómo evito que se ejecuten videojuegos?

¿Cómo verifico si Control de aplicaciones se ha configurado correctamente?

¿Cómo añado una aplicación a la lista de aplicaciones de confianza?

DISPOSITIVOS

¿Cómo puedo impedir el uso de unidades flash?

¿Cómo añado un dispositivo a la lista de dispositivos de confianza?

¿Es posible obtener acceso a un dispositivo bloqueado?

CIFRADO

¿En qué casos no es posible usar las funciones de cifrado?

¿Cómo puedo restringir con contraseña el acceso a un archivo de almacenamiento?

¿Puedo usar una tarjeta inteligente o un token con las funciones de cifrado?

¿Puedo acceder a los archivos que cifre si no tengo conexión con Kaspersky Security Center?

¿Qué debo hacer ante un problema con el sistema operativo si mi información está cifrada?

SOPORTE

¿Dónde se guardan los archivos de los informes?

¿Cómo creo un archivo de seguimiento?

¿Cómo activo la creación de archivos de volcado?

Kaspersky Endpoint Security para Windows

Kaspersky Endpoint Security para Windows (en lo sucesivo denominado Kaspersky Endpoint Security) proporciona a los equipos una protección integral contra diversos tipos de amenazas, ataques de red y phishing.

La aplicación no está destinada a utilizarse en procesos tecnológicos que involucren sistemas de control automatizados. Para proteger los dispositivos en dichos sistemas, se recomienda utilizar la aplicación Kaspersky Industrial CyberSecurity for Nodes.

Tecnologías de detección de amenazas



Aprendizaje automático

Kaspersky Endpoint Security utiliza un modelo basado en el aprendizaje automático. El modelo está desarrollado por expertos de Kaspersky. Luego, el modelo se alimenta continuamente con datos de amenazas de KSN (capacitación de modelos).



Análisis de nube

Kaspersky Endpoint Security recibe datos de amenazas de Kaspersky Security Network. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software.



Análisis experto

Kaspersky Endpoint Security utiliza datos de amenazas añadidos por los analistas de virus de Kaspersky. Los analistas de virus evalúan los objetos si la reputación de un objeto no se puede determinar automáticamente.



Análisis de comportamiento

Kaspersky Endpoint Security analiza la actividad de un objeto en tiempo real.



Análisis automático

Kaspersky Endpoint Security recibe datos del sistema automático de análisis de objetos. El sistema procesa todos los objetos que se envían a Kaspersky. Luego, el sistema determina la reputación del objeto y añade los datos a las bases de datos antivirus. Si el sistema no puede determinar la reputación del objeto, el sistema consulta a los analistas de virus de Kaspersky.



Sandbox

Kaspersky Endpoint Security procesa el objeto en una máquina virtual. Kaspersky Sandbox analiza el comportamiento de un objeto y decide acerca de su reputación. Esta tecnología solo está disponible si se utiliza la solución Kaspersky Sandbox.



Sandbox en la nube

Kaspersky Endpoint Security analiza objetos en un entorno aislado que proporciona Kaspersky. La tecnología Sandbox en la nube se activa de manera permanente y está disponible para todos los usuarios de Kaspersky Security Network, más allá del tipo de licencia que usen. Si ya implementó la solución Endpoint Detection and Response, puede activar un contador individual para las amenazas detectadas por Sandbox en la nube.

Árbol de selección

Un componente específico gestiona cada tipo de amenaza. Los componentes se pueden activar o desactivar de forma independiente y es posible configurar sus ajustes.

Sección	Componente
Protección frente a amenazas básicas 	**Protección frente a amenazas en archivos** El componente Protección frente a amenazas en archivos le permite evitar la infección del sistema de archivos del equipo. De forma predeterminada, el componente Protección frente a amenazas en archivos reside permanentemente en la RAM del equipo y analiza todos los archivos abiertos, guardados o ejecutados en tiempo real. Este componente analiza archivos en todas las unidades del equipo, incluidas las unidades conectadas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico. **Protección frente a amenazas web** El componente Protección frente a amenazas web evita la descarga de archivos maliciosos de internet y también bloquea la conexión a sitios web maliciosos y de phishing. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico. **Protección frente a amenazas en el correo** El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico. Protección frente a amenazas en el correo puede analizar tanto los mensajes entrantes como los salientes. La aplicación es compatible con POP3, SMTP, IMAP y NNTP en los siguientes clientes de correo: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Para analizar el tráfico en los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, debe añadir el certificado de Kaspersky a la tienda de certificados y seleccionar su tienda propia de certificados. Protección frente a amenazas en el correo no es compatible con otros protocolos y clientes de correo. Es posible que Protección frente a amenazas en el correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, Protección frente a amenazas en el correo incluye una extensión para Microsoft Office Outlook. La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección frente a amenazas en el correo admite las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365. En equipos basados en Arm, la extensión Protección frente a amenazas en el correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64. **Protección frente a amenazas en la red** El componente *Protección frente a amenazas en la red* (también denominado Intrusion Detection System, IDS) supervisa el tráfico de red entrante en busca de actividad característica de los ataques de red. Cuando la aplicación detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante. Las bases de datos de la aplicación ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos. La lista de ataques de red que detecta el componente Protección frente a amenazas en la red se actualiza durante las actualizaciones de módulos de aplicaciones y bases de datos. **Firewall** El componente Firewall bloquea las conexiones no autorizadas a un equipo mientras se trabaja en Internet o en una red local. Firewall también controla la actividad de red de las aplicaciones en el equipo. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y *reglas de red* predefinidas. **Prevención de ataques de BadUSB** El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo. **Protección AMSI** El componente Protección AMSI está diseñado para admitir la Interfaz de análisis antimalware de Microsoft. La *interfaz de análisis antimalware (AMSI)* permite que las aplicaciones de terceros con soporte de la AMSI envíen a Kaspersky Endpoint Security aquellos objetos para los cuales precisan un análisis adicional (por ejemplo, scripts de PowerShell). Una vez que el análisis se completa, el resultado se devuelve a la aplicación que originó la solicitud.

Sección	Componente
Protección frente a amenazas avanzadas 	**Kaspersky Security Network** *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, los servicios de KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web que se analicen, así como sobre la categoría y reputación de los archivos analizados. **Detección de comportamiento** El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones de su equipo y ofrece esta información a otros componentes de protección mejorar su rendimiento. El componente Detección de comportamientos utiliza firmas de patrones de actividad peligrosa (Behavior stream signatures, BSS) para aplicaciones. Si la actividad de la aplicación coincide con una BSS Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security se basa en bases de datos de reglas heurísticas ofrece protección proactiva al equipo. El componente Detección de comportamiento también supervisa los puertos de red en busca de procesos de aplicaciones que puedan poner en peligro la seguridad del equipo. La aplicación obtiene información sobre dichos procesos con bases de datos antivirus. **Anti-Cryptor** El componente Anti-Cryptor analiza la actividad en las carpetas compartidas. Si esta actividad coincide con un tipo de comportamiento típico del cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada. **Prevención de exploits** El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para hacerlo, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malicioso. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario. El componente Prevención de exploits también supervisa los puertos de red en busca de procesos de aplicaciones que puedan poner en peligro la seguridad del equipo. La aplicación obtiene información sobre dichos procesos con bases de datos antivirus. **Prevención de intrusiones en el host** El componente Prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus y el servicio en la nube Kaspersky Security Network. **Motor de reparación** El componente Motor de reparación permite a Kaspersky Endpoint Security anular acciones que han sido realizadas por el malware en el sistema operativo.

Sección	Componente
Controles de seguridad 	**Control de aplicaciones** El Control de aplicaciones gestiona el inicio de aplicaciones en los equipos de los usuarios. Esto le permite implementar una directiva corporativa de seguridad al usar aplicaciones. El Control de aplicaciones también reduce el riesgo de infección del equipo al restringir el acceso a las aplicaciones. **Control de dispositivos** Control de dispositivos administra el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi). Esto le permite proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos. **Control Web** Control web permite regular el acceso de los usuarios a los recursos web. El componente ayuda a reducir tanto el volumen de tráfico como el tiempo que se malgasta en actividades no laborales. Cuando un usuario intenta abrir un sitio web que se ha restringido mediante Control web, Kaspersky Endpoint Security bloquea el acceso o muestra una advertencia. **Control de anomalías adaptativo** El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos en una red de la empresa. El Control de anomalías adaptativo utiliza un conjunto de reglas para supervisar el comportamiento atípico (por ejemplo, la regla *Inicio de Microsoft Powershell desde una aplicación de Office*). Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa. Puede configurar el modo en que el Control de anomalías adaptativo gestiona cada regla y, por ejemplo, permitir la ejecución de scripts de PowerShell que automatizan determinadas tareas de flujo de trabajo. Kaspersky Endpoint Security actualiza el conjunto de reglas junto con las bases de datos de la aplicación. **Inspección de registros** La inspección de registros supervisa la integridad del entorno protegido basándose en los resultados del análisis del Registro de eventos de Windows. Cuando la aplicación detecta señales de comportamientos atípicos en el sistema, informa al administrador debido a que este comportamiento puede indicar un intento de ataque cibernético. **Control de integridad del sistema** El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que pueden indicar infracciones de la seguridad del equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos correspondientes y alerta al administrador.
Tareas 	**Análisis antimalware** Kaspersky Endpoint Security analiza el equipo para detectar virus y otras amenazas. El análisis antimalware ayuda a descartar la posibilidad de que se propague malware que los componentes de protección no hayan detectado, por ejemplo, debido a un nivel de seguridad bajo. **Actualización de las bases de datos y módulos de la aplicación** Kaspersky Endpoint Security descarga bases de datos y módulos de la aplicación actualizados. La actualización mantiene el equipo protegido contra los virus más recientes y otras amenazas. De forma predeterminada, la aplicación se actualiza automáticamente, pero, si es necesario, puede actualizar las bases de datos y los módulos de la aplicación manualmente. **Reversión de la última actualización** Kaspersky Endpoint Security revierte la última actualización de bases de datos y módulos. Esto le permite revertir las bases de datos y los módulos de aplicación a sus versiones anteriores cuando sea necesario, por ejemplo, si la nueva versión de la base de datos contiene una firma no válida que hace que Kaspersky Endpoint Security bloquee una aplicación segura. **Comprobación de integridad de la aplicación** Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en la carpeta de instalación de la aplicación en busca de datos corruptos o modificaciones. Si un módulo de la aplicación tiene una firma digital incorrecta, el módulo se considera corrupto.
Cifrado de datos 	**Cifrado de archivos** El componente permite crear reglas de cifrado de archivos. Puede seleccionar carpetas predeterminadas para el cifrado, seleccionar una carpeta manualmente o seleccionar archivos individuales por extensión. **Cifrado de disco completo** El componente permite cifrar el disco duro mediante el Cifrado de disco de Kaspersky o el Cifrado de unidad BitLocker. **Cifrado de unidades extraíbles** El componente permite proteger datos en unidades extraíbles. Puede utilizar el Cifrado de disco completo (FDE) o Cifrado de archivos (FLE).

Sección	Componente
Detection and Response 	**Endpoint Detection and Response Optimum** Agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante también "EDR Optimum"). *Kaspersky Endpoint Detection and Response* es una solución para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Agente integrado para la solución Kaspersky Endpoint Detection and Response Expert (en adelante también "EDR Expert"). EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** y **Network Detection and Response (KATA)** Agentes integrados para administrar los componentes Endpoint Detection and Response y Network Detection and Response que forman parte de la solución Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* es una solución diseñada para detener a tiempo amenazas sofisticadas, como ataques dirigidos, amenazas persistentes avanzadas (APT) y ataques de día cero, entre otras. Kaspersky Anti Targeted Attack Platform incluye tres unidades funcionales: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Puede comprar todas las unidades funcionales o unidades funcionales individuales por separado. Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform. **Sandbox** Agente integrado para Sandbox. El componente *Sandbox* detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Sandbox analiza el comportamiento de los objetos para detectar la actividad maliciosa y la actividad característica de los ataques dirigidos a la infraestructura de TI de la organización. Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Sandbox). Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Sandbox y la Ayuda de Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Agente integrado para respaldar el funcionamiento de la solución Kaspersky Managed Detection and Response. La solución *Kaspersky Managed Detection and Response (MDR)* detecta y analiza automáticamente los incidentes de seguridad en su infraestructura. Para hacerlo, MDR utiliza datos de telemetría recibidos de endpoints y aprendizaje automático. MDR envía datos de incidentes a los expertos de Kaspersky. Luego, los expertos pueden procesar el incidente y, por ejemplo, añadir una nueva entrada a las bases de datos antivirus. De manera alternativa, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener información detallada sobre cómo funciona la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Modos de aplicación: Estándar, EDR Agent, Light Agent

Kaspersky Endpoint Security para Windows es parte de las muchas soluciones de Kaspersky. Dependiendo de la solución, debe seleccionar un modo para la aplicación.



Modo estándar

Este es el modo principal y predeterminado de la aplicación. Puede instalar la aplicación en este modo como parte de las soluciones de Kaspersky EPP (Endpoint Protection Platform). Por ejemplo, Kaspersky Endpoint Security en modo Estándar es parte de Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security proporciona una protección completa de estaciones de trabajo y servidores contra diversas amenazas, ataques de red y estafas. En el modo estándar, los agentes integrados también están disponibles para la integración con las soluciones de Kaspersky Detection and Response, incluidos EDR, MDR, KUMA y otros.



EDR Agent

Este modo permite implementar las soluciones de Kaspersky Detection and Response junto con soluciones EPP de terceros. Las soluciones de Detection and Response incluyen Kaspersky Managed Detection and Response (MDR) y Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent también es compatible con la solución Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

En este modo, los componentes de protección estándar, como Protección frente a amenazas en archivos o Protección frente a amenazas web, no están disponibles. La solución EPP de terceros proporciona la protección estándar del equipo. ADR Agent supervisa continuamente los procesos que se ejecutan en estos equipos, las conexiones de red abiertas y los archivos que se modifican, e interactúa con las soluciones de Detection and Response.



Light Agent

Este modo se utiliza para proteger entornos virtuales. Kaspersky Endpoint Security en modo Light Agent es parte de la solución Kaspersky Hybrid Cloud Security. Light Agent protege las máquinas virtuales con sistemas operativos para estaciones de trabajo y servidores. En este modo y en el modo Estándar están disponibles los mismos componentes de protección y control. La diferencia es que los objetos se analizan en busca de virus y otro malware mediante un componente especial de la solución instalado en una máquina virtual separada, SVM (Secure Virtual Machine). Por lo tanto, el Light Agent utiliza los recursos de la SVM para garantizar la seguridad de la infraestructura, en lugar de los recursos de la máquina virtual.

Kit de distribución

El kit de distribución incluye los siguientes paquetes de distribución:

- **AES256**

  Este paquete de distribución está diseñado para instalarse en equipos con arquitectura x86/x64. Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado AES (Advanced Encryption Standard) con una longitud de clave efectiva de 256 bits.

- **AES56**

  Este paquete de distribución está diseñado para instalarse en equipos con arquitectura x86/x64. Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado AES con una longitud de clave efectiva de 56 bits.

- **Arm64**

  Este paquete de distribución está diseñado para su instalación en equipos basados en Arm. Este paquete de distribución no está diseñado para instalarse en servidores.

Antes de la instalación, asegúrese de que el paquete de distribución coincida con la arquitectura de su procesador. Si el paquete de distribución no coincide con la arquitectura del procesador, el instalador finalizará la instalación con un error.

El paquete de distribución es un archivo autoextraíble en formato EXE. Para ver el contenido del paquete de distribución debe extraer el archivo en una carpeta independiente. Cada paquete de distribución contiene los siguientes archivos:

`kes_win.msi`	Paquete de instalación de Kaspersky Endpoint Security.
`setup_kes.exe`	Archivos necesarios para instalar la aplicación mediante cualquiera de los métodos disponibles.
`kes_win.kud`	Archivo para crear paquetes de instalación para Kaspersky Endpoint Security.
`klcfginst.msi`	Paquete de instalación para el complemento de administración de aplicaciones en la Consola de administración de Kaspersky Security Center.
`bases.cab`	Archivos del paquete de actualización que se utilizan durante la instalación.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Archivos para eliminar software no compatible.
`incompatible.txt`	Archivo que contiene la lista de software que puede causar problemas de compatibilidad con Kaspersky Endpoint Security. Kaspersky no garantiza la compatibilidad de Kaspersky Endpoint Security con el software de la lista.
`ksn_<language ID>.txt`	Archivo que detalla las condiciones de participación en Kaspersky Security Network.
`license.txt`	Archivo que detalla el Contrato de Licencia de Usuario Final y la Política de privacidad.
`installer.ini`	Archivo que contiene la configuración interna del kit de distribución.
`kes.cab`	Archivos para la interfaz gráfica de la aplicación.
`aes256.cab` / `aes56.cab`	Archivos para el algoritmo criptográfico de AES (no incluidos en el paquete de distribución de Arm64).
`package.kcat`	Archivo con firmas del kit de distribución de la aplicación. La firma digital garantiza la autenticidad e integridad del kit de distribución de la aplicación.

No se recomienda cambiar los valores de esta configuración. Si desea cambiar las opciones de instalación, utilice el archivo setup.ini.

Requisitos de hardware y software

En este artículo se indican las versiones de software en las que se ha probado la aplicación y con las que se garantiza que funciona correctamente. La aplicación también puede funcionar con otras versiones de software, pero esas configuraciones no se han sometido a un ciclo de pruebas completo y no se incluyen en la lista de versiones con compatibilidad garantizada.

Para garantizar el funcionamiento adecuado de Kaspersky Endpoint Security, el equipo debe cumplir los siguientes requisitos:

Para instalar la aplicación, necesita derechos de administrador en el equipo.

Requisitos generales mínimos

Requisitos mínimos	Estación de trabajo (x86/x64)	Servidor (x86/x64)	Arm
Almacenamiento	2 GB	2 GB	2 GB
CPU	1 GHz, Soporte de instrucciones SSE2	1.4 GHz, Soporte de instrucciones SSE2	1 GHz, arquitectura Armv8.1

Requisitos mínimos	Estación de trabajo (x86/x64)	Servidor (x86/x64)	Arm
RAM	Estación de trabajo (x86): 1 GB Estación de trabajo (x64): 2 GB	2 GB Nota: El servidor requiere 8 GB de memoria para instalar la aplicación con el agente integrado para la integración con Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	4 o posterior	4 o posterior	4.8 o posterior

Estaciones de trabajo

Sistemas operativos admitidos para estaciones de trabajo:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión
- Windows 11 para Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Los sistemas operativos Windows, a partir de la versión 11 24H2, admiten la tecnología UDP Receive Segment Coalescing Offload (URO). La tecnología está activada de forma predeterminada si hay una tarjeta de red compatible y controladores instalados en el equipo. Desactivar URO en el equipo de un usuario puede reducir significativamente el rendimiento de la aplicación.

Para asegurarse de que Kaspersky Endpoint Security funcione correctamente, el servicio Windows Security Center (wscsvc) debe estar ejecutándose en el equipo del usuario.

Kaspersky Endpoint Security no se puede instalar en Microsoft Windows 7 si no se encuentran instaladas las actualizaciones del sistema operativo: KB4490628 (12 de marzo de 2019) y KB4474419 (23 de septiembre de 2019). Para obtener información detallada, consulte la Base de conocimientos de soporte técnico.

Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows 10, visite la Base de conocimientos del Soporte técnico.

Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows 11, visite la Base de conocimientos del Soporte técnico.

Servidores

Kaspersky Endpoint Security admite los componentes principales de la aplicación en equipos con sistema operativo Windows para servidores. Puede utilizar Kaspersky Endpoint Security para Windows en lugar de Kaspersky Security for Windows Server en servidores y clústeres de su organización (Cluster Mode). La aplicación también es compatible con el Server Core Mode (consulte los problemas conocidos).

Sistemas operativos admitidos para servidores:

- Windows Small Business Server 2011 Essentials / Standard (64 bits)

  Microsoft Small Business Server 2011 Standard (64 bits) solo se admite si el Service Pack 1 para Microsoft Windows Server 2008 R2 está instalado.

- Windows MultiPoint Server 2011 (64 bits)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (incluso el modo Server Core)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (incluso el modo Server Core)
- Windows Server 2016 Essentials / Standard / Datacenter (modo Server Core incluido)
- Windows Server 2019 Essentials / Standard / Datacenter (modo Server Core incluido)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (modo Server Core incluido)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security no se puede instalar en Microsoft Windows Server 2008 R2 si no se encuentran instaladas las actualizaciones del sistema operativo: KB4490628 (12 de marzo de 2019) y KB4474419 (23 de septiembre de 2019).

Para más información sobre la compatibilidad con Microsoft Windows Server 2016 y Microsoft Windows Server 2019, visite la Base de conocimientos del Soporte técnico.

Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows Server 2022, visite la Base de conocimientos del Soporte técnico.

Sistemas operativos no compatibles para servidores:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2

- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 R2 Core / Standard / Enterprise / Datacenter Service Pack 2 o versiones posteriores
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Plataformas virtuales

Plataformas virtuales compatibles para el funcionamiento de la aplicación en modo estándar:

- VMware Workstation Pro 15.5.2
- Versión de parche ESXi 7.0b de VMware ESXi 7.0
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

La aplicación admite máquinas virtuales que ejecutan Windows 11 Pro Arm64 creadas con Hyper-V.

Máquinas virtuales para la instalación de Light Agent

No se admite la instalación de Kaspersky Endpoint Security en modo de Light Agent en máquinas virtuales basadas en Arm.

El BIOS de las máquinas virtuales debe admitir la versión 2.1 o posterior de la especificación SMBIOS.

Los siguientes paquetes y utilidades deben estar instalados en las máquinas virtuales:

- Al usar Microsoft Hyper-V: paquete de servicios de integración.
- Al utilizar VMware vSphere: paquete de VMware Tools.
- Al usar el paquete XenServer: XenTools.
- Al usar HUAWEI FusionSphere: paquete HUAWEI Tools.
- Al utilizar hipervisores basados en KVM: QEMU Guest Agent.

Consulte la Ayuda de Kaspersky Security for Virtualization Light Agent para saber cuáles son los requisitos de la infraestructura virtual para ejecutar la aplicación en el modo Light Agent.

Para que la aplicación funcione correctamente, utilice una interfaz de red virtualizada con un ancho de banda de al menos 100 Mbit/s.

Servidores de terminales

Tipos de servidores de terminales admitidos:

- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2008 R2 SP1
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2012
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2012 R2
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2016
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2019
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2022
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2025
- Citrix RDSH de Citrix Virtual Apps and Desktops 7 2507 LTSR

Compatibilidad con Kaspersky Security Center

Kaspersky Endpoint Security funciona con las siguientes versiones de Kaspersky Security Center:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16

- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

Comparación de funciones disponibles en la aplicación según el tipo de sistema operativo

El conjunto de funciones disponibles de Kaspersky Endpoint Security depende del tipo de sistema operativo: estación de trabajo o servidor (consulte la siguiente tabla).

A partir de Kaspersky Endpoint Security 12.8 para Windows, puede configurar diferentes conjuntos de componentes para diferentes tipos de sistemas operativos en el paquete de instalación. Es decir, puede implementar la aplicación en estaciones de trabajo y servidores usando el mismo paquete de instalación.

No se admite la instalación de Kaspersky Endpoint Security en modo de Light Agent en máquinas virtuales basadas en Arm.

Comparación de las funciones de Kaspersky Endpoint Security

Función	Estación de trabajo	Estación de trabajo basada en Arm	Servidor	Modo Server Core
Protección frente a amenazas avanzadas				
Kaspersky Security Network	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	–	–
Motor de reparación	✓	✓	✓	✓
Protección frente a amenazas básicas				
Protección frente a amenazas en archivos	✓	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓	–
Protección frente a amenazas en el correo	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓	–
Protección AMSI	✓	✓	✓	✓
Controles de seguridad				
Inspección de registros	–	–	✓	–
Control de aplicaciones	✓	✓	✓	✓
Control de dispositivos	✓	✓	✓	✓
Control Web	✓	✓	✓	–

Función	Estación de trabajo	Estación de trabajo basada en Arm	Servidor	Modo Server Core
Control de anomalías adaptativo	✓	✓	–	–
Control de integridad del sistema	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Cifrado de datos				
Cifrado de disco de Kaspersky	✓	–	–	–
Cifrado de unidad BitLocker	✓	✓	✓	✓
Cifrado de archivos	✓	–	–	–
Cifrado de unidades extraíbles	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Integración con KUMA	✓	✓	✓	✓

Comparación: disponibilidad de características por herramienta de administración

El conjunto de características disponibles en Kaspersky Endpoint Security depende de la herramienta de administración (consulte la tabla más abajo).

Para administrar la aplicación, se pueden utilizar las siguientes consolas de Kaspersky Security Center:

- Consola de administración. Complemento de Microsoft Management Console (MMC) instalado en la estación de trabajo del administrador.
- Web Console. Componente de Kaspersky Security Center instalado en el Servidor de Administración. Puede trabajar en Web Console mediante un navegador desde cualquier equipo.

La aplicación también puede administrarse a través de Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* es la versión en la nube de Kaspersky Security Center. Esto significa que el Servidor de administración y los demás componentes de Kaspersky Security Center están instalados en la infraestructura de nube de Kaspersky. Para obtener más información sobre cómo administrar la aplicación mediante Kaspersky Security Center Cloud Console, consulte la Guía de ayuda de Kaspersky Security Center Cloud Console.

Kaspersky Endpoint Security es parte de la solución Kaspersky Next Pro View. Para obtener más información sobre las funciones de la aplicación disponibles cuando funciona como parte de esta solución, consulte la Ayuda de Kaspersky Next.

Función	Kaspersky Security Center		Kaspersky Security Center
	Consola de administración	Web Console	Cloud Console
Protección frente a amenazas avanzadas			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Detección de comportamiento	✓	✓	✓
Anti-Cryptor			
Prevención de exploits	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	✓
Motor de reparación	✓	✓	✓
Protección frente a amenazas básicas			
Protección frente a amenazas en archivos	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓
Protección frente a amenazas en el correo	✓	✓	✓
Firewall	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓
Protección AMSI	✓	✓	✓
Controles de seguridad			
Inspección de registros	✓	✓	✓
Control de aplicaciones	✓	✓	✓
Control de dispositivos	✓	✓	✓
Control Web	✓	✓	✓
Control de anomalías adaptativo	✓	✓	✓
Control de integridad del sistema	✓	✓	✓
Cloud Discovery	–	–	✓
Cifrado de datos			
Cifrado de disco de Kaspersky	✓	✓	–
Cifrado de unidad BitLocker	✓	✓	✓
Cifrado de archivos	✓	✓	–
Cifrado de unidades extraíbles	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Integración con KUMA	✓	✓	✓
Tareas			

Función	Kaspersky Security Center		Kaspersky Security Center
	Consola de administración	Web Console	Cloud Console
Añadir clave	✓	✓	✓
Cambiar componentes de la aplicación	✓	✓	✓
Inventario	✓	✓	✓
Actualización	✓	✓	✓
Revertir actualización	✓	✓	✓
Análisis antimalware	✓	✓	✓
Comprobación de integridad de la aplicación	✓	✓	–
Eliminación de datos	✓	✓	✓
Administrar cuentas del Agente de autenticación (Cifrado de disco de Kaspersky)	✓	✓	–
Análisis de IOC (EDR)	–	✓	✓
Mover archivo a Cuarentena (EDR)	–	✓	✓
Obtener archivo (EDR)	–	✓	✓
Eliminar archivo (EDR)	–	✓	✓
Iniciar proceso (EDR)	–	✓	✓
Terminar proceso (EDR)	–	✓	✓

Compatibilidad con otras aplicaciones

Kaspersky Endpoint Security es incompatible con algunas aplicaciones de Kaspersky y con algunas aplicaciones de terceros. Por lo tanto, antes de la instalación, de actualizar la versión de la aplicación y de cambiar los componentes de la aplicación, Kaspersky Endpoint Security analiza el equipo para ver si hay aplicaciones de este tipo.

Compatibilidad con aplicaciones de terceros

Kaspersky Endpoint Security es incompatible con aplicaciones que forman parte de sistemas de protección de endpoint de terceros (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security también puede experimentar problemas de compatibilidad con otras aplicaciones. Para determinar la compatibilidad, Kaspersky Endpoint Security consulta una lista de software preparada por Kaspersky. Esta lista está contenida en el archivo incompatible.txt. El archivo se incluye en el kit de distribución.

Kaspersky no garantiza la compatibilidad de Kaspersky Endpoint Security con el software de la lista. Si se detecta una aplicación de la lista, el instalador detiene la implementación de Kaspersky Endpoint Security. El instalador puede eliminar automáticamente algunas aplicaciones de la lista. Si desea ignorar los riesgos e instalar Kaspersky Endpoint Security y un software de la lista en el mismo equipo, puede omitir la verificación del equipo (consulte las instrucciones a continuación).

DESCARGAR EL ARCHIVO INCOMPATIBLE.TXT

Compatibilidad con aplicaciones de Kaspersky

Kaspersky Endpoint Security es incompatible con las siguientes aplicaciones de Kaspersky:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Endpoint Sensor como parte de las soluciones Kaspersky Anti Targeted Attack Platform y Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent como parte de las soluciones de Detection and Response de Kaspersky.

  Kaspersky está cambiando todo Detection and Response para que funcione con el agente integrado de Kaspersky Endpoint Security en lugar de Kaspersky Endpoint Agent. A partir de la versión 12.1, la aplicación admite todas las soluciones de Detection and Response.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention para Endpoint.
- Kaspersky Security for Windows Server

  A partir de Kaspersky Endpoint Security 12.0, puede migrar de Kaspersky Security for Windows Server a Kaspersky Endpoint Security para Windows y usar la misma solución para proteger estaciones de trabajo y servidores.

- Kaspersky Embedded Systems Security.

Si las aplicaciones de Kaspersky de esta lista están instaladas en el equipo, Kaspersky Endpoint Security elimina estas aplicaciones. Espere que se complete este proceso antes de continuar con la instalación de Kaspersky Endpoint Security.

Omitir la verificación de software que pueda causar problemas de compatibilidad

Si Kaspersky Endpoint Security detecta software de la lista de incompatible.txt, la instalación de la aplicación finalizará. Para continuar con la instalación, debe eliminar esa aplicación. Sin embargo, si el proveedor del software de terceros ha indicado en su documentación que su software es compatible con Endpoint Protection Platform (EPP), puede instalar Kaspersky Endpoint Security en un equipo que contenga una aplicación de este proveedor. Por ejemplo, el proveedor de la solución Endpoint Detection and Response (EDR) puede declarar su compatibilidad con sistemas EPP de terceros. Si este es el caso, debe iniciar la instalación de Kaspersky Endpoint Security sin ejecutar una comprobación de software instalado. Para hacerlo, transmita los siguientes parámetros al instalador:

- `SKIPPRODUCTCHECK=1` Desactivación de la comprobación de software instalado. La lista de software que puede causar problemas de incompatibilidad está disponible en el archivo incompatible.txt que se incluye en el kit de distribución. Si no se establece ningún valor para este parámetro y se detecta software de la lista, la instalación de Kaspersky Endpoint Security finalizará.

- `SKIPPRODUCTUNINSTALL=1` Desactivación de la eliminación automática del software detectado de la lista de incompatible.txt. Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security intentará eliminar el software que puede causar problemas de incompatibilidad.

- `CLEANERSIGNCHECK=0` Desactivación de la verificación de firma digital de las aplicaciones encontradas en la comprobación. Si no se establece este parámetro, la verificación de firmas digitales se deshabilita al desplegar la aplicación a través de Kaspersky Security Center. Cuando la aplicación se instala localmente, la verificación de firma digital está activada de forma predeterminada.

Puede transmitir los parámetros en la línea de comandos al instalar localmente la aplicación.

Si durante el proceso de instalación omitió el análisis para buscar software que pueda causar problemas de compatibilidad, Kaspersky Endpoint Security puede volver a realizar esta verificación cuando los componentes de la aplicación cambien. Para omitir el análisis del software instalado, debe configurar la tarea *Cambiar componentes de la aplicación*.

Ejemplo:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Para instalar de forma remota Kaspersky Endpoint Security, debe añadir los parámetros adecuados al archivo de generación del paquete de instalación, llamado `kes_win.kud`, en `[Setup]` (consulte la información a continuación). El archivo `kes_win.kud` se incluye en el kit de distribución.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Instalación y eliminación de la aplicación

Kaspersky Endpoint Security se puede instalar en el equipo de varias maneras:

- de forma local, utilizando el Asistente de instalación;
- de forma local, utilizando la línea de comando;
- de forma remota utilizando Kaspersky Security Center.
- de forma remota, utilizando el Editor de administración de directivas de grupo de Microsoft Windows (para más información, visite el sitio web de soporte técnico de Microsoft).
- de forma remota, utilizando System Center Configuration Manager.

Los parámetros de instalación del programa también pueden configurarse de más de una manera. Cuando se emplea más de un método, Kaspersky Endpoint Security utiliza los valores de configuración de mayor prioridad. El orden de prioridad es el siguiente:

1. los ajustes recibidos del archivo setup.ini,
2. los ajustes recibidos del archivo installer.ini,
3. los ajustes recibidos de la línea de comando.
4. Configuración recibida del archivo de configuración (install.cfg).

Le recomendamos que cierre todas las aplicaciones activas antes de comenzar la instalación de Kaspersky Endpoint Security (incluida la instalación remota).

Al instalar Kaspersky Endpoint Security, el sistema operativo puede mostrar sus propios mensajes. Las conexiones de red e Internet también pueden interrumpirse cuando se instala la aplicación.

Al instalar, actualizar o desinstalar Kaspersky Endpoint Security, pueden producirse errores. Para obtener más información sobre cómo solucionar estos errores, consulte la Base de conocimientos de soporte técnico.

Despliegue a través de Kaspersky Security Center

Kaspersky Endpoint Security puede desplegarse de varias maneras en los equipos de una red corporativa. Puede elegir el escenario de despliegue más adecuado para su organización o combinar varios escenarios de despliegue al mismo tiempo. Antes de instalar la aplicación, debe asegurarse de que Kaspersky Security Center Network Agent esté instalado en el equipo. El *Agente de red* facilita la interacción entre el Servidor de administración y un equipo cliente.

Kaspersky Security Center admite los siguientes métodos de despliegue principales:

- Instalación de la aplicación mediante el Asistente de despliegue de la protección.

  El método de instalación estándar es conveniente si está satisfecho con la configuración predeterminada de Kaspersky Endpoint Security y su organización tiene una infraestructura simple que no requiere configuraciones especiales.

- Instalación de la aplicación mediante la tarea de instalación remota.

  El método de instalación universal, que permite configurar los ajustes de Kaspersky Endpoint Security y administrar de manera flexible las tareas de instalación remota. La instalación de Kaspersky Endpoint Security consta de los siguientes pasos:

  1. Creación de un paquete de instalación.
  2. Creación de una tarea de instalación remota.

Kaspersky Security Center también admite otros métodos de instalación de Kaspersky Endpoint Security, como el despliegue dentro de una imagen del sistema operativo. Para obtener más información sobre otros métodos de despliegue, consulte la Ayuda de Kaspersky Security Center.

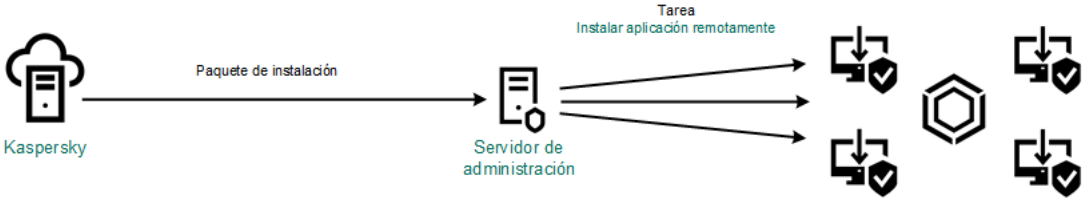
Instalación estándar de la aplicación

Kaspersky Security Center proporciona un Asistente de despliegue de protección para instalar la aplicación en equipos corporativos. El Asistente de despliegue de protección incluye las siguientes acciones principales:

1. Selección del paquete de instalación de Kaspersky Endpoint Security.

   Un *paquete de instalación* es un conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky mediante Kaspersky Security Center. El paquete de instalación contiene una serie de ajustes necesarios para instalar la aplicación y ejecutarla inmediatamente después de la instalación. El paquete de instalación se crea utilizando los archivos con extensiones .kpd y .kud incluidas en el kit de distribución de la aplicación. El paquete de instalación de Kaspersky Endpoint Security es uno solo para todas las versiones de Windows y los tipos de arquitectura de procesador compatibles.

2. Creación de la tarea *Instalar aplicación en remoto* del Servidor de administración de Kaspersky Security Center.



Despliegue de Kaspersky Endpoint Security

Cómo ejecutar el Asistente de despliegue de protección en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Avanzado** → **Instalación remota**.
3. Haga clic en el enlace **Desplegar paquete de instalación en los dispositivos administrados (estaciones de trabajo)**.

Esto iniciará el Asistente de despliegue de la protección. Siga las instrucciones del Asistente.

Los puertos TCP 139 y 445, y los puertos UDP 137 y 138 deben abrirse en el equipo cliente.

Paso 1. Seleccionar un paquete de instalación.

Seleccione en la lista el paquete de instalación de Kaspersky Endpoint Security. Si la lista no contiene el paquete de instalación de Kaspersky Endpoint Security, puede crear el paquete en el Asistente.

Puede configurar los ajustes del paquete de instalación en Kaspersky Security Center. Por ejemplo, puede seleccionar qué componentes de la aplicación se instalarán en un equipo.

El Agente de red también se instalará junto con Kaspersky Endpoint Security. El *Agente de red* facilita la interacción entre el Servidor de administración y un equipo cliente. Si el Agente de red ya está instalado en el equipo, no se volverá a instalar.

Paso 2. Seleccionar el origen del paquete de instalación

Seleccione el origen **Desplegar el paquete de Kaspersky Security Center**.

Paso 3. Selección de dispositivos para realizar la instalación

Seleccione en qué equipos se instalará Kaspersky Endpoint Security. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. El Agente de red no está instalado en los dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Definir la configuración de la tarea de instalación remota

Haga los cambios adicionales que necesite en la configuración de la aplicación:

- **Forzar la descarga del paquete de instalación**. Seleccionar el método para instalar la aplicación:
  - **Usando el Agente de red**. El Agente de red es responsable de entregar el paquete de instalación de Kaspersky Endpoint Security a los equipos cliente. Si el Agente de red no está instalado, la tarea finaliza con un error. En este caso, añada el paquete de instalación del Agente de red a la tarea *Instalar aplicación en remoto* y habilite la entrega de archivos mediante recursos del sistema operativo. A continuación, el Agente de red se instalará utilizando recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.
  - **Usando los recursos del sistema operativo mediante puntos de distribución**. El paquete de instalación se entrega a los equipos cliente mediante recursos del sistema operativo a través de puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center.
  - **Usando los recursos del sistema operativo mediante el Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante los recursos del sistema operativo a través del Servidor de Administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.
- **Comportamiento para dispositivos administrados a través de otros Servidores de administración**. Seleccione el método de instalación de Kaspersky Endpoint Security. Si la red tiene más de un Servidor de administración instalado, estos Servidores de administración pueden ver los mismos equipos cliente. Esto puede causar, por ejemplo, que una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes servidores de administración, o puede generar otros conflictos.
- **No reinstalar la aplicación si ya se encuentra instalada**. Desactive esta casilla de verificación si, por ejemplo, desea instalar una versión anterior de la aplicación.
- **Asignar instalación del Agente de red en las directivas de grupo de Active Directory**. Instalación manual del Agente de red con recursos de Active Directory. Para instalar el Agente de red, la tarea de instalación remota debe ejecutarse con privilegios de administrador de dominio.

Paso 5. Selección de una clave de licencia

Añada una clave al paquete de instalación para activar la aplicación. Este paso es opcional. Si el Servidor de administración contiene una clave de licencia que puede distribuirse automáticamente, se la añadirá más adelante sin que usted intervenga. También puede activar la aplicación más adelante mediante la tarea *Añadir clave*.

Paso 6. Selección de la configuración de reinicio del sistema operativo

Seleccione qué acción se realizará si se requiere reiniciar el equipo. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.

Paso 7. Eliminación de aplicaciones incompatibles antes de instalar la aplicación

Lea atentamente la lista de aplicaciones incompatibles y permita la eliminación de estas aplicaciones. Si hay aplicaciones incompatibles instaladas en el equipo, la instalación de Kaspersky Endpoint Security terminará con un error.

Paso 8. Selección de una cuenta para acceder a los dispositivos

Seleccione la cuenta para instalar el Agente de red mediante las herramientas del sistema operativo. En este caso, se necesitan derechos de administrador para acceder al equipo. Puede añadir varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación utiliza la siguiente cuenta. Si instala Kaspersky Endpoint Security mediante las herramientas del Agente de red, no tiene que seleccionar una cuenta.

Paso 9. Inicio de la instalación

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo iniciar el Asistente de despliegue de la protección en Web Console y Cloud Console

En la ventana principal de Web Console, seleccione **Detección y despliegue** → **Despliegue y asignación** → **Asistente de despliegue de la protección**.

Esto iniciará el Asistente de despliegue de la protección. Siga las instrucciones del Asistente.

Los puertos TCP 139 y 445, y los puertos UDP 137 y 138 deben abrirse en el equipo cliente.

Paso 1. Seleccionar un paquete de instalación.

Seleccione en la lista el paquete de instalación de Kaspersky Endpoint Security. Si la lista no contiene el paquete de instalación de Kaspersky Endpoint Security, puede crear el paquete en el Asistente. Para crear el paquete de instalación, no es necesario buscar el paquete de distribución correspondiente y guardarlo en el equipo. En Kaspersky Security Center, puede ver la lista de paquetes de distribución que residen en los servidores de Kaspersky. El paquete de instalación se crea automáticamente. Kaspersky actualiza la lista después del lanzamiento de nuevas versiones de las aplicaciones.

Puede configurar los ajustes del paquete de instalación en Kaspersky Security Center. Por ejemplo, puede seleccionar qué componentes de la aplicación se instalarán en un equipo.

Paso 2. Selección de una clave de licencia

Añada una clave al paquete de instalación para activar la aplicación. Este paso es opcional. Si el Servidor de administración contiene una clave de licencia que puede distribuirse automáticamente, se la añadirá más adelante sin que usted intervenga. También puede activar la aplicación más adelante mediante la tarea *Añadir clave*.

Paso 3. Selección de un agente de red

Seleccione la versión del Agente de red que se instalará junto con Kaspersky Endpoint Security. El *Agente de red* facilita la interacción entre el Servidor de administración y un equipo cliente. Si el Agente de red ya está instalado en el equipo, no se volverá a instalar.

Paso 4. Selección de dispositivos para realizar la instalación

Seleccione en qué equipos se instalará Kaspersky Endpoint Security. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. El Agente de red no está instalado en los dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 5. Configuración de los parámetros avanzados

Haga los cambios adicionales que necesite en la configuración de la aplicación:

- **Forzar la descarga del paquete de instalación**. Seleccionar el método para instalar la aplicación:
  - **Usando el Agente de red**. El Agente de red es responsable de entregar el paquete de instalación de Kaspersky Endpoint Security a los equipos cliente. Si el Agente de red no está instalado, la tarea finaliza con un error. En este caso, añada el paquete de instalación del Agente de red a la tarea *Instalar aplicación en remoto* y habilite la entrega de archivos mediante recursos del sistema operativo. A continuación, el Agente de red se instalará utilizando recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.
  - **Usando los recursos del sistema operativo mediante puntos de distribución**. El paquete de instalación se entrega a los equipos cliente mediante recursos del sistema operativo a través de puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center.
  - **Usando los recursos del sistema operativo mediante el Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante los recursos del sistema operativo a través del Servidor de Administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.
- **No reinstalar la aplicación si ya se encuentra instalada**. Desactive esta casilla de verificación si, por ejemplo, desea instalar una versión anterior de la aplicación.
- **Asignar instalación del paquete en las directivas de grupo de Active Directory**. Kaspersky Endpoint Security se instala mediante el Agente de red o manualmente mediante Active Directory. Para instalar el Agente de red, la tarea de instalación remota debe ejecutarse con privilegios de administrador de dominio.

Paso 6. Selección de la configuración de reinicio del sistema operativo

Seleccione qué acción se realizará si se requiere reiniciar el equipo. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.

Paso 7. Eliminación de aplicaciones incompatibles antes de instalar la aplicación

Lea atentamente la lista de aplicaciones incompatibles y permita la eliminación de estas aplicaciones. Si hay aplicaciones incompatibles instaladas en el equipo, la instalación de Kaspersky Endpoint Security terminará con un error.

Paso 8. Asignación a un grupo de administración

Seleccione el grupo de administración al que se moverán los equipos después de instalar el Agente de red. Los equipos deben moverse a un grupo de administración para poder aplicar directivas y tareas de grupo. Si un equipo ya está en un grupo de administración, no se moverá. Si no selecciona un grupo de administración, los equipos se añadirán al grupo **Dispositivos no asignados**.

Paso 9. Selección de una cuenta para acceder a los dispositivos

Seleccione la cuenta para instalar el Agente de red mediante las herramientas del sistema operativo. En este caso, se necesitan derechos de administrador para acceder al equipo. Puede añadir varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación utiliza la siguiente cuenta. Si instala Kaspersky Endpoint Security mediante las herramientas del Agente de red, no tiene que seleccionar una cuenta.

Paso 10. Inicio de la instalación

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Creación de un paquete de instalación

Un *paquete de instalación* es un conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky mediante Kaspersky Security Center. El paquete de instalación contiene una serie de ajustes necesarios para instalar la aplicación y ejecutarla inmediatamente después de la instalación. El paquete de instalación se crea utilizando los archivos con extensiones .kpd y .kud incluidas en el kit de distribución de la aplicación. El paquete de instalación de Kaspersky Endpoint Security es uno solo para todas las versiones de Windows y los tipos de arquitectura de procesador compatibles.

Cómo crear un paquete de instalación en la Consola de administración (MMC)

1. En la Consola de administración, vaya a la carpeta **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación**.

   Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.

2. Haga clic en **Crear paquete de instalación**.

Se abre el Asistente de nuevo paquete. Siga las instrucciones del Asistente.

Paso 1. Seleccionar el tipo de paquete de instalación

Seleccione la opción **Crear un paquete de instalación para una aplicación de Kaspersky**.

Paso 2. Definir el nombre del paquete de instalación

Introduzca el nombre del paquete de instalación, por ejemplo, *Kaspersky Endpoint Security para Windows 14.2*.

Paso 3. Seleccionar el paquete de distribución para la instalación

Haga clic en el botón **Examinar** y seleccione el archivo `kes_win.kud` que se incluye en el kit de distribución.

Si es necesario, actualice las bases de datos antivirus en el paquete de instalación utilizando la casilla de verificación **Copiar actualizaciones del repositorio al paquete de instalación**.

Paso 4. Contrato de licencia de usuario final y Política de privacidad

Lea y acepte las condiciones del Contrato de licencia de usuario final y la Política de privacidad.

El paquete de instalación se creará y se añadirá a Kaspersky Security Center. Mediante el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación.

En la configuración del paquete de instalación, puede seleccionar componentes de la aplicación para diferentes tipos de sistema operativo. Es decir, el paquete de instalación incluye dos conjuntos de componentes: para estaciones de trabajo y para servidores. Antes de implementar el paquete de instalación, el instalador detecta el tipo de sistema operativo e instala solo los componentes de la aplicación que ha seleccionado para dicho tipo. De esta forma, puede utilizar el mismo paquete de instalación para estaciones de trabajo y servidores.

El paquete de instalación contiene bases de datos antivirus del repositorio del Servidor de administración. Puede actualizar las bases de datos en el paquete de instalación para reducir el consumo de tráfico al actualizar las bases de datos después de instalar Kaspersky Endpoint Security.

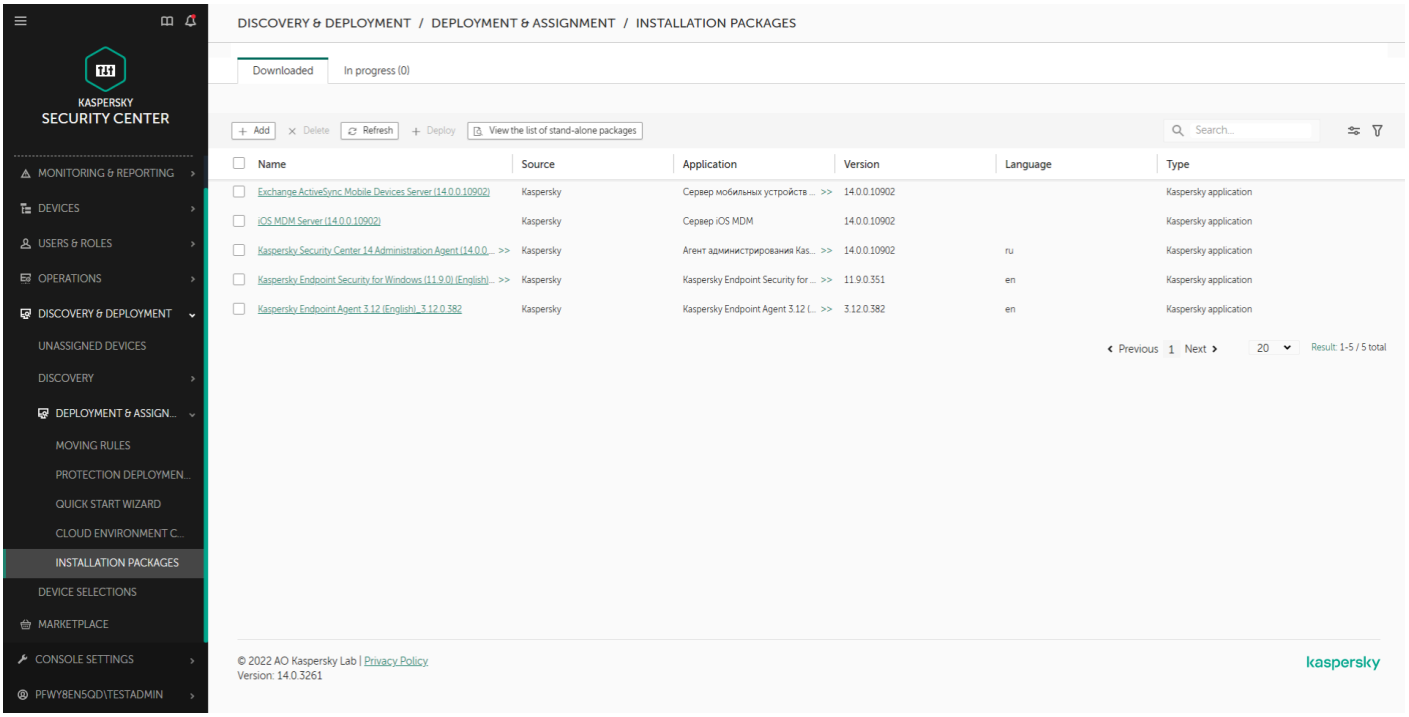
Cómo crear un paquete de instalación en la Consola web

1. En la ventana principal de Web Console, seleccione **Detección y despliegue → Despliegue y asignación → Paquetes de instalación**.

   Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.

2. Haga clic en **Añadir**.

Se abre el Asistente de nuevo paquete. Siga las instrucciones del Asistente.



Lista de paquetes de instalación

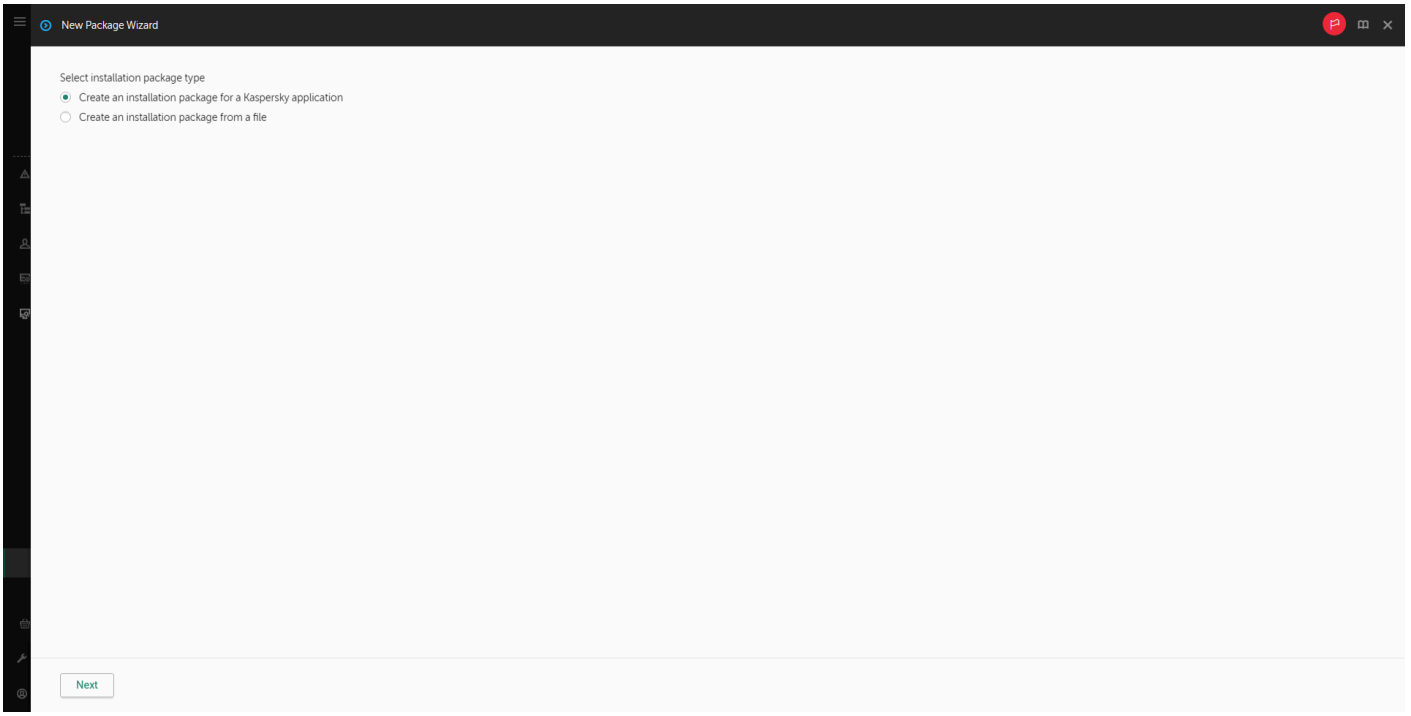
Paso 1. Seleccionar el tipo de paquete de instalación

Seleccione la opción **Crear un paquete de instalación para una aplicación de Kaspersky**.

El asistente creará un paquete de instalación a partir del paquete de distribución alojado en los servidores de Kaspersky. La lista se actualiza automáticamente a medida que se publican nuevas versiones de las aplicaciones. Para instalar Kaspersky Endpoint Security, recomendamos utilizar esta opción.

También es posible crear un paquete de instalación a partir de un archivo.

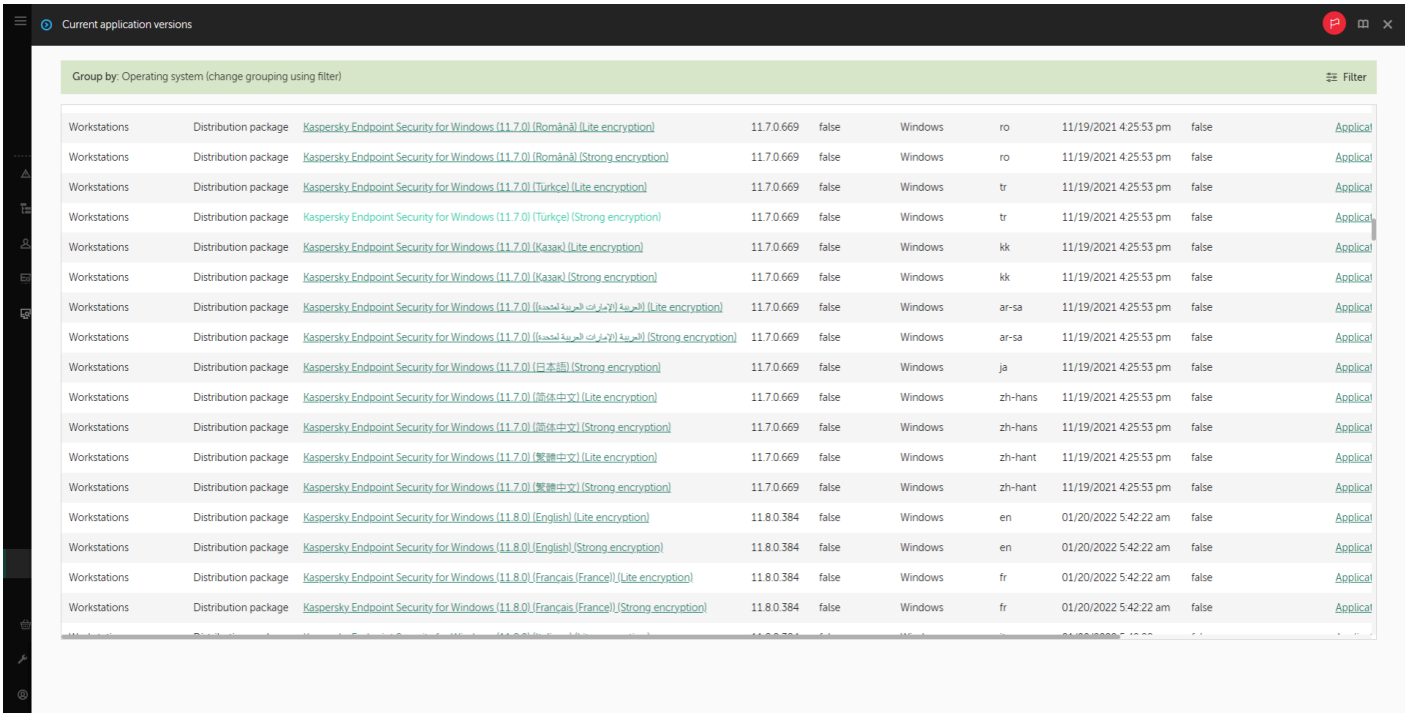
La posibilidad de crear un paquete de instalación para Kaspersky Endpoint Security a partir de un archivo solo está disponible en Kaspersky Security Center Web Console.



Tipos de paquetes de instalación

Paso 2. Paquetes de instalación

Seleccione el paquete de instalación de Kaspersky Endpoint Security para Windows. Se inicia el proceso de creación del paquete de instalación. Como parte del proceso, deberá aceptar los términos del Contrato de licencia de usuario final y la Política de privacidad.

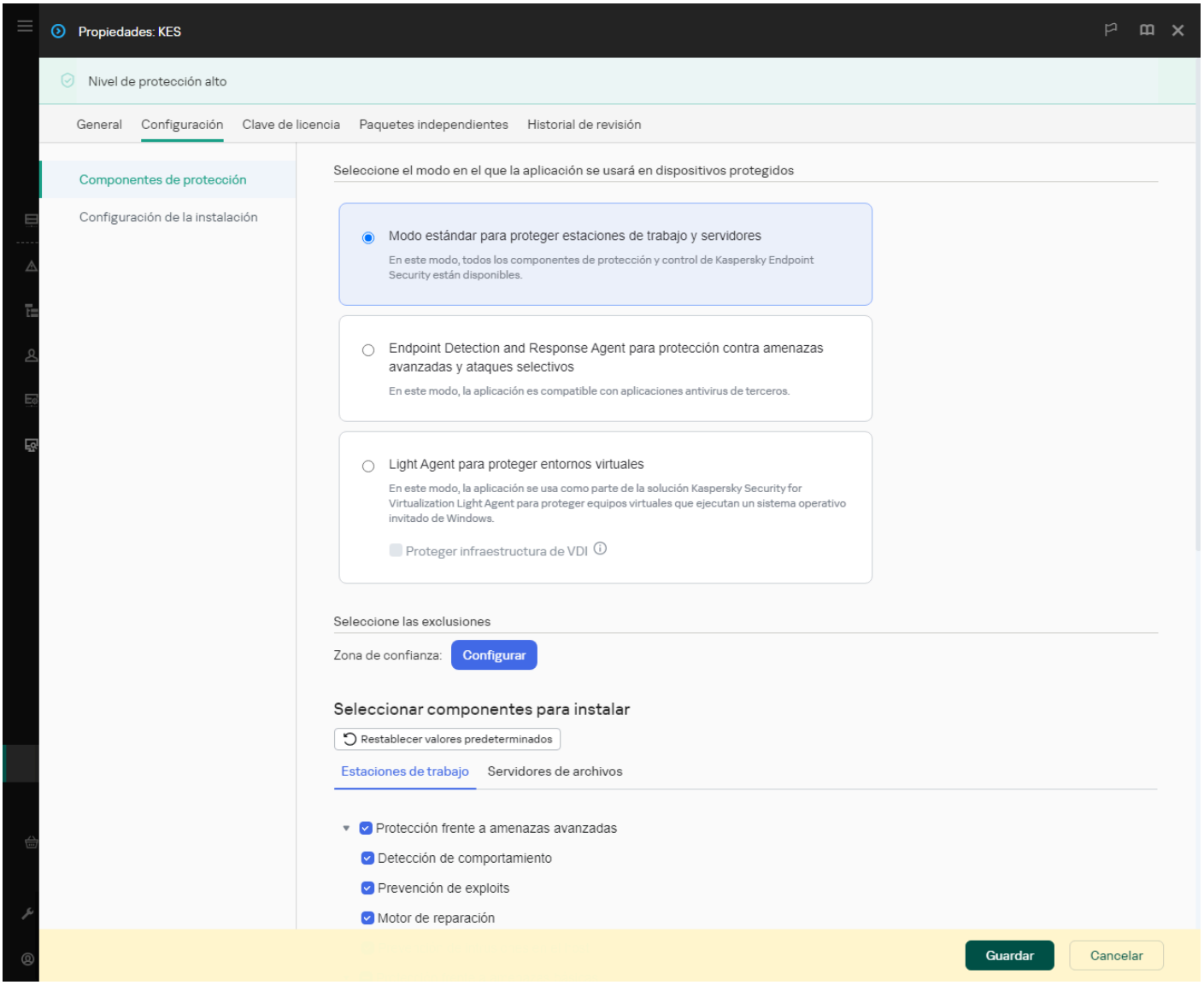


Lista de paquetes de instalación en servidores de Kaspersky

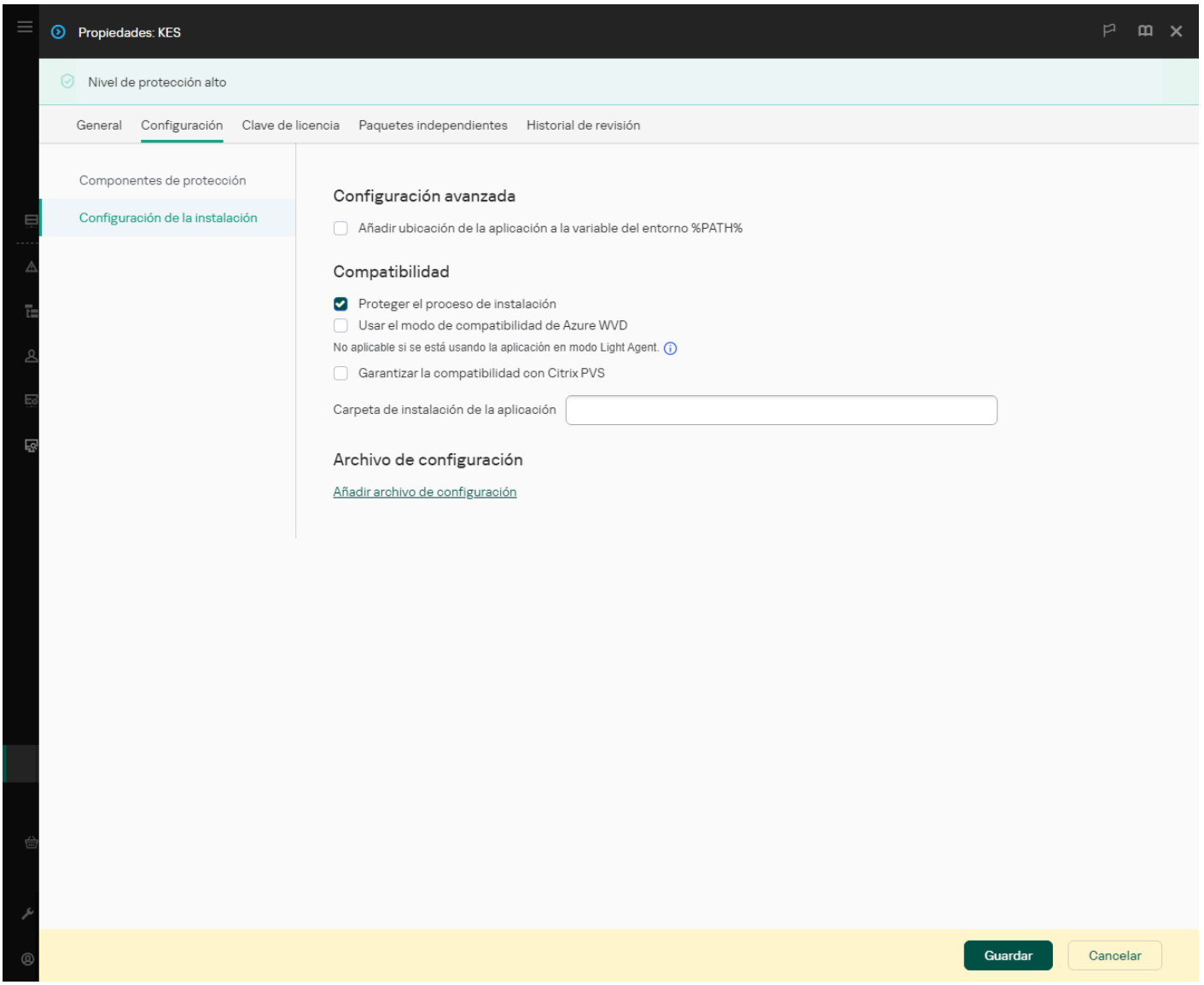
El paquete de instalación se creará y se añadirá a Kaspersky Security Center. Mediante el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación.

En la configuración del paquete de instalación, puede seleccionar componentes de la aplicación para diferentes tipos de sistema operativo. Es decir, el paquete de instalación incluye dos conjuntos de componentes: para estaciones de trabajo y para servidores. Antes de implementar el paquete de instalación, el instalador detecta el tipo de sistema operativo e instala solo los componentes de la aplicación que ha seleccionado para dicho tipo. De esta forma, puede utilizar el mismo paquete de instalación para estaciones de trabajo y servidores.

El paquete de instalación contiene bases de datos antivirus del repositorio del Servidor de administración. Puede actualizar las bases de datos en el paquete de instalación para reducir el consumo de tráfico al actualizar las bases de datos después de instalar Kaspersky Endpoint Security.



Componentes incluidos en el paquete de instalación



Configuración de instalación del paquete de instalación

Ajustes del paquete de instalación

Sección	Descripción
Componentes de protección	**Modo estándar**. Es la configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para soluciones de Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra varias amenazas, ataques de red y fraudes. **Endpoint Detection and Response Agent**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros. **Light Agent para proteger entornos virtuales**. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Sección	Descripción
Exclusiones	A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. A partir de Kaspersky Endpoint Security 12.8 para Windows, puede instalar la aplicación en modo Light Agent para proteger los entornos virtuales. Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware. También puede configurar la zona de confianza más adelante en las propiedades de la directiva: exclusiones de análisis y aplicaciones de confianza.
Seleccionar componentes para instalar	En esta sección, puede seleccionar qué componentes de la aplicación estarán disponibles. Puede cambiar el conjunto de componentes de la apliación posteriormente a través de la tarea *Cambiar componentes de la aplicación*. Puede crear conjuntos de componentes independientes para estaciones de trabajo y servidores. Antes de implementar el paquete de instalación, el instalador detecta el tipo de sistema operativo e instala solo los componentes de la aplicación que ha seleccionado para dicho tipo. De esta forma, puede utilizar el mismo paquete de instalación para estaciones de trabajo y servidores. El conjunto de componentes disponibles depende de la configuración de la aplicación: **Modo estándar** Kaspersky Data Encryption, Cifrado de archivos y todos los agentes integrados, excepto EDR Optimum, no se instalan de forma predeterminada. Estos componentes se pueden añadir en la configuración del paquete de instalación. **Endpoint Detection and Response Agent** En esta configuración, solo están disponibles los agentes integrados para las soluciones de Kaspersky Detection and Response. **Light Agent para proteger entornos virtuales** En esta configuración, puede utilizar casi todos los componentes de la aplicación que están disponibles en la configuración **Modo estándar**, excepto los componentes de cifrado de datos y el Control de anomalías adaptativo.
Clave de licencia	En esta sección, puede activar la aplicación. Para activar la aplicación, debe seleccionar una clave de licencia. Antes de hacerlo, debe añadir la clave al Servidor de administración. Para obtener más información sobre cómo añadir una clave al Servidor de administración de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.
Aplicaciones incompatibles	Lea atentamente la lista de aplicaciones incompatibles y permita la eliminación de estas aplicaciones. Si hay aplicaciones incompatibles instaladas en el equipo, la instalación de Kaspersky Endpoint Security terminará con un error.
Configuración de la instalación	**Añada la ruta del archivo avp.com a la variable de entorno %PATH%**. Puede añadir la ruta de instalación a la variable %PATH% para un uso conveniente de la interfaz de línea de comandos. **Proteger el proceso de instalación**. La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Windows Remote Desktop), se aconseja que desactive la protección del proceso de instalación. **Garantizar la compatibilidad con Citrix PVS**. Puede habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual. **Usar el modo de compatibilidad de Azure WVD**. Esta función garantiza que el estado de las máquinas virtuales de Azure se muestre correctamente en la consola de Kaspersky Anti Targeted Attack Platform. Para supervisar el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar un Sensor ID único y permanente a estas máquinas virtuales. Si el modo de compatibilidad se desactiva, el Sensor ID puede cambiar después de reiniciar el equipo debido al funcionamiento de las máquinas virtuales de Azure. Esto puede hacer que aparezcan duplicados de máquinas virtuales en la consola. **Carpeta de instalación de la aplicación**. Puede cambiar la ruta de instalación de Kaspersky Endpoint Security en un equipo cliente. De manera predeterminada, la aplicación se instala en la carpeta `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`. **Archivo de configuración**. Instalación de la aplicación con configuraciones predefinidas. Para hacerlo, debe subir un archivo que defina la configuración de Kaspersky Endpoint Security. Puede crear un archivo de configuración en la interfaz local de la aplicación. El asistente para crear un paquete nuevo no admite archivos de configuración cifrados. Al exportar el archivo de configuración, omita el paso de cifrado del archivo.

Actualización de bases de datos en el paquete de instalación

El paquete de instalación contiene bases de datos antivirus del repositorio del Servidor de administración que están actualizadas cuando se crea el paquete de instalación. Después de crear el paquete de instalación, puede actualizar las bases de datos antivirus en el paquete de instalación. Así puede reducir el consumo de tráfico al actualizar las bases de datos antivirus después de instalar Kaspersky Endpoint Security.

Para actualizar las bases de datos antivirus en el repositorio del Servidor de administración, utilice la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* del Servidor de administración. Para obtener más información sobre la actualización de las bases de datos antivirus en el repositorio del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

Puede actualizar las bases de datos en el paquete de instalación solo en la Consola de administración y en Kaspersky Security Center Web Console. No se pueden actualizar las bases de datos en el paquete de instalación en Kaspersky Security Center Cloud Console.

Cómo actualizar las bases de datos antivirus en el paquete de instalación mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione la carpeta **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

   Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.
3. Abra las propiedades del paquete de instalación.
4. En la sección **General**, haga clic en **Actualizar bases de datos**.

Como resultado, las bases de datos antivirus en el paquete de instalación se actualizarán desde el repositorio del Servidor de administración. El archivo `bases.cab` que se incluye en el kit de distribución será reemplazado por la carpeta `bases`. Los archivos del paquete de actualización estarán dentro de la carpeta.

Cómo actualizar las bases de datos antivirus en un paquete de instalación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

   Esto abre una lista de paquetes de instalación descargados en Web Console.
2. Haga clic en el nombre del paquete de instalación de Kaspersky Endpoint Security en el que desea actualizar las bases de datos antivirus.

   Se abre la ventana de propiedades del paquete de instalación.
3. En la pestaña **Información general**, haga clic en el enlace **Actualizar bases de datos**.

Como resultado, las bases de datos antivirus en el paquete de instalación se actualizarán desde el repositorio del Servidor de administración. El archivo `bases.cab` que se incluye en el kit de distribución será reemplazado por la carpeta `bases`. Los archivos del paquete de actualización estarán dentro de la carpeta.

Creación de una tarea de instalación remota

La tarea *Instalar aplicación en remoto* está diseñada para la instalación remota de Kaspersky Endpoint Security. La tarea *Instalar aplicación en remoto* le permite desplegar el paquete de instalación de la aplicación en todos los equipos de la organización. Antes de desplegar el paquete de instalación, puede actualizar las bases de datos antivirus dentro del paquete de instalación y seleccionar los componentes de la aplicación disponibles en las propiedades del paquete de instalación.

Cómo crear una tarea de instalación remota en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.

   Se abre la lista de tareas.
3. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Servidor de administración de Kaspersky Security Center → Instalar aplicación en remoto**.

Paso 2. Seleccionar un paquete de instalación.

Seleccione en la lista el paquete de instalación de Kaspersky Endpoint Security. Si la lista no contiene el paquete de instalación de Kaspersky Endpoint Security, puede crear el paquete en el Asistente.

Puede configurar los ajustes del paquete de instalación en Kaspersky Security Center. Por ejemplo, puede seleccionar qué componentes de la aplicación se instalarán en un equipo.

El Agente de red también se instalará junto con Kaspersky Endpoint Security. El *Agente de red* facilita la interacción entre el Servidor de administración y un equipo cliente. Si el Agente de red ya está instalado en el equipo, no se volverá a instalar.

Paso 3. Adicional

Seleccione el paquete de instalación del Agente de red. Cuando se instale Kaspersky Endpoint Security, se instalará también la versión seleccionada del Agente de red.

Paso 4. Configuración

Haga los cambios adicionales que necesite en la configuración de la aplicación:

- **Forzar la descarga del paquete de instalación**. Seleccionar el método para instalar la aplicación:

  - **Usando el Agente de red**. El Agente de red es responsable de entregar el paquete de instalación de Kaspersky Endpoint Security a los equipos cliente. Si el Agente de red no está instalado, la tarea finaliza con un error. En este caso, añada el paquete de instalación del Agente de red a la tarea *Instalar aplicación en remoto* y habilite la entrega de archivos mediante recursos del sistema operativo. A continuación, el Agente de red se instalará utilizando recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.

  - **Usando los recursos del sistema operativo mediante puntos de distribución**. El paquete de instalación se entrega a los equipos cliente mediante recursos del sistema operativo a través de puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

  - **Usando los recursos del sistema operativo mediante el Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante los recursos del sistema operativo a través del Servidor de Administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.

- **Comportamiento para dispositivos administrados a través de otros Servidores de administración**. Seleccione el método de instalación de Kaspersky Endpoint Security. Si la red tiene más de un Servidor de administración instalado, estos Servidores de administración pueden ver los mismos equipos cliente. Esto puede causar, por ejemplo, que una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes servidores de administración, o puede generar otros conflictos.

- **No reinstalar la aplicación si ya se encuentra instalada**. Desactive esta casilla de verificación si, por ejemplo, desea instalar una versión anterior de la aplicación.

Paso 5. Selección de la configuración de reinicio del sistema operativo

Seleccione qué acción se realizará si se requiere reiniciar el equipo. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.

Paso 6. Selección de los dispositivos a los que se asignará la tarea

Seleccione en qué equipos se instalará Kaspersky Endpoint Security. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. El Agente de red no está instalado en los dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 7. Selección de la cuenta para ejecutar la tarea

Seleccione la cuenta para instalar el Agente de red mediante las herramientas del sistema operativo. En este caso, se necesitan derechos de administrador para acceder al equipo. Puede añadir varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación utiliza la siguiente cuenta. Si instala Kaspersky Endpoint Security mediante las herramientas del Agente de red, no tiene que seleccionar una cuenta.

Paso 8. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando el equipo está inactivo.

Paso 9. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Desinstalar Kaspersky Endpoint Security para Windows 14.2*.

Paso 10. Finalización de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. La aplicación se instalará en modo silencioso. Después de la instalación, el icono aparecerá en al área de notificación del equipo del usuario. Si el icono que aparece es , compruebe si la aplicación está activada.

Cómo crear una tarea de instalación remota en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Instalar aplicación en remoto**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Instalación de Kaspersky Endpoint Security para administradores*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

Paso 2. Selección de equipos para realizar la instalación

En este paso, seleccione los equipos en los que se instalará Kaspersky Endpoint Security de acuerdo con la opción de cobertura que haya elegido para la tarea.

Paso 3. Configuración de un paquete de instalación

En este paso, configure el paquete de instalación:

1. Seleccione el paquete de instalación de Kaspersky Endpoint Security para Windows (14.2).
2. Seleccione el paquete de instalación del Agente de red.

   Cuando se instale Kaspersky Endpoint Security, se instalará también la versión seleccionada del Agente de red. El *Agente de red* facilita la interacción entre el Servidor de administración y un equipo cliente. Si el Agente de red ya está instalado en el equipo, no se volverá a instalar.

3. En el bloque **Forzar la descarga del paquete de instalación**, seleccione el grupo de confianza necesario:

   - **Usando el Agente de red**. El Agente de red es responsable de entregar el paquete de instalación de Kaspersky Endpoint Security a los equipos cliente. Si el Agente de red no está instalado, la tarea finaliza con un error. En este caso, añada el paquete de instalación del Agente de red a la tarea *Instalar aplicación en remoto* y habilite la entrega de archivos mediante recursos del sistema operativo. A continuación, el Agente de red se instalará utilizando recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.

   - **Usando los recursos del sistema operativo mediante puntos de distribución**. El paquete de instalación se entrega a los equipos cliente mediante recursos del sistema operativo a través de puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

   - **Usando los recursos del sistema operativo mediante el Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante los recursos del sistema operativo a través del Servidor de Administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.

4. En el campo **Número máximo de descargas concurrentes**, establezca un límite para el número de solicitudes de descarga de paquetes de instalación que se envían al Servidor de administración. Limitar el número de solicitudes ayudará a evitar que la red se sobrecargue.

5. En el campo **Número máximo de intentos de instalación**, establezca un límite para el número de intentos de instalación de la aplicación. Si la instalación de Kaspersky Endpoint Security termina con un error, la tarea volverá a empezar automáticamente.

6. Si es necesario, desactive la casilla **No reinstalar la aplicación si ya se encuentra instalada**. Permite, por ejemplo, instalar una de las versiones anteriores de la aplicación.

7. Si es necesario, desactive la casilla **Verificar el tipo de sistema operativo antes de descargar**. Esto le permite evitar la descarga de un paquete de distribución de aplicaciones si el sistema operativo del equipo no cumple los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple los requisitos de software, puede omitir esta verificación.

8. Si es necesario, active la casilla **Asignar instalación del paquete en las directivas de grupo de Active Directory**. Kaspersky Endpoint Security se instala mediante el Agente de red o manualmente mediante Active Directory. Para instalar el Agente de red, la tarea de instalación remota debe ejecutarse con privilegios de administrador de dominio.

9. Si es necesario, active la casilla **Indicar a los usuarios que cierren las aplicaciones en ejecución**. La instalación de Kaspersky Endpoint Security consume recursos del equipo. Para comodidad del usuario, el Asistente de instalación de la aplicación le pide que cierre las aplicaciones en ejecución antes de iniciar la instalación. Esto ayuda a evitar interrupciones en el funcionamiento de las demás aplicaciones y evita posibles fallos en el equipo.

10. En el bloque **Comportamiento para dispositivos administrados a través de otros Servidores de administración**, seleccione el método de instalación de Kaspersky Endpoint Security. Si la red tiene más de un Servidor de administración instalado, estos Servidores de administración pueden ver los mismos equipos cliente. Esto puede causar, por ejemplo, que una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes servidores de administración, o puede generar otros conflictos.

Paso 4. Selección de la cuenta para ejecutar la tarea

Seleccione la cuenta para instalar el Agente de red mediante las herramientas del sistema operativo. En este caso, se necesitan derechos de administrador para acceder al equipo. Puede añadir varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación utiliza la siguiente cuenta. Si instala Kaspersky Endpoint Security mediante las herramientas del Agente de red, no tiene que seleccionar una cuenta.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente haciendo clic en el botón **Finalizar**. La nueva tarea aparecerá en la lista de tareas. Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**. La aplicación se instalará en modo silencioso. Después de la instalación, el icono aparecerá en al área de notificación del equipo del usuario. Si el icono que aparece es , compruebe si la aplicación está activada.

Instalación de la aplicación de manera local mediante el Asistente de instalación

La interfaz del Asistente de configuración de aplicaciones consta de una secuencia de ventanas correspondientes a los pasos de instalación de la aplicación. Asegúrese de que la cuenta de usuario con la que está ejecutando el Asistente de instalación esté en el grupo de administradores.

Para instalar la aplicación (o actualizar una versión anterior) con el Asistente de instalación:

1. Copie la carpeta del kit de distribución al equipo del usuario.
2. Ejecute setup_kes.exe.

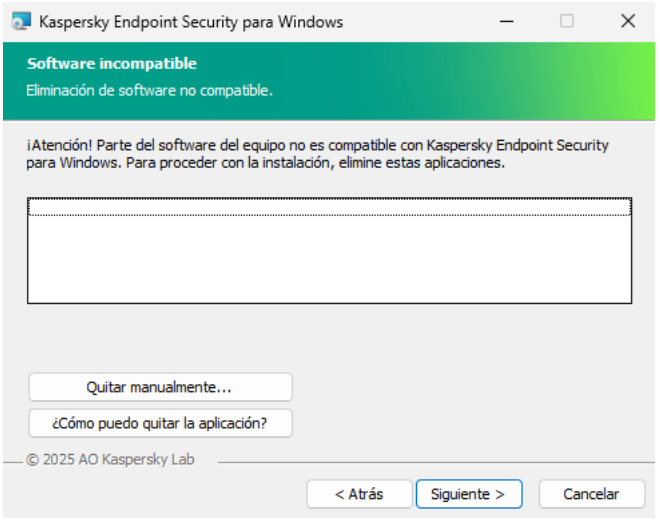
   Se iniciará el Asistente de instalación.

Preparativos para la instalación

Antes de instalar Kaspersky Endpoint Security en un equipo o actualizarlo desde una versión anterior, se comprueban las siguientes condiciones:

- Si hay algún software instalado que pueda tener problemas de compatibilidad con Kaspersky Endpoint Security (la lista de software está disponible en el archivo incompatible.txt que se incluye en el kit de distribución).
- Si se cumplen o no los requisitos de hardware y software.
- Si Microsoft .NET Framework está presente.
- Si el usuario tiene los derechos necesarios para instalar el producto de software.

Si alguno de los requisitos previos no se cumple, se muestra una notificación pertinente en pantalla. Por ejemplo, una notificación acerca de software incompatible (vea la imagen más abajo).



Eliminación de software incompatible

Si el equipo cumple con los requerimientos arriba indicados, el Asistente de instalación buscará aplicaciones de Kaspersky que puedan provocar conflictos si se ejecutan al mismo tiempo que la aplicación que se va a instalar. Si se encuentran estas aplicaciones, se le pregunta si desea eliminarlas manualmente.

Si las aplicaciones detectadas incluyen versiones anteriores de Kaspersky Endpoint Security, todos los datos que se pueden migrar (por ejemplo, datos de activación y configuración de la aplicación) se conservan y se usan durante la instalación de Kaspersky Endpoint Security 14.2 para Windows, y la versión anterior de la aplicación se elimina automáticamente. Esto se aplica a las siguientes versiones de la aplicación:

- Kaspersky Endpoint Security 12.3 para Windows (compilación 12.3.0.493)
- Kaspersky Endpoint Security 12.4 para Windows (compilación 12.4.0.467)
- Kaspersky Endpoint Security 12.5 para Windows (compilación 12.5.0.539)
- Kaspersky Endpoint Security 12.6 para Windows (compilación 12.6.0.438)
- Kaspersky Endpoint Security 12.7 para Windows (compilación 12.7.0.533)
- Kaspersky Endpoint Security 12.8 para Windows (compilación 12.8.0.505)
- Kaspersky Endpoint Security 12.9 para Windows (compilación 12.9.0.384)
- Kaspersky Endpoint Security 12.10 para Windows (compilación 12.10.0.466)
- Kaspersky Endpoint Security 12.11 para Windows (compilación 12.11.0.637)
- Kaspersky Endpoint Security 12.12 para Windows (compilación 12.12.0.522)
- Kaspersky Endpoint Security 14.0 para Windows (compilación 14.0.0.504)
- Kaspersky Endpoint Security 14.1 para Windows (compilación 14.1.0.423)

Configuración de Kaspersky Endpoint Security



Elección de la configuración de la aplicación

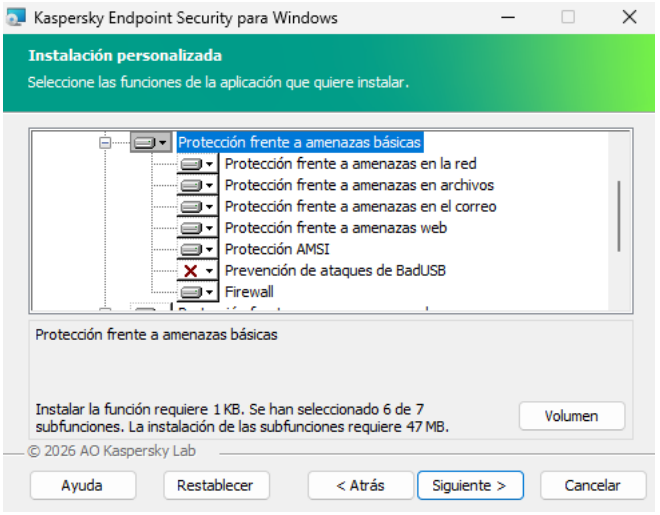
Modo estándar. Es la configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para soluciones de Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra varias amenazas, ataques de red y fraudes.

Endpoint Detection and Response Agent. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.

Light Agent para proteger entornos virtuales. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Los componentes de Kaspersky Endpoint Security

Durante la instalación, puede seleccionar los componentes de Kaspersky Endpoint Security que desea instalar (vea la imagen más abajo). El componente de Protección frente a amenazas en archivos es un componente obligatorio que se debe instalar. No puede cancelar su instalación.



Elegir componentes de la aplicación para instalar

De forma predeterminada, se seleccionan todos los componentes de la aplicación para la instalación, a excepción de los siguientes:

- Cifrado de disco de Kaspersky
- Cifrado de archivos
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- Integración con KUMA

Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación. Para ello, tiene que ejecutar el Asistente de instalación de nuevo y elegir cambiar los componentes disponibles.

Si necesita instalar los componentes de Detection and Response, Kaspersky Endpoint Security admite las siguientes configuraciones:

- Solo Endpoint Detection and Response Optimum
- Solo Endpoint Detection and Response Expert (cloud)
- Solo Endpoint Detection and Response Expert (on-premises)

- Solo Network Detection and Response (KATA)
- Solo Sandbox
- Endpoint Detection and Response Optimum y Sandbox
- Endpoint Detection and Response Expert (cloud) y Sandbox
- Endpoint Detection and Response Expert (on-premises) y Sandbox
- Network Detection and Response (KATA) y Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) y Managed Detection and Response

Kaspersky Endpoint Security verifica la selección de los componentes antes de instalar la aplicación. Si la configuración seleccionada de los componentes de Detection and Response no es compatible, no se puede instalar Kaspersky Endpoint Security.

Seleccionar la carpeta para instalar la aplicación

Puede cambiar la ruta de instalación de Kaspersky Endpoint Security en un equipo cliente. De manera predeterminada, la aplicación se instala en la carpeta `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`.

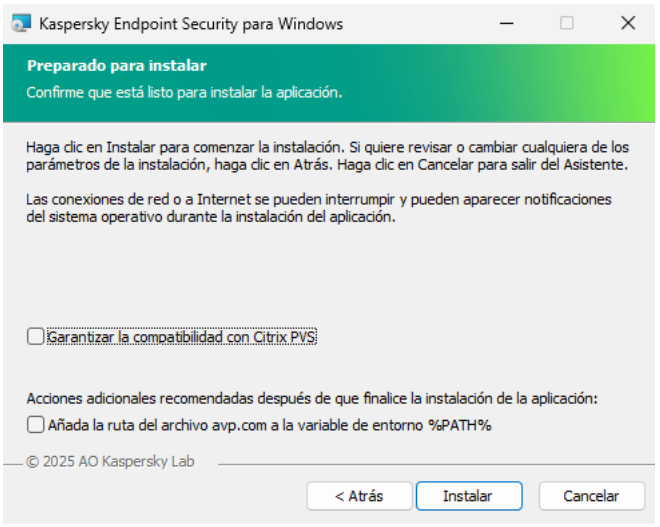
Configurar la zona de confianza

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores.

A partir de Kaspersky Endpoint Security 12.8 para Windows, puede instalar la aplicación en modo Light Agent para proteger los entornos virtuales. Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware.

También puede configurar la zona de confianza más adelante en las propiedades de la directiva: exclusiones de análisis y aplicaciones de confianza.

Configuración avanzada



Configuración de la instalación de la aplicación avanzada

Proteger el proceso de instalación de la aplicación. La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Windows Remote Desktop), se aconseja que desactive la protección del proceso de instalación.

Garantizar la compatibilidad con Citrix PVS. Puede habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual.

Añada la ruta del archivo avp.com a la variable de entorno %PATH%. Puede añadir la ruta de instalación a la variable %PATH% para un uso conveniente de la interfaz de línea de comandos.

Instalando remotamente la aplicación usando System Center Configuration Manager

Estas instrucciones se aplican a System Center Configuration Manager 2012 R2.

Para una aplicación de forma remota mediante System Center Configuration Manager:

1. Abra la consola de Configuration Manager.
2. En la parte derecha de la consola, en el bloque **Administración de aplicaciones**, seleccione **Paquetes**.
3. En la parte superior de la consola del panel de control, haga clic en el botón **Crear paquete**.
   Esto inicia el *Asistente de nuevo paquete y aplicación*.

4. En el Asistente de nuevo paquete y aplicación:

   a. En la sección **Paquete**:

      - En el campo **Nombre**, introduzca el nombre del paquete de instalación.
      - En el campo **Carpeta de origen**, especifique la ruta a la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security.

   b. En la sección **Tipo de aplicación**, seleccione la opción **Programa estándar**.

   c. En la sección **Programa estándar**:

      - En el campo **Nombre**, introduzca el nombre único para el paquete de instalación (por ejemplo, el nombre de la aplicación que incluye la versión).
      - En el campo **Línea de comandos**, especifique las opciones de instalación de Kaspersky Endpoint Security en la línea de comandos.
      - Haga clic en el botón **Examinar** para especificar la ruta al archivo ejecutable de la aplicación.
      - Asegúrese de que la lista **Modo de ejecución** tenga seleccionado el elemento **Ejecutar con derechos administrativos**.

   d. En la sección **Requisitos**:

      - Seleccione la casilla de verificación **Ejecutar otro programa primero** si desea que se inicie una aplicación diferente antes de instalar Kaspersky Endpoint Security.

        Seleccione la aplicación de la lista desplegable **Aplicación** o especifique la ruta al archivo ejecutable de esta aplicación haciendo clic en el botón **Examinar**.

      - Seleccione la opción **Este programa solo puede ejecutarse en las plataformas especificadas** en el bloque **Requisitos de plataforma** si desea que la aplicación solo se instale en los sistemas operativos especificados.

        En la siguiente lista, seleccione las casillas de verificación que hay junto a los sistemas operativos en los cuales se instalará Kaspersky Endpoint Security.

      Este paso es opcional.

   e. En la sección **Resumen**, compruebe todos los valores de la configuración que se han introducido y haga clic en **Siguiente**.

   El paquete de instalación creado aparecerá en la sección **Paquetes** de la lista de paquetes de instalación disponibles.

5. En el menú contextual del paquete de instalación, seleccione **Implementar**.

   Esto inicia el *Asistente de implementación*.

6. En el Asistente de implementación:

   a. En la sección **General**:

      - En el campo **Software**, introduzca el nombre único del paquete de instalación o seleccione el paquete de instalación de la lista haciendo clic en el botón **Examinar**.

      - En el campo **Colección**, introduzca el nombre de la colección de equipos en los cuales se instalará la aplicación, o bien seleccione la colección haciendo clic en el botón **Examinar**.

   b. En la sección **Contiene**, añada puntos de distribución (si desea obtener más información, consulte la documentación de ayuda para System Center Configuration Manager).

   c. Si es necesario, especifique los valores de otra configuración en el Asistente de implementación. Estos ajustes son opcionales para la instalación remota de Kaspersky Endpoint Security.

   d. En la sección **Resumen**, compruebe todos los valores de la configuración que se han introducido y haga clic en **Siguiente**.

Después de que finalice el Asistente de implementación, se creará una tarea para la instalación remota de Kaspersky Endpoint Security.

Descripción de la configuración de instalación del archivo setup.ini

El archivo setup.ini se utiliza al instalar la aplicación desde la línea de comandos o al utilizar del Editor de directivas de grupo de Microsoft Windows. Para aplicar la configuración del archivo setup.ini, coloque estos archivos en la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security.

Use el archivo setup.ini solo para instalar la aplicación en modo silencioso.

No se puede añadir una ruta al archivo de configuración install.cfg en el archivo setup.ini. La aplicación también omite el archivo de configuración install.cfg si se encuentra en la misma carpeta que el kit de distribución de Kaspersky Endpoint Security. Para aplicar los parámetros del archivo de configuración install.cfg, debe especificar la ruta al archivo en el siguiente comando de instalación de la aplicación: `CONFIGPATH=<path to the configuration file>`.

DESCARGAR EL ARCHIVO SETUP.INI

El archivo setup.ini contiene las siguientes secciones:

- `[Setup]`: configuración general de instalación de la aplicación.
- `[Components]`: selección de los componentes de la aplicación que se van a instalar en el modo estándar. Si no se especifica ningún componente, se instalarán todos los componentes que estén disponibles en el sistema operativo. Protección frente a amenazas en archivos es un componente obligatorio y se instala en el equipo al margen de la configuración indicada en esta sección.
- `[Tasks]`: selección de tareas que se incluirán en la lista de tareas de Kaspersky Endpoint Security. Si no se especifica la tarea, se incluirán todas las tareas de la lista de tareas de Kaspersky Endpoint Security.

Las alternativas al valor `1` son los valores `yes`, `on`, `enable`, `enabled` y `true`. Las alternativas al valor `0` son los valores `no`, `off`, `disable`, `disabled` y `false`.

Configuración del archivo setup.ini

Sección	Parámetro	Descripción
`[Setup]`	`InstallDir`	Ruta a la carpeta de instalación de la aplicación.
	`ActivationCode`	Código de activación de Kaspersky Endpoint Security.
	`Eula`	Aceptación de las condiciones del Contrato de licencia de usuario final. El contenido del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Se requiere la aceptación de los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar la versión de esta.
	`PrivacyPolicy`	Aceptación de la Política de privacidad. El texto de la Política de privacidad se incluye en el Kit de distribución de Kaspersky Endpoint Security. Para instalar la aplicación o actualizar su versión, debe aceptar la Política de privacidad.
	`KSN`	Aceptación o rechazo de la participación en Kaspersky Security Network (KSN). Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security solicitará la confirmación de su consentimiento o el rechazo de la participación en KSN cuando se inicie Kaspersky Endpoint Security por primera vez. Valores disponibles: • `1`: aceptación de la participación en KSN. • `0`: rechazo de la participación en KSN (valor predeterminado). El paquete de distribución de Kaspersky Endpoint Security se optimiza para su uso con Kaspersky Security Network. Si optara por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que la instalación se haya completado.
	`CLEANERSIGNCHECK`	Verificación de firmas digitales de los archivos de software detectados de la lista de incompatible.txt. Para eliminar el software, Kaspersky Endpoint Security ejecuta el archivo de instalación del software. Si el archivo de instalación no tiene una firma digital, Kaspersky Endpoint Security considera que el archivo no es de confianza y detiene la eliminación del software para evitar la ejecución de código potencialmente malicioso. Si la aplicación no puede verificar la firma digital del archivo de software detectado, la instalación de Kaspersky Endpoint Security se detiene con un error. El valor predeterminado difiere en función del método de instalación del software: • `0` significa que la verificación de firmas digitales está desactivada (es el valor predeterminado si se implementa a través de Kaspersky Security Center). • `1` significa que la verificación de firma digital está activada (es el valor predeterminado si la aplicación se está instalando localmente).
	`Login`	Configure el nombre de usuario para acceder a las funciones y ajustes de Kaspersky Endpoint Security (el componente Protección con contraseña). El nombre de usuario se configura junto con los parámetros `Password` y `PasswordArea`. El nombre de usuario KLAdmin se utiliza de forma predeterminada.

Sección	Parámetro	Descripción
	`Password`	Especifique una contraseña para acceder a las funciones y ajustes de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros `Login` y `PasswordArea`). Si especificó una contraseña, pero no especificó un nombre de usuario con el parámetro `Login`, se utiliza de forma predeterminada el nombre de usuario KLAdmin.
	`PasswordArea`	Especifique el alcance de la contraseña para acceder a Kaspersky Endpoint Security. Cuando un usuario intenta realizar una acción que está dentro de este alcance, Kaspersky Endpoint Security solicita las credenciales de la cuenta del usuario (parámetros `Login` y `Password`). Si necesita especificar más de un valor, use el carácter `;`. Valores disponibles: • `SET`: modificar la configuración de la aplicación. • `EXIT`: salir de la aplicación. • `DISPROTECT`: desactivar componentes de protección y detener tareas de análisis. • `DISPOLICY`: desactivar la directiva de Kaspersky Security Center. • `UNINST`: eliminar la aplicación del equipo. • `DISCTRL`: desactivar componentes de control. • `REMOVELIC`: eliminar la clave. • `REPORTS`: consultar informes. • `EXPORT` - exportar ajustes de la aplicación. Por ejemplo, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Activación o desactivación del mecanismo que protege la instalación de la aplicación. Valores disponibles: • `1`: se activa el mecanismo de protección de la instalación de la aplicación (valor predeterminado). • `0`: se desactiva el mecanismo de protección de la instalación de la aplicación. La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Windows Remote Desktop), se aconseja que desactive la protección del proceso de instalación.
	`PROTECTOSSERVICES`	Funcionalidad de protección de los servicios del sistema operativo. La protección de los servicios del sistema operativo evita que aplicaciones de terceros interfieran con el funcionamiento de los servicios del sistema operativo. Dichos servicios incluyen, por ejemplo, la aplicación del servicio de autoarranque. • `1` significa que la protección de los servicios del sistema operativo está activada (valor predeterminado). • `0` significa que la protección de los servicios del sistema operativo está desactivada.
	`EnableAzureSupport`	Activación o desactivación del modo de compatibilidad de Azure WVD. Valores disponibles: • `1`: modo de compatibilidad de Azure WVD activado. • `0`: modo de compatibilidad de Azure WVD desactivado (valor predeterminado). Esta función garantiza que el estado de las máquinas virtuales de Azure se muestre correctamente en la consola de Kaspersky Anti Targeted Attack Platform. Para supervisar el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar un Sensor ID único y permanente a estas máquinas virtuales. Si el modo de compatibilidad se desactiva, el Sensor ID puede cambiar después de reiniciar el equipo debido al funcionamiento de las máquinas virtuales de Azure. Esto puede hacer que aparezcan duplicados de máquinas virtuales en la consola.
	`Reboot`	Reinicio automático del equipo, si es necesario después de la instalación o la actualización de la aplicación. Si no se establece ningún valor para este parámetro, se bloquea el reinicio automático del equipo. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.
	`AddEnvironment`	En la variable del sistema %PATH%, añada la ruta hacia los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security. Valores disponibles: • `1`: la variable del sistema %PATH% se complementa con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security. • `0`: la variable del sistema %PATH% no se complementa con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security.

Sección	Parámetro	Descripción
	AMPPL	Activa o desactiva el uso de la tecnología AM-PPL (Antimalware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para obtener más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019. Valores disponibles: • 1: los procesos de Kaspersky Endpoint Security se protegen con la tecnología AM-PPL. • 0: los procesos de Kaspersky Endpoint Security no se protegen con la tecnología AM-PPL.
	UPGRADEMODE	Modo de actualización de la aplicación: • Seamless significa que la aplicación se actualiza con un reinicio del equipo (valor predeterminado). • Force significa que la aplicación se actualiza sin reiniciar. La posibilidad de actualizar la aplicación sin reiniciar se incluye a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo. La posibilidad de instalar parches sin reiniciar también se incluye a partir de la versión 11.11.0. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. Por tanto, el modo de actualización de la aplicación se especifica en la configuración de la aplicación. Puede cambiar este parámetro en la configuración de la aplicación o en la directiva. Al actualizar la aplicación ya instalada, la prioridad del parámetro especificado en el archivo setup.ini es más alta que la del parámetro especificado en la configuración de la aplicación o en la línea de comandos. Por ejemplo, si se especifica el modo de actualización Force en el archivo setup.ini file y el modo Seamless en la configuración de la aplicación, la actualización se instalará sin reiniciar (Force). Si usa el archivo setup.ini file, donde no se especifica el parámetro UPGRADEMODE, el instalador usará un valor predeterminado (Seamless) e instalará la actualización reiniciando el equipo.
	SetupReg	Permite que se graben en el Registro las claves del archivo setup.reg. SetupReg: setup.reg valor del parámetro.
	EnableTraces	Activar o desactivar el rastreo de la aplicación. Una vez que Kaspersky Endpoint Security se inicia, los archivos de seguimiento se guardan en la carpeta %ProgramData%\Kaspersky Lab\KES.14.2\Traces. Valores disponibles: • 1: el rastreo está activado. • 0: el rastreo está desactivado (valor predeterminado).
	TracesLevel	Nivel de detalle del seguimiento. Valores disponibles: • 100 (crítico). Solo mensajes sobre errores graves. • 200 (alto). Mensajes sobre todos los errores, incluidos los errores graves. • 300 (diagnóstico). Mensajes sobre todos los errores, además de las advertencias. • 400 (importante). Todos los mensajes de error y de advertencia, así como otra información adicional. • 500 (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado). • 600 (bajo). Todos los mensajes.
	RESTAPI	Administrar la aplicación a través de la API REST. Para administrar la aplicación a través de la API REST, debe especificar el nombre de usuario (parámetro RESTAPI_User). Valores disponibles: • 1: se permite la administración a través de la API REST. • 0: se bloquea la administración a través de la API REST (valor predeterminado). Para administrar la aplicación a través de la API REST, debe permitirse la administración mediante sistemas de administración. Para ello, configure el parámetro AdminKitConnector=1. Si administra la aplicación a través de la API REST, no es posible administrarla mediante los sistemas de administración de Kaspersky.
	RESTAPI_User	Nombre de usuario de la cuenta de dominio de Windows utilizada para administrar la aplicación a través de la API REST. La administración de la aplicación a través de la API REST solo está disponible para este usuario. Introduzca el nombre de usuario con el formato <DOMAIN>\<UserName> (por ejemplo, RESTAPI_User=COMPANY\Administrator). Solo puede seleccionar un usuario para que funcione con la API REST. Añadir un nombre de usuario es un requisito previo para poder administrar la aplicación a través de la API REST.
	RESTAPI_Port	Puerto utilizado para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782. Asegúrese de que el puerto esté libre.

Sección	Parámetro	Descripción
	`RESTAPI_Certificate`	Certificado para identificar solicitudes (por ejemplo, `RESTAPI_Certificate=C:\cert.pem`). La interacción segura de Kaspersky Endpoint Security con el cliente REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga útil de cada solicitud.
	`StandaloneMode`	Instalación de la aplicación en modo Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* es una aplicación que se instala en estaciones de trabajo y servidores individuales en la infraestructura de TI de la organización para dar soporte a las soluciones Kaspersky Managed Detection and Response y Kaspersky Anti Targeted Attack Platform. EDR Agent es compatible con aplicaciones EPP de terceros. Esto le permite utilizar herramientas de seguridad de infraestructura de terceros junto con Detection and Response de Kaspersky. Para instalar EDR Agent, en la sección `[Components]`, seleccione los componentes `StandaloneKATA`, `StandaloneNDR` o `StandaloneMDR`. EDR Agent no es compatible con otros componentes de la aplicación. Valores disponibles: • `1` para instalar la aplicación en modo EDR Agent. • `0` para instalar la aplicación en modo Estándar (predeterminado).
	`KSVLAMode`	Instalación de la aplicación en modo Light Agent. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. Valores disponibles: • `1` para instalar la aplicación en modo Light Agent. • `0` para instalar la aplicación en modo Estándar (predeterminado).
	`InstallOnVDI`	Activación del modo de protección VDI al instalar la aplicación en modo Light Agent (`KSVLAMode=1`). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas. Valores disponibles: • `1` para activar el modo de protección VDI. • `0` para desactivar el modo de protección VDI (predeterminado).
	`KESExclusions`	Añadir exclusiones de análisis y aplicaciones de confianza predefinidas al instalar la aplicación en el servidor. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Por ejemplo, las exclusiones de análisis predefinidas para servidores SQL incluyen archivos de base de datos MDF y LDF. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. Valores disponibles: • `1` activa exclusiones de análisis predefinidas y aplicaciones de confianza. • `0` desactiva exclusiones de análisis predefinidas y aplicaciones de confianza.
	`LAExclusions`	Añadir exclusiones de análisis y aplicaciones de confianza predefinidas al instalar la aplicación en una máquina virtual (modo Light Agent). Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware. Valores disponibles: • `1` activa exclusiones de análisis predefinidas y aplicaciones de confianza. • `0` desactiva exclusiones de análisis predefinidas y aplicaciones de confianza.

Sección	Parámetro	Descripción
	`EnableUniqueSensorID`	Creación de un identificador de equipo único (Sensor ID) durante la instalación o actualización de la aplicación. Sensor ID se utiliza en la solución Kaspersky Anti Targeted Attack Platform para identificar los equipos que envían telemetría al servidor. Al crear Sensor ID, la aplicación utiliza un algoritmo que tiene en cuenta la configuración del equipo, como el número de serie de la placa base. En algunos casos, por ejemplo, al usar la aplicación en un entorno virtual, Sensor ID puede estar duplicado. Como resultado, Kaspersky Anti Targeted Attack Platform no puede identificar el equipo desde el que se envía la telemetría. Para crear un Sensor ID único, debe establecer el parámetro `EnableUniqueSensorID=1`. Como resultado, la aplicación utilizará un algoritmo diferente para crear el Sensor ID, que tiene en cuenta otros datos sobre el equipo. Esto asegura un Sensor ID único. De forma predeterminada, el parámetro no está configurado. La aplicación hereda el Sensor ID en los siguientes casos: • actualización de la versión de la aplicación; • migración de la configuración [KES + KEA] a la configuración [KES + agente incorporado]. Como parte de la reparación de la aplicación, el instalador intenta heredar el Sensor ID. Si el Sensor ID no se puede restaurar, la aplicación crea un nuevo Sensor ID.
	`CitrixCompatibility`	Habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual.
`[Components]`	`ALL`	Instalación de todos los componentes. Si se especifica el valor del parámetro `1`, todos los componentes se instalarán sin tener en cuenta la configuración de la instalación de componentes concretos. Debido a la forma en que se soportan las soluciones de Detection and Response, los componentes Endpoint Detection and Response Optimum y Sandbox se instalan en el equipo. El componente Endpoint Detection and Response Expert (cloud) no es compatible con esta configuración.
	`MailThreatProtection`	Protección frente a amenazas en el correo.
	`WebThreatProtection`	Protección frente a amenazas web.
	`AMSI`	Protección AMSI.
	`HostIntrusionPrevention`	Prevención de intrusiones en el host.
	`BehaviorDetection`	Detección de comportamiento.
	`ExploitPrevention`	Prevención de vulnerabilidades.
	`RemediationEngine`	Motor de reparación.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Protección frente a amenazas en la red.
	`WebControl`	Control web.
	`DeviceControl`	Control de dispositivos.
	`ApplicationControl`	Control de aplicaciones.
	`AdaptiveAnomaliesControl`	Control de anomalías adaptativo.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Inspección de registros
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	Protección frente a amenazas en archivos.
	`SystemIntegrityMonitor`	Control de integridad del sistema.
	`FileEncryption`	Bibliotecas de cifrado de archivos.
	`DiskEncryption`	Bibliotecas de cifrado de disco completo.
	`MSBitLocker`	Bibliotecas de administración de cifrado de BitLocker.
	`BadUSBAttackPrevention`	Prevención de ataques de BadUSB.

Sección	Parámetro	Descripción
	`EDR`	Endpoint Detection and Response Optimum El componente no es compatible con los componentes Endpoint Detection and Response Expert (cloud) (`EDRCloud`) y Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) El componente no es compatible con los componentes Endpoint Detection and Response Optimum (`EDR`) y Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) El componente no es compatible con los componentes Endpoint Detection and Response Expert (cloud) (`EDRCloud`) y Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox o KATA Sandbox. *Kaspersky Sandbox* es una solución independiente de Detection and Response de Kaspersky. *KATA Sandbox* es un componente de la solución Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) El componente no es compatible con los componentes Endpoint Detection and Response Expert (cloud) (`EDRCloud`) y Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Administración de aplicaciones mediante sistemas de administración. Los sistemas de administración incluyen, por ejemplo, Kaspersky Security Center. Además de los sistemas de administración de Kaspersky, puede usar soluciones de terceros. Kaspersky Endpoint Security proporciona una API para este fin. Valores disponibles: • `1`: se permite la administración de aplicaciones con la ayuda de sistemas de administración (valor predeterminado). • `0`: se permite la administración de aplicaciones solo a través de la interfaz local.
	`KUMAIntegration`	Integración con KUMA.
	`StandaloneKATA`	Instalación de la aplicación en el modo Endpoint Detection and Response Agent (EDR Agent) para la integración con Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Instalación de la aplicación en el modo Endpoint Detection and Response Agent (EDR Agent) para la integración con Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalación de la aplicación en el modo Endpoint Detection and Response Agent (EDR Agent) para la integración con Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalación de la aplicación en el modo Endpoint Detection and Response Agent (EDR Agent) para la integración con KUMA.
`[Tasks]`	`ScanMyComputer`	Tarea de Análisis completo. Valores disponibles: • `1`: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0`: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.
	`ScanCritical`	Tarea de Análisis de áreas críticas. Valores disponibles: • `1`: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0`: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.

Sección	Parámetro	Descripción
	`Updater`	Tarea de actualización. Valores disponibles: • `1`: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0`: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.

Procesos de Kaspersky Endpoint Security para Windows

Kaspersky Endpoint Security para Windows inicia los procesos descritos en la tabla siguiente.

Procesos de Kaspersky Endpoint Security para Windows

Nombre del archivo	Finalidad
avp.exe	Proceso de trabajo de Kaspersky Endpoint Security para Windows.
avpsus.exe	Este proceso permite instalar y revertir las actualizaciones críticas y aprobadas de los módulos de la aplicación.

Cambiar componentes de la aplicación

Durante la instalación de la aplicación, puede seleccionar qué componentes estarán disponibles. Puede cambiar los componentes de la aplicación disponibles de las siguientes maneras.

- De forma local, utilizando el Asistente de instalación.

  Los componentes de la aplicación se cambian a través del Panel de control, siguiendo el procedimiento típico para las aplicaciones de Windows. Ejecute el Asistente de configuración de la aplicación y seleccione la opción para cambiar los componentes de la aplicación que están disponibles. Las instrucciones en pantalla le indicarán qué hacer.

  > Este método no está disponible si la aplicación se instaló a través de Kaspersky Security Center. Puede cambiar la selección de componentes de la aplicación en el Panel de control solo después de instalar la aplicación localmente.

- De forma remota utilizando Kaspersky Security Center.

  Para cambiar los componentes una vez que la aplicación se ha instalado, puede usar la tarea *Cambiar componentes de la aplicación*.

Tenga en cuenta las siguientes consideraciones especiales al cambiar los componentes de la aplicación:

- En los equipos que ejecutan Windows Server, no puede instalar todos los componentes de Kaspersky Endpoint Security (por ejemplo, el componente Control de anomalías adaptativo no está disponible).

- Si los discos duros de su equipo están protegidos por la característica Cifrado de disco completo (FDE), no puede eliminar el componente Cifrado de disco completo. Para eliminar el componente Cifrado de disco completo, descifre todos los discos duros del equipo.

- Si el equipo tiene archivos cifrados (FLE) o el usuario utiliza unidades extraíbles cifradas (FDE o FLE), no se podrá acceder a los archivos y unidades extraíbles después de que se eliminen los componentes de Cifrado de datos. Puede acceder a los archivos y unidades extraíbles volviendo a instalar los componentes de Cifrado de datos.

- Si la aplicación se instala en modo Light Agent en una infraestructura VDI, no se admite el cambio de los componentes del conjunto.

Cómo añadir o quitar componentes de la aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Seleccionar componentes para instalar**.

Paso 2. Configuración de tareas para cambiar los componentes de la aplicación

Seleccione la configuración de la aplicación:

- **Modo estándar para proteger hosts**. Es la configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para soluciones de Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra varias amenazas, ataques de red y fraudes.

- **Endpoint Detection and Response Agent para protección contra amenazas avanzadas y ataques selectivos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.

  Al cambiar la configuración de la aplicación para que el EDR Agent funcione con MDR, asegúrese de que los componentes responsables de recibir la telemetría estén activados.

- **Light Agent para proteger entornos virtuales**. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Seleccione los componentes de la aplicación que estarán disponibles en el equipo del usuario.

Paso 3. Configuración avanzada

Establezca la configuración avanzada de la tarea (consulte la tabla a continuación).

Paso 4. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 5. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando el equipo está inactivo.

Paso 6. Definir el nombre de la tarea

Escriba un nombre para la tarea (por ejemplo, *Añadir el componente Control de aplicaciones*).

Paso 7. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo añadir o quitar componentes de la aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2.0**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Cambiar componentes de la aplicación**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Añadir el componente Control de aplicaciones*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Por ejemplo, seleccione un grupo de administración independiente o cree una selección.

Paso 3. Conclusión de la creación de tareas

Seleccione la casilla **Abrir los detalles de la tarea cuando se complete la creación** y finalice el asistente.

En las propiedades de tarea, seleccione la pestaña **Configuración de la aplicación**. A continuación, seleccione la configuración de la aplicación:

- **Modo estándar para proteger estaciones de trabajo y servidores**. Es la configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para soluciones de Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra varias amenazas, ataques de red y fraudes.

- **Endpoint Detection and Response Agent para protección contra amenazas avanzadas y ataques selectivos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.

  Al cambiar la configuración de la aplicación para que el EDR Agent funcione con MDR, asegúrese de que los componentes responsables de recibir la telemetría estén activados.

- **Light Agent para proteger entornos virtuales**. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Seleccione los componentes de la aplicación que estarán disponibles en el equipo del usuario. Establezca la configuración avanzada de la tarea (consulte la tabla a continuación).

El conjunto de componentes de Kaspersky Endpoint Security se modificará en los equipos de los usuarios en modo silencioso. Las opciones de configuración de los componentes disponibles se mostrarán en la interfaz local de la aplicación. Los componentes que no se hayan incluido en la aplicación estarán desactivados, y sus opciones de configuración no estarán disponibles.

Al instalar, actualizar o desinstalar Kaspersky Endpoint Security, pueden producirse errores. Para obtener más información sobre cómo solucionar estos errores, consulte la Base de conocimientos de soporte técnico.

Parámetro	Descripción
Configuración de tareas	**Comprobar si existen aplicaciones de terceros incompatibles**. De forma predeterminada, Kaspersky Endpoint Security comprueba la compatibilidad de las aplicaciones instaladas. La lista de software que puede causar problemas de incompatibilidad está disponible en el archivo incompatible.txt. El archivo se incluye en el kit de distribución. Si el análisis del software instalado está activado, cuando se detecta una aplicación de la lista, Kaspersky Endpoint Security detiene la tarea. Puede desactivar el análisis del software instalado si la documentación del proveedor de software de terceros afirma ser compatible con Endpoint Protection Platform (EPP). **Eliminar aplicaciones de terceros incompatibles**. Eliminación automática de aplicaciones de la lista incompatible.txt antes de cambiar el conjunto de componentes. Si esta función está activada, Kaspersky Endpoint Security intenta eliminar las aplicaciones que pueden causar problemas de compatibilidad para continuar con la tarea. **Usar el modo de compatibilidad de Azure WVD**. Esta función garantiza que el estado de las máquinas virtuales de Azure se muestre correctamente en la consola de Kaspersky Anti Targeted Attack Platform. Para supervisar el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar un Sensor ID único y permanente a estas máquinas virtuales. Si el modo de compatibilidad se desactiva, el Sensor ID puede cambiar después de reiniciar el equipo debido al funcionamiento de las máquinas virtuales de Azure. Esto puede hacer que aparezcan duplicados de máquinas virtuales en la consola.
Exclusiones	A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. A partir de Kaspersky Endpoint Security 12.8 para Windows, puede instalar la aplicación en modo Light Agent para proteger los entornos virtuales. Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware. También puede configurar la zona de confianza más adelante en las propiedades de la directiva: exclusiones de análisis y aplicaciones de confianza.
Modo independiente/Modo combinado	Puede crear conjuntos de componentes independientes para estaciones de trabajo y servidores: **Modo independiente**. Antes de implementar el paquete de instalación, el instalador detecta el tipo de sistema operativo e instala solo los componentes de la aplicación que ha seleccionado para dicho tipo. De esta forma, puede utilizar el mismo paquete de instalación para estaciones de trabajo y servidores. **Modo combinado** ofrece una lista común de componentes para estaciones de trabajo y servidores. La disponibilidad de componentes individuales depende del tipo de sistema operativo. En este modo, recomendamos crear un paquete de instalación independiente para las estaciones de trabajo y un paquete de instalación independiente para los servidores. Puede configurar la lista común de componentes en el paquete de instalación solo en el modo Estándar.
Usar una contraseña para modificar el conjunto de componentes de la aplicación	Los administradores suelen activar la protección con contraseña para restringir el acceso a Kaspersky Endpoint Security. Es decir, para modificar la selección de componentes de la aplicación, debe introducir credenciales de un usuario que tenga permiso **Eliminar/modificar/restaurar la aplicación**. Por ejemplo, puede utilizar la cuenta KLAdmin.
Usar la contraseña para desinstalar Kaspersky Endpoint Agent y Kaspersky Security for Windows Server	Los administradores suelen activar la protección con contraseña en la configuración de estas tareas para restringir el acceso a Kaspersky Endpoint Agent (KEA) y Kaspersky Security for Windows Server (KSWS). Es decir, si está migrando de la configuración [KES KEA] a [KES + agente integrado], o si está migrando de KSWS a KES, debe introducir una contraseña para eliminar estas aplicaciones.

Actualización de una versión anterior de la aplicación

Cuando actualice de una versión anterior de la aplicación a una más reciente, tenga en cuenta lo siguiente:

- Se recomienda cerrar todas las aplicaciones activas antes de realizar la actualización.
- Antes de que comience la actualización, Kaspersky Endpoint Security bloqueará la característica de cifrado de disco completo. Si el cifrado de disco completo no se pudiera bloquear, la instalación de actualización no se iniciará. El cifrado de disco completo se desbloqueará una vez que concluya la actualización.
- Para cambiar el idioma de la aplicación, en la tarea *Instalar aplicación en remoto*, seleccione el paquete de instalación con la localización que prefiera y actualice la aplicación. La posibilidad de cambiar el idioma de la aplicación se incorporó por primera vez en Kaspersky Endpoint Security para Windows 14.2.

Puede actualizar las siguientes versiones de Kaspersky Endpoint Security:

- Kaspersky Endpoint Security 12.3 para Windows (compilación 12.3.0.493)
- Kaspersky Endpoint Security 12.4 para Windows (compilación 12.4.0.467)
- Kaspersky Endpoint Security 12.5 para Windows (compilación 12.5.0.539)
- Kaspersky Endpoint Security 12.6 para Windows (compilación 12.6.0.438)
- Kaspersky Endpoint Security 12.7 para Windows (compilación 12.7.0.533)
- Kaspersky Endpoint Security 12.8 para Windows (compilación 12.8.0.505)
- Kaspersky Endpoint Security 12.9 para Windows (compilación 12.9.0.384)
- Kaspersky Endpoint Security 12.10 para Windows (compilación 12.10.0.466)
- Kaspersky Endpoint Security 12.11 para Windows (compilación 12.11.0.637)
- Kaspersky Endpoint Security 12.12 para Windows (compilación 12.12.0.522)
- Kaspersky Endpoint Security 14.0 para Windows (compilación 14.0.0.504)
- Kaspersky Endpoint Security 14.1 para Windows (compilación 14.1.0.423)

Al instalar, actualizar o desinstalar Kaspersky Endpoint Security, pueden producirse errores. Para obtener más información sobre cómo solucionar estos errores, consulte la Base de conocimientos de soporte técnico.

Métodos de actualización de la aplicación

Kaspersky Endpoint Security se puede actualizar en el equipo de varias maneras:

- Usar el servicio de actualización de Kaspersky (Seamless Update – SMU).
- de forma local, utilizando el Asistente de instalación;
- de forma local, utilizando la línea de comando;
- de forma remota utilizando Kaspersky Security Center.
- de forma remota, utilizando el Editor de administración de directivas de grupo de Microsoft Windows (para más información, visite el sitio web de soporte técnico de Microsoft).
- de forma remota, utilizando System Center Configuration Manager.

Si la aplicación implementada en la red corporativa presenta un conjunto de componentes distinto del conjunto predeterminado, la actualización de la aplicación mediante la Consola de administración (MMC) difiere de la actualización mediante Web Console. Cuando actualice Kaspersky Endpoint Security, tenga en cuenta lo siguiente:

- Kaspersky Security Center Web Console.

  Si ha creado un paquete de instalación para la nueva versión de la aplicación con el conjunto de componentes predeterminado, el conjunto de componentes en el equipo de un usuario no cambiará. Para usar Kaspersky Endpoint Security con el conjunto de componentes predeterminado, debe abrir las propiedades del paquete de instalación, cambiar el conjunto de componentes y, después, volver al conjunto de componentes original y guardar los cambios.

- Consola de administración de Kaspersky Security Center.

  El conjunto de componentes de la aplicación después de la actualización coincidirá con el conjunto de componentes en el paquete de instalación. Es decir, si la nueva versión de la aplicación tiene el conjunto de componentes predeterminado, por ejemplo, el agente de MDR integrado se eliminará del equipo, ya que este componente no forma parte del conjunto predeterminado. Para seguir utilizando la aplicación con el mismo conjunto de componentes que antes de la actualización, seleccione los componentes necesarios en la configuración del paquete de instalación.

Actualizar la aplicación sin reiniciar

La actualización de la aplicación sin reiniciar ofrece una operación ininterrumpida del servidor cuando se actualiza la versión de la aplicación.

Actualizar la aplicación sin reiniciar presenta las siguientes limitaciones:

- La posibilidad de actualizar la aplicación sin reiniciar se incluye a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo.
- La posibilidad de instalar parches sin reiniciar el equipo se incluye a partir de la versión 11.11.0. Para instalar parches en versiones anteriores de la aplicación, es posible que deba reiniciar el equipo.
- La actualización de la aplicación sin reiniciar no está disponible en equipos con cifrado de datos activado (cifrado de Kaspersky (FDE), BitLocker, Cifrado de archivos (FLE)). Para actualizar la aplicación en equipos con cifrado de datos activado, el equipo se debe reiniciar.
- La aplicación no se puede actualizar en una máquina virtual sin reiniciar. Para actualizar la aplicación en una máquina virtual, debe reiniciar la máquina virtual.

Después de actualizar la aplicación, instalar un parche, cambiar el conjunto de componentes de la aplicación o restaurar, Kaspersky Endpoint Security se reinicia para comenzar a usar la nueva versión. Reiniciar Kaspersky Endpoint Security puede tardar hasta un minuto. Durante este período, el nivel de protección del equipo se reduce. Después de reiniciar la aplicación, se restaurará el nivel de protección del equipo.

Cómo seleccionar el modo de actualización de la aplicación en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.

5. En el bloque **Configuración avanzada**, seleccione o desactive la casilla de verificación **Instalar actualizaciones de la aplicación sin reiniciar** para configurar el modo de actualización de la aplicación.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar el modo de actualización de la aplicación en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general → Interacción del usuario**.

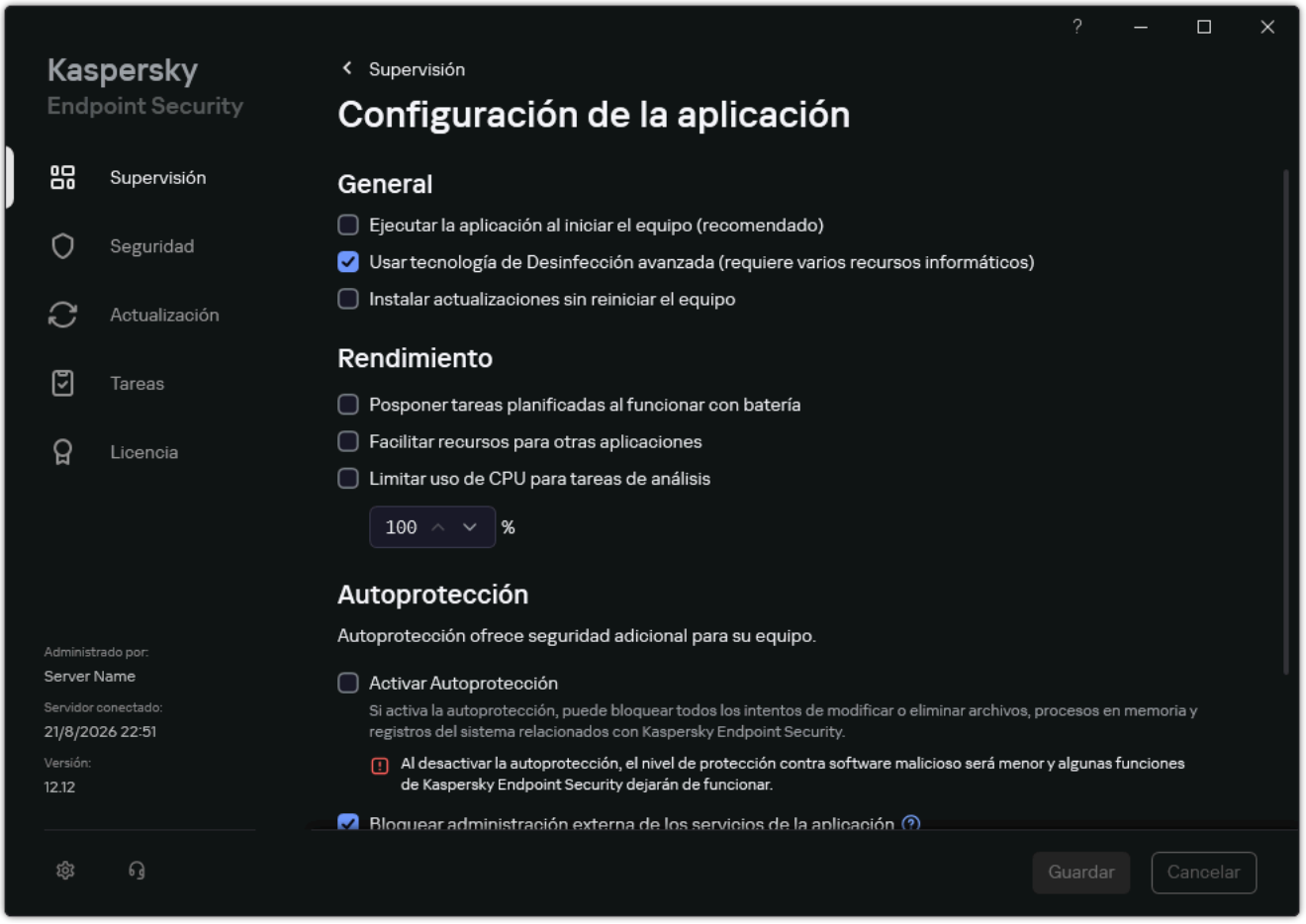
5. En el bloque **Configuración de actualización de aplicaciones**, seleccione o desactive la casilla de verificación **Instalar actualizaciones de la aplicación sin reiniciar** para configurar el modo de actualización de la aplicación.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar el modo de actualización de la aplicación en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Configuración de la aplicación**.



3. En el bloque **General**, seleccione o desactive la casilla de verificación **Instalar actualizaciones sin reiniciar el equipo** para configurar el modo de actualización de la aplicación.

4. Guarde los cambios.

También puede seleccionar el modo de actualización de la aplicación al instalar la aplicación desde la línea de comandos (mediante la opción `UPGRADEMODE`).

Cuando el procedimiento de actualización de la aplicación sin reiniciar finalice, se habrá instalado la nueva versión de Kaspersky Endpoint Security en el equipo. La versión anterior de la aplicación se elimina automáticamente.

No puede iniciar una actualización de la aplicación antes de que la actualización anterior finalice por completo.

Puede comprobar el estado de la actualización de Kaspersky Endpoint Security utilizando el informe de la versión de la aplicación de Kaspersky en la consola de Kaspersky Security Center.

Actualización de SMU de la aplicación

Para actualizar la aplicación mediante el servicio de actualización de Kaspersky (Seamless Update; SMU), no es necesario ejecutar el instalador, a diferencia de otros métodos de actualización. Kaspersky Endpoint Security obtiene la nueva versión de la aplicación, junto con las bases de datos antivirus, de la misma fuente.

Una actualización de SMU permite actualizar la aplicación en todos los equipos de su organización a la última versión. Antes de aplicar una actualización de SMU, recomendamos probar la nueva versión de la aplicación en algunos equipos. Para hacerlo, debe actualizar la aplicación en estos equipos manualmente (por ejemplo, de forma local, usando el Asistente de configuración). No puede seleccionar equipos individuales al realizar una actualización de SMU.

El personal de Kaspersky determina el calendario de actualización de la aplicación. Para asegurarse de que la nueva versión de la aplicación se ejecuta sin problemas, Kaspersky ofrece actualizaciones paso a paso. Esto significa que puede obtener la actualización de SMU hasta dos meses después del lanzamiento de una nueva versión.

Puede administrar la actualización de SMU de la aplicación utilizando la tarea *Actualización de las bases de datos y módulos de la aplicación*. Para tener la nueva versión de la aplicación incluida en el mismo paquete que las bases de datos antivirus, debe permitir la actualización de los *módulos de la aplicación* en la configuración de la tarea *Actualización de las bases de datos y módulos de la aplicación*. También en la configuración de la tarea *Actualización de las bases de datos y módulos de la aplicación* puede permitir la actualización de la aplicación sin reiniciar.

Pasos de una actualización de SMU de la aplicación

1. **Después del lanzamiento de una nueva versión de la aplicación, Kaspersky distribuye la actualización.**

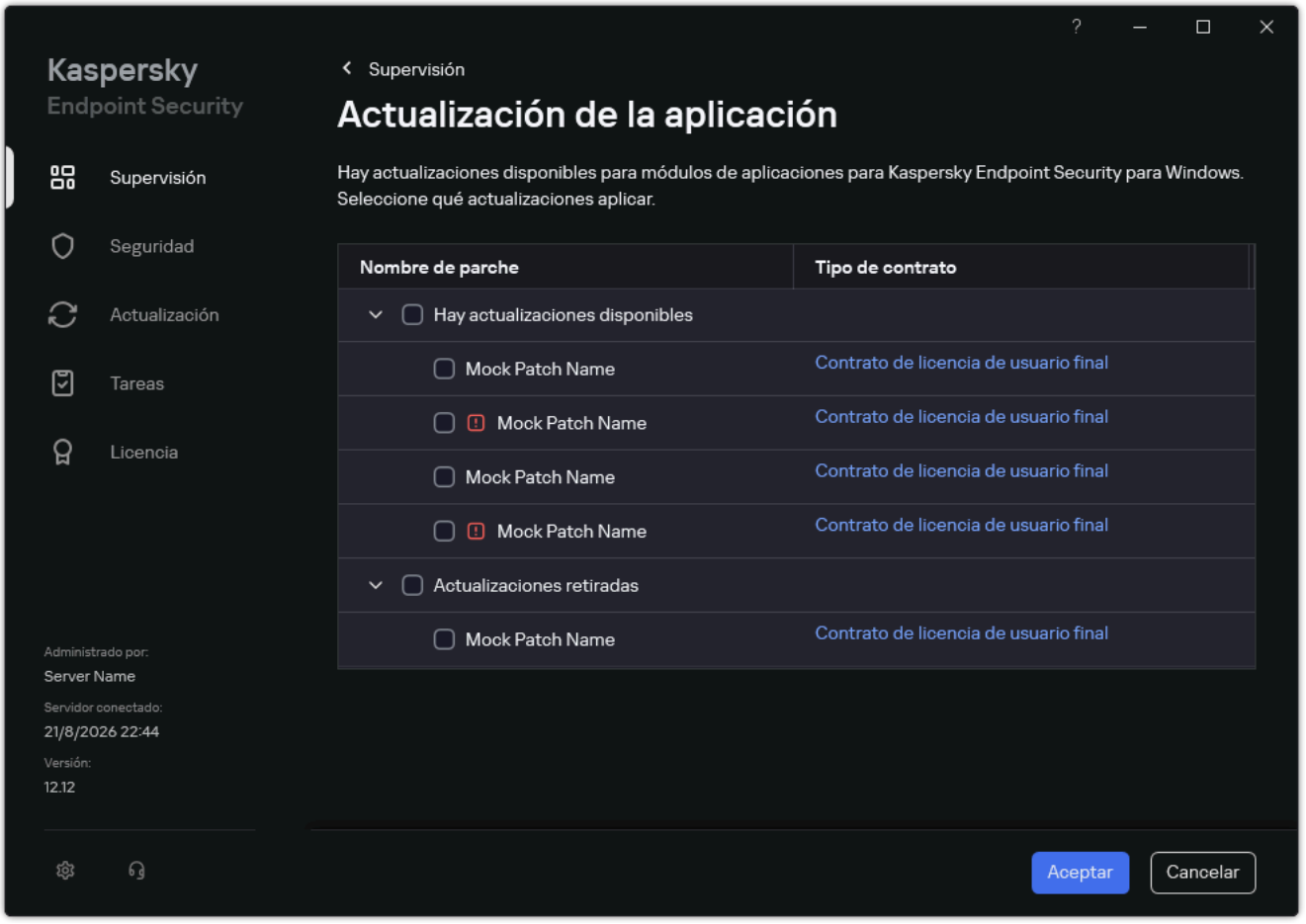
2. **El usuario aprueba la actualización de la aplicación.**

   Si el equipo está conectado a Kaspersky Security Center, la actualización está disponible en Kaspersky Security Center, en la sección de **actualización de las bases de datos y los módulos de la aplicación de Kaspersky**. Para obtener más información sobre la aprobación de actualizaciones, consulte la Ayuda de Kaspersky Security Center.

   Si el equipo no está conectado a Kaspersky Security Center, la actualización está disponible en la sección de notificaciones de la interfaz de la aplicación: . Para aprobar la actualización, seleccione una versión de la aplicación y acepte los términos y condiciones de los contratos (consulte la figura a continuación).

3. **Kaspersky Endpoint Security ejecuta la tarea *Actualización de las bases de datos y módulos de la aplicación* de acuerdo con el calendario configurado.**

Como resultado, Kaspersky Endpoint Security actualiza la aplicación en modo "silencioso".



Actualizaciones de aplicaciones disponibles

Eliminar la aplicación

La eliminación de Kaspersky Endpoint Security deja al equipo y a los datos del usuario desprotegidos frente a las amenazas.

Al instalar, actualizar o desinstalar Kaspersky Endpoint Security, pueden producirse errores. Para obtener más información sobre cómo solucionar estos errores, consulte la Base de conocimientos de soporte técnico.

Eliminación de la aplicación de forma remota con Kaspersky Security Center

Para desinstalar la aplicación a distancia, puede utilizar la tarea *Desinstalar aplicación en remoto*. Cuando se ejecuta esta tarea, Kaspersky Endpoint Security descarga al equipo del usuario una utilidad que permite llevar a cabo la desinstalación. La utilidad se elimina automáticamente una vez desinstalada la aplicación.

Cómo quitar la aplicación mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.

   Se abre la lista de tareas.
3. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Servidor de administración de Kaspersky Security Center → Avanzado → Desinstalar aplicación en remoto**.

Paso 2. Selección de la aplicación que se quitará

Seleccione **Desinstalar aplicación compatible con Kaspersky Security Center**.

Paso 3. Configuración de tareas para la desinstalación de la aplicación

Seleccione **Kaspersky Endpoint Security para Windows (14.2)**.

Paso 4. Desinstalación de la configuración de utilidades

Haga los cambios adicionales que necesite en la configuración de la aplicación:

- **Forzar la descarga de la utilidad de desinstalación**. Seleccione el método de entrega de la utilidad:
  - **Usando el Agente de red**. Si el Agente de red no se ha instalado en el equipo, primero se instalará el Agente de red utilizando las herramientas del sistema operativo. Kaspersky Endpoint Security se desinstalará entonces con las herramientas del Agente de red.
  - **Usando los recursos del sistema operativo mediante el Servidor de administración**. La utilidad se enviará a los equipos cliente a través del Servidor de administración, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.
  - **Usando los recursos del sistema operativo mediante puntos de distribución**. La utilidad se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center.
- **Verificar el tipo de sistema operativo antes de descargar**. Si es necesario, desactive esta casilla de verificación. Esto evitará que la utilidad de desinstalación se descargue si el sistema operativo del equipo no cumple con los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple los requisitos de software, puede omitir esta verificación.

Si la operación para desinstalar la aplicación está protegida con contraseña, haga lo siguiente:

1. Seleccione la casilla **Utilizar contraseña de desinstalación**.
2. Haga clic en el botón **Editar**.
3. Escriba la contraseña de la cuenta KLAdmin.

Paso 5. Selección de la configuración de reinicio del sistema operativo

Después de desinstalar la aplicación es necesario reiniciar. Seleccione la acción que se llevará a cabo para reiniciar el equipo.

Paso 6. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 7. Selección de la cuenta para ejecutar la tarea

Seleccione la cuenta para instalar el Agente de red mediante las herramientas del sistema operativo. En este caso, se necesitan derechos de administrador para acceder al equipo. Puede añadir varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación utiliza la siguiente cuenta. Si Kaspersky Endpoint Security se va a desinstalar con las herramientas del Agente de red, no es necesario que seleccionar una cuenta.

Paso 8. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando el equipo está inactivo.

Paso 9. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Desinstalar Kaspersky Endpoint Security 14.2*.

Paso 10. Finalización de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

La aplicación se desinstalará en modo silencioso.

Cómo quitar la aplicación mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.
   Se abre la lista de tareas.
2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Desinstalar aplicación en remoto**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Desinstalar Kaspersky Endpoint Security de los equipos de soporte técnico*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Por ejemplo, seleccione un grupo de administración independiente o cree una selección.

Paso 3. Configuración de los parámetros para desinstalar la aplicación

En este paso, configure los parámetros que se usarán para desinstalar la aplicación:

1. Seleccione el tipo **Desinstalar aplicación administrada**.
2. Seleccione **Kaspersky Endpoint Security para Windows**.

3. **Forzar la descarga de la utilidad de desinstalación**. Seleccione el método de entrega de la utilidad:

   - **Usando el Agente de red**. Si el Agente de red no se ha instalado en el equipo, primero se instalará el Agente de red utilizando las herramientas del sistema operativo. Kaspersky Endpoint Security se desinstalará entonces con las herramientas del Agente de red.

   - **Usando los recursos del sistema operativo mediante el Servidor de administración**. La utilidad se enviará a los equipos cliente a través del Servidor de administración, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.

   - **Usando los recursos del sistema operativo mediante puntos de distribución**. La utilidad se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

4. En el campo **Número máximo de descargas concurrentes**, establezca un límite a la cantidad de solicitudes que podrán enviarse al Servidor de administración para descargar la utilidad de desinstalación. Limitar el número de solicitudes ayudará a evitar que la red se sobrecargue.

5. En el campo **Número máximo de intentos de desinstalación**, establezca un límite a la cantidad de veces que se intentará desinstalar la aplicación. Cuando la desinstalación de Kaspersky Endpoint Security finaliza con un error, la tarea hace un nuevo intento automáticamente.

6. Si es necesario, desactive la casilla **Verificar el tipo de sistema operativo antes de descargar**. Esto evitará que la utilidad de desinstalación se descargue si el sistema operativo del equipo no cumple con los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple los requisitos de software, puede omitir esta verificación.

Paso 4. Selección de la cuenta para ejecutar la tarea

Seleccione la cuenta para instalar el Agente de red mediante las herramientas del sistema operativo. En este caso, se necesitan derechos de administrador para acceder al equipo. Puede añadir varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación utiliza la siguiente cuenta. Si Kaspersky Endpoint Security se va a desinstalar con las herramientas del Agente de red, no es necesario que seleccionar una cuenta.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente haciendo clic en el botón **Finalizar**. La nueva tarea aparecerá en la lista de tareas.

Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**. La aplicación se desinstalará en modo silencioso. Una vez que se complete la desinstalación, Kaspersky Endpoint Security mostrará una solicitud para que se reinicie el equipo.

Si la operación para desinstalar la aplicación está protegida con contraseña, deberá introducir la contraseña de la cuenta KLAdmin en las propiedades de la tarea *Desinstalar aplicación de forma remota*. La tarea no podrá ejecutarse sin esta contraseña.

Para utilizar la contraseña de la cuenta de KLAdmin en la tarea Desinstalar aplicación de forma remota, haga lo siguiente:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Desinstalar aplicación en remoto** de Kaspersky Security Center.

   Se abre la ventana propiedades de la tarea.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione la casilla **Utilizar contraseña de desinstalación**.

5. Escriba la contraseña de la cuenta KLAdmin.

6. Guarde los cambios.

Reinicie el equipo para completar la desinstalación. Para hacerlo, el Agente de red muestra una ventana emergente.

Eliminación de la aplicación de forma remota con Active Directory

Puede desinstalar de forma remota la aplicación con una directiva de grupo de Microsoft Windows. Para desinstalar la aplicación, debe abrir la consola de administración de directivas de grupo (gpmc.msc) y utilizar el editor de directivas de grupo para crear una tarea de eliminación de la aplicación (para más detalles, visite el sitio web de soporte técnico de Microsoft).

Si la operación para desinstalar la aplicación está protegida con contraseña, debe hacer lo siguiente:

1. Cree un archivo BAT con el siguiente contenido:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   `<GUID>` es el id. único de la aplicación. Puede utilizar el siguiente comando para descubrir el GUID de la aplicación en la Base de conocimientos de soporte técnico:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Ejemplo

   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Cree una nueva directiva de Microsoft Windows para los equipos en la consola de administración de directivas de grupo (gpmc.msc).

3. Use la nueva directiva para ejecutar el archivo BAT creado en los equipos.

Eliminar la aplicación localmente

Puede eliminar la aplicación de manera local, utilizando el Asistente de instalación. Kaspersky Endpoint Security se elimina a través del Panel de control, siguiendo el procedimiento típico para las aplicaciones de Windows. Se iniciará el Asistente de instalación. Las instrucciones en pantalla le indicarán qué hacer.



Selección de la operación de eliminación de la aplicación

Si lo desea, puede guardar algunos datos de la aplicación para usarlos si la instala nuevamente (por ejemplo, si actualiza la aplicación a una versión más reciente). Si no especifica ningún dato, la aplicación se eliminará por completo (vea la imagen abajo).



Guardado de datos después de la eliminación

Los datos que puede guardar son los siguientes:

- **Datos de activación**. Si conserva estos datos, no necesitará volver a activar la aplicación. Mientras la licencia siga vigente al momento de realizar la instalación, Kaspersky Endpoint Security añadirá una clave de licencia automáticamente.

- **Archivos de la copia de seguridad**. Estos son los archivos que la aplicación analizó y guardó en Copia de seguridad.

Se puede acceder a los archivos de Copia de seguridad que se han guardado después de eliminar la aplicación únicamente desde la misma versión de la aplicación que se utilizó para guardar los archivos.

Si planea utilizar los objetos de Copia de seguridad después de eliminar la aplicación, deberá restaurarlos mientras la aplicación aún esté instalada. Tenga en cuenta que estos objetos podrían ocasionar daños en el equipo, por lo que los expertos de Kaspersky no recomiendan restaurarlos.

- **Configuración operativa de la aplicación**. Son los valores seleccionados al configurar la aplicación.
- **Almacenamiento local de las claves de cifrado**. Son los datos que brindan acceso a los archivos y a las unidades que se cifraron antes de que se eliminara la aplicación. Para no quedar sin acceso a estos archivos y unidades, asegúrese de seleccionar las características de cifrado de datos cuando reinstale Kaspersky Endpoint Security. No se requiere ninguna otra acción para acceder a archivos y unidades cifrados anteriormente.

Kaspersky Endpoint Security guarda datos en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

También puede eliminar la aplicación de forma local, mediante la línea de comandos.

Licencias de la aplicación

Esta sección ofrece información sobre los conceptos generales relacionados con las licencias de Kaspersky Endpoint Security.

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* es un contrato vinculante entre usted y AO Kaspersky Lab en el que se estipulan los términos en los que puede utilizar la aplicación.

Le recomendamos que lea detenidamente los términos del Contrato de licencia antes de utilizar la aplicación.

Puede ver los términos del Contrato de licencia de las siguientes formas:

- Al instalar la aplicación de Kaspersky Endpoint Security en modo interactivo.
- Mediante la lectura del archivo license.txt. Este documento se incluye en el kit de distribución de la aplicación y también se encuentra en la carpeta de instalación de la aplicación `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Al confirmar que está de acuerdo con el Contrato de licencia de usuario final mientras instala la aplicación, acepta los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe cancelar la instalación.

Acerca de la licencia

Una *licencia* es un derecho de duración limitada para utilizar la aplicación garantizado en el Contrato de licencia de usuario final.

La licencia le permite usar la aplicación de acuerdo con los términos del Contrato de licencia de usuario final y recibir soporte técnico. La lista de funciones disponibles y la duración del uso de la aplicación dependen del tipo de licencia que se haya utilizado para activar la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Licencia de evaluación:* Licencia gratuita destinada a probar la aplicación.

  La licencia de evaluación suele durar poco tiempo. Cuando finaliza la licencia de evaluación, se desactivan todas las funciones de Kaspersky Endpoint Security. Para seguir utilizando la aplicación, debe comprar una licencia comercial.

  Puede activar la aplicación con una licencia de prueba solo una vez. La aplicación no se puede activar con una licencia de prueba después de haberse activado con una licencia comercial.

- *Licencia comercial:* Licencia de pago que se facilita cuando compra Kaspersky Endpoint Security.

  La funcionalidad de la aplicación que está disponible con licencia comercial depende del tipo de producto elegido. El producto seleccionado se indica en el Certificado de licencia. Encontrará información sobre los productos disponibles en el sitio web de Kaspersky.

Cuando la licencia comercial expira, las funciones clave de la aplicación se desactivan. Para seguir utilizando la aplicación, debe renovar la licencia comercial. Si no tiene pensado renovar la licencia, debe eliminar la aplicación del equipo.

Acerca del certificado de licencia

Un *certificado de la licencia* es un documento transferido al usuario junto con un archivo clave o código de activación.

El certificado de la licencia contiene la siguiente información sobre la licencia:

- ID de licencia o número de pedido.
- Detalles del usuario a quien se concede la licencia.
- Detalles de la aplicación que se puede activar con la licencia.
- Límite de unidades autorizadas (por ejemplo, el número de dispositivos en los cuales la aplicación se puede utilizar con la licencia).
- Fecha de inicio del período de validez de la licencia.
- Fecha de caducidad o período de validez de la licencia.
- Tipo de licencia.

Acerca de la suscripción

Una *suscripción a Kaspersky Endpoint Security* es un pedido de compra de la aplicación con parámetros específicos (como la fecha de vencimiento de la suscripción y el número de dispositivos protegidos). Puede solicitar una suscripción a Kaspersky Endpoint Security a través de su proveedor de servicios (por ejemplo, como su ISP). La suscripción puede renovarse manual o automáticamente, o bien puede cancelar su suscripción. Puede gestionar su suscripción en el sitio web del proveedor de servicios.

Es posible aplicar límites a la suscripción (por ejemplo, un año) o cancelarlos (sin una fecha de vencimiento). Para mantener Kaspersky Endpoint Security en funcionamiento después del vencimiento del plazo de suscripción limitado, tiene que renovar la suscripción. La suscripción ilimitada se renueva automáticamente si los servicios del proveedor se han pagado por adelantado a tiempo.

Cuando caduca una suscripción limitada, le pueden proporcionar un período de gracia de renovación de la suscripción durante el que la aplicación continúa funcionando. El proveedor decide la disponibilidad y la duración de ese período de gracia.

Para utilizar Kaspersky Endpoint Security mediante suscripción, necesita aplicar el código de activación recibido del proveedor de servicios. Después de que se aplique el código de activación, se añade la clave de licencia activa. La clave de licencia activa determina la licencia para usar la aplicación mediante suscripción. No puede activar la aplicación con la suscripción utilizando un archivo de clave. El proveedor de servicios puede proporcionar un solo código de activación. No se puede añadir una clave de licencia de reserva bajo una suscripción.

Los códigos de activación adquiridos mediante suscripción pueden no utilizarse para activar versiones anteriores de Kaspersky Endpoint Security.

Sobre una clave de licencia

Una *clave de licencia* es una secuencia de bits que puede usar para activar y posteriormente usar la aplicación de acuerdo con los términos del Contrato de licencia de usuario final.

Un certificado de la licencia no se proporciona para una clave añadida mediante suscripción.

Puede añadir una clave de licencia a la aplicación mediante la aplicación de un archivo de clave o el ingreso de un código de activación.

Kaspersky puede bloquear la clave si se infringen los términos de Contrato de licencia de usuario final. Si la clave se ha bloqueado, tiene que añadir otra clave distinta para continuar utilizando la aplicación.

Existen dos tipos de claves: activa y de reserva.

Una *clave de licencia activa* es aquella que utiliza actualmente la aplicación. Se puede añadir una clave de licencia de evaluación o comercial como clave de licencia activa. La aplicación solo podrá utilizar una única clave activa.

Una *clave de reserva* es una clave que da derecho al usuario a utilizar la aplicación, pero que no se encuentra actualmente en uso. Cuando la clave de licencia activa vence, se activa automáticamente una clave de licencia de reserva. Solo puede añadirse una clave de licencia de reserva si la clave de licencia activa está disponible.

Una clave para una licencia de evaluación solo se puede añadir como una clave de licencia activa. No puede añadirse como la clave de licencia de reserva. Una clave de licencia de evaluación no puede sustituir a la clave de licencia activa de una licencia comercial.

Si se añade una clave a la lista de claves prohibidas, la funcionalidad de la aplicación definida por la licencia utilizada para activar la aplicación permanece disponible durante ocho días. La aplicación notifica al usuario que la clave se ha añadido a la lista de claves prohibidas. Transcurridos ocho días, la funcionalidad de la aplicación se limita al nivel de funcionalidad disponible tras el vencimiento de la licencia. Puede usar los componentes de protección y control y ejecutar un análisis mediante las bases de datos de la aplicación que se instalaron antes de que la licencia caducara. La aplicación también continúa cifrando archivos que habían sido modificados y cifrados antes de que caducara la licencia, pero no cifra los nuevos archivos. El uso de Kaspersky Security Network no está disponible.

Acerca del código de activación

Un *código de activación* es una secuencia única de 20 caracteres alfanuméricos. Usted introduce un código de activación para añadir una clave de licencia que activa Kaspersky Endpoint Security. Recibirá un código de activación en la dirección de correo electrónico que especificó después de comprar Kaspersky Endpoint Security.

Para activar la aplicación con un código de activación, se requiere acceso a Internet con el fin de conectarse a servidores de activación de Kaspersky.

Cuando la aplicación se activa mediante un código de activación, se agrega la clave activa. Puede añadirse una clave de licencia de reserva solo con un código de activación y no con un archivo clave.

Si se extravía un código de activación después de activar la aplicación, se puede restaurar. Puede necesitar un código de activación, por ejemplo, para registrar una CompanyAccount de Kaspersky. Si se perdió el código de activación después de la activación de la aplicación, póngase en contacto con el socio de Kaspersky al que le compró la licencia.

Acerca del archivo clave

Un *archivo clave* es un archivo con la extensión .key que recibe de Kaspersky. El propósito del archivo clave es añadir una clave de licencia que active la aplicación.

Recibirá un archivo clave en la dirección de correo electrónico que haya proporcionado al comprar Kaspersky Endpoint Security o al solicitar la versión de prueba de Kaspersky Endpoint Security.

No es necesario que se conecte con los servidores de activación de Kaspersky a fin de activar la aplicación con un archivo clave.

Puede recuperar un archivo clave si se ha eliminado accidentalmente. Por ejemplo, es posible que necesite un archivo clave para registrarse en CompanyAccount de Kaspersky.

Para recuperar un archivo clave, realice uno de las siguientes acciones:

- Póngase en contacto con el vendedor de la licencia.
- Obtenga un archivo clave en el sitio web de Kaspersky según su código de activación existente.
- Obtenga un archivo clave de otro Servidor de administración.

Cuando la aplicación se activa mediante un archivo clave, se añade una clave de licencia activa. Puede añadirse una clave de licencia de reserva solo con un archivo clave y no con un código de activación.

Comparación de la funcionalidad de la aplicación según el tipo de licencia para las estaciones de trabajo

El conjunto de funcionalidades de Kaspersky Endpoint Security disponible en las estaciones de trabajo depende del tipo de licencia (consulte la siguiente tabla).

[Consulte también la comparación de la funcionalidad de la aplicación para los servidores]

Comparación de la funcionalidad de la aplicación según el tipo de licencia de Kaspersky Next, consulte la Ayuda de Kaspersky Next.

Comparación de las funciones de Kaspersky Endpoint Security

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Protección frente a amenazas avanzadas								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	✓	✓	✓	✓	✓	✓
Motor de reparación	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas básicas								
Protección frente a amenazas en archivos	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en el correo	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protección AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controles de seguridad								
Inspección de registros	–	–	–	–	–	–	–	–
Control de aplicaciones	✓	✓	✓	✓	✓	✓	✓	✓
Control de dispositivos	✓	✓	✓	✓	✓	✓	✓	✓
Control Web	✓	✓	✓	✓	✓	✓	✓	✓
Control de anomalías adaptativo	–	✓	✓	✓	✓	✓	–	✓
Control de integridad del sistema	–	–	–	–	–	–	–	–

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Cifrado de datos								
Cifrado de disco de Kaspersky	–	✓	✓	✓	✓	✓	–	✓
Cifrado de unidad BitLocker	–	✓	✓	✓	✓	✓	–	✓
Cifrado de archivos	–	✓	✓	✓	✓	✓	–	✓
Cifrado de unidades extraíbles	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(La licencia de Kaspersky Sandbox se debe comprar por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Integración con KUMA *(la licencia para la integración de KUMA se debe comprar por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo de Light Agent *(para activar la aplicación, debe añadir una clave de licencia a la SVM a la que está conectado el Light Agent)*	–	–	–	–	–	–	✓	✓

Comparación de la funcionalidad de la aplicación según el tipo de licencia para servidores

El conjunto de funcionalidades de Kaspersky Endpoint Security disponible en los servidores depende del tipo de licencia (consulte la siguiente tabla).

Consulte también la comparación de la funcionalidad de la aplicación para estaciones de trabajo

Comparación de la funcionalidad de la aplicación según el tipo de licencia de Kaspersky Next, consulte la Ayuda de Kaspersky Next.

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Protección frente a amenazas avanzadas								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de intrusiones en el host	–	–	–	–	–	–	–	–
Motor de reparación	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas básicas								
Protección frente a amenazas en archivos	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas web	–	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en el correo	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protección AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controles de seguridad								
Inspección de registros	–	–	–	–	–	–	–	✓
Control de aplicaciones	–	✓	✓	✓	✓	✓	–	✓
Control de dispositivos	–	✓	✓	✓	✓	✓	✓	✓
Control Web	–	✓	✓	✓	✓	✓	✓	✓
Control de anomalías adaptativo	–	–	–	–	–	–	–	–
Control de integridad del sistema	–	–	–	–	–	–	–	✓
Cifrado de datos								
Cifrado de disco de Kaspersky	–	–	–	–	–	–	–	–
Cifrado de unidad BitLocker	–	✓	✓	✓	✓	✓	–	✓
Cifrado de archivos	–	–	–	–	–	–	–	–

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Cifrado de unidades extraíbles	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(La licencia de Kaspersky Sandbox se debe comprar por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Integración con KUMA *(la licencia para la integración de KUMA se debe comprar por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo de Light Agent *(para activar la aplicación, debe añadir una clave de licencia a la SVM a la que está conectado el Light Agent)*	–	–	–	–	–	–	✓	✓

Activación de la aplicación

Se denomina *activación* al proceso de activar una licencia que, hasta que se llega a su fecha de caducidad, permite usar la aplicación con todas sus funciones. La activación de la aplicación implica añadir una clave de licencia.

Puede activar la aplicación de una de las siguientes formas:

- Localmente, desde la interfaz de la aplicación, mediante el Asistente de activación. Puede añadir la clave activa y la clave de reserva de esta manera.
- De forma remota, utilizando el paquete de software Kaspersky Security Center.
  - Uso de la tarea *Añadir clave*.

    Este método puede usarse para añadir una clave tanto en un equipo específico como en una serie de equipos pertenecientes a un grupo de administración. Puede añadir la clave activa y la clave de reserva de esta manera.
  - Distribuyendo a los equipos una clave almacenada en el Servidor de administración de Kaspersky Security Center.

Este método puede usarse para añadir una clave automáticamente tanto en equipos nuevos como en otros que ya se han conectado a Kaspersky Security Center. Para usar este método, primero tiene que añadir una clave al Servidor de administración de Kaspersky Security Center. Para obtener más información sobre cómo añadir una clave al Servidor de administración de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

En primer lugar, se distribuye el código de activación adquirido mediante suscripción.

- Añadiendo la clave al paquete de instalación de Kaspersky Endpoint Security.

  Este método le permite añadir la clave en las Propiedades del paquete de instalación durante el despliegue de Kaspersky Endpoint Security. La aplicación se activa automáticamente después de la instalación.

- Mediante la línea de comandos.

La activación de la aplicación con un código de activación puede llevar algún tiempo (durante la instalación remota o no interactiva), debido a la distribución de la carga a través de los servidores de activación de Kaspersky. Si necesita activar la aplicación inmediatamente, puede interrumpir la activación del proceso e iniciar la activación con el Asistente de activación.

Si Kaspersky Endpoint Security se utiliza en modo Light Agent para proteger los entornos virtuales, no es necesario activar la aplicación por separado.

Activación de la aplicación

Cómo activar la aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Añadir clave**.

Paso 2. Añadir una clave

Introduzca un código de activación o seleccione un archivo clave.

Para obtener más información sobre cómo añadir una clave al repositorio de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando el equipo está inactivo.

Paso 5. Definir el nombre de la tarea

Introduzca un nombre para la tarea, como *Activar Kaspersky Endpoint Security para Windows*.

Paso 6. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, Kaspersky Endpoint Security se activará en los equipos de los usuarios en modo silencioso.

Cómo activar la aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Añadir clave**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Activación de Kaspersky Endpoint Security para Windows*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea. Ir al paso siguiente.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Selección de una licencia

Seleccione la licencia que se usará para activar la aplicación. Ir al paso siguiente.

Puede añadir claves a Web Console (**Operaciones → Licencias**).

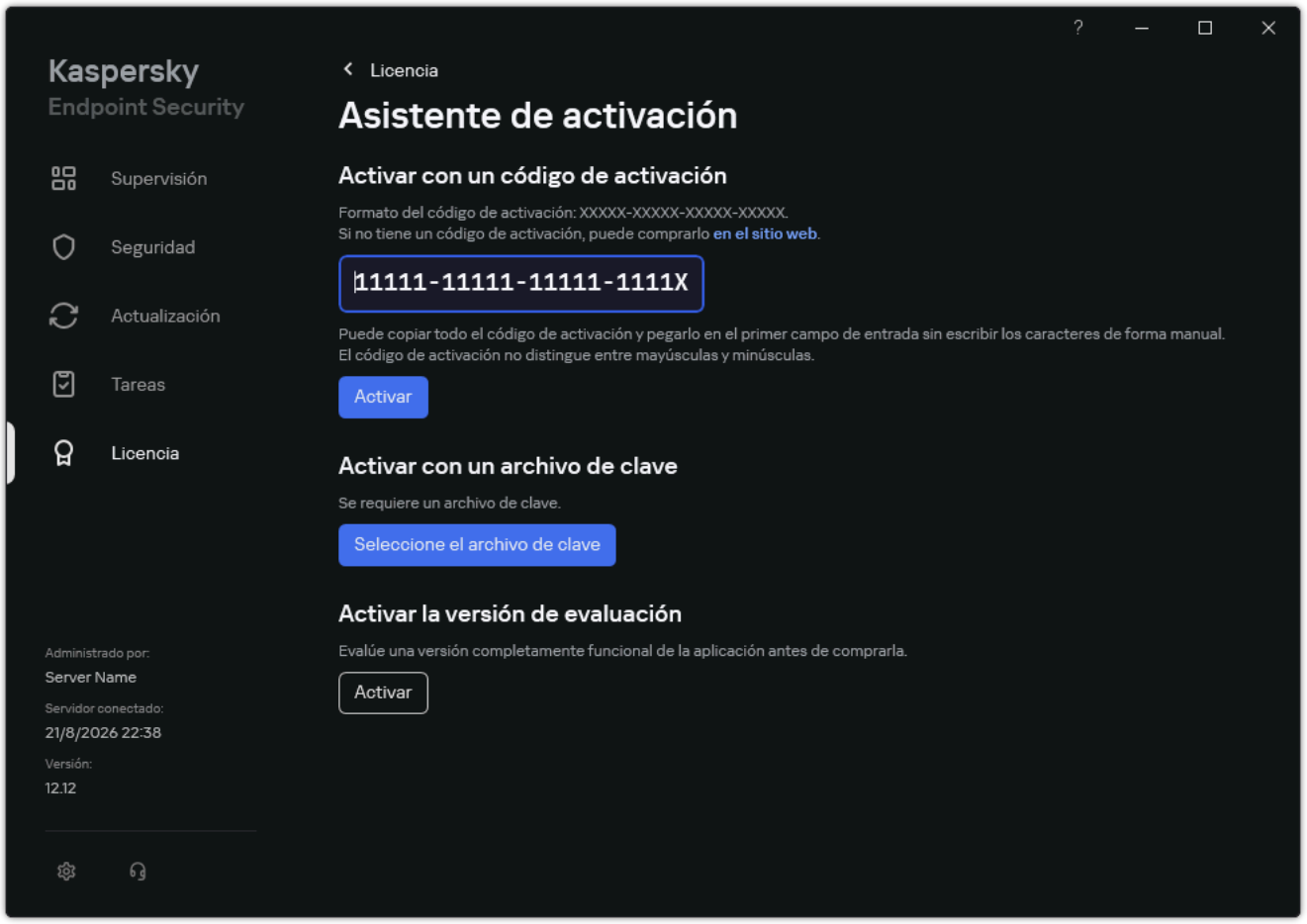
Paso 4. Conclusión de la creación de tareas

Finalice el asistente haciendo clic en el botón **Finalizar**. La nueva tarea aparecerá en la lista de tareas. Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**. Como resultado, Kaspersky Endpoint Security se activará en los equipos de los usuarios en modo silencioso.

Cómo activar la aplicación en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.
2. Haga clic en **Activar la aplicación con una licencia nueva**.

Se inicia el Asistente de activación de la aplicación. Siga las instrucciones del Asistente de activación.



Activación de la aplicación

En las propiedades de la tarea *Añadir clave*, encontrará una opción para añadir una clave de reserva al equipo. Una *clave de reserva* se activa cuando caduca la clave activa. Al haber una clave de reserva disponible, las funciones de la aplicación no quedarán limitadas cuando la licencia caduque.

Cómo añadir automáticamente una clave de licencia a los equipos mediante la Consola de administración (MMC)

1. En la Consola de administración, vaya a la carpeta **Licencias de Kaspersky**.

   Se mostrará una lista de claves de licencia.

2. Abra las propiedades de la clave de licencia.

3. En la tabla sección **General**, seleccione la casilla **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

4. Guarde los cambios.

   La clave se distribuirá a los equipos adecuados automáticamente. Durante la distribución automática de una clave en calidad de clave activa o de reserva, se tiene en cuenta el límite del número de equipos permitidos por la licencia (establecido en las propiedades de la clave). En cuanto se alcanza el límite, el proceso de distribución se detiene. El número de equipos en los que se ha añadido una clave, junto con otros datos, puede consultarse en la sección **Dispositivos** de las propiedades de la clave.

Cómo añadir automáticamente una clave de licencia a los equipos mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Operaciones → Licencias → Licencias**.

   Se mostrará una lista de claves de licencia.

2. Abra las propiedades de la clave de licencia.

3. En la pestaña **General**, active el interruptor **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

4. Guarde los cambios.

   La clave se distribuirá a los equipos adecuados automáticamente. Durante la distribución automática de una clave en calidad de clave activa o de reserva, se tiene en cuenta el límite del número de equipos permitidos por la licencia (establecido en las propiedades de la clave). En cuanto se alcanza el límite, el proceso de distribución se detiene. El número de equipos en los que se ha añadido una clave, junto con otros datos, puede consultarse en la pestaña **Dispositivos** de las propiedades de la clave.

Si activa la aplicación con un *código de activación*, necesitará acceso a Internet con el fin de conectarse a servidores de activación de Kaspersky. Si activa la aplicación con un *archivo de clave*, el acceso a Internet no será necesario. Si los equipos se encuentran en un segmento aislado de la red sin acceso a Internet, para activar la aplicación con un código, debe permitir el uso del Servidor de administración de Kaspersky Security Center como servidor proxy. Es decir, la aplicación puede acceder a los servidores de activación a través del Servidor de administración que tiene acceso a Internet.

Cómo permitir el uso del Servidor de administración como servidor proxy para activar la aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.

4. Seleccione la casilla **Usar Kaspersky Security Center como servidor proxy para la activación**.

5. Guarde los cambios.

Cómo permitir el uso del Servidor de administración como servidor proxy para activar la aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general → Integración con KSC**.

5. Seleccione la casilla **Usar Kaspersky Security Center como servidor proxy para la activación**.

6. Guarde los cambios.

Si no puede activar la aplicación con un *código de activación*, puede intentar conseguir un *archivo de clave* a través de la solución de Kaspersky e intentar volver a activar la aplicación con un método diferente.

Supervisión del uso de licencias

Para controlar el uso de las licencias, puede hacer lo siguiente:

- Ver el *Informe de uso de claves de licencia* de la infraestructura de la organización (**Supervisión** → **Informes**).
- Ver el estado de los equipos en la pestaña **Dispositivos administrados** → **Dispositivos**. Si la aplicación no está activada, el equipo tendrá el estado ⚠ *La aplicación no está activada*.
- Ver la información de la licencia en las propiedades de los equipos.
- Ver propiedades clave (**Operaciones** → **Licencias**).

Detalles de la activación de la aplicación como parte de Kaspersky Security Center Cloud Console

Se proporciona una versión de prueba para Kaspersky Security Center Cloud Console. La *versión de prueba* es una versión especial de Kaspersky Security Center Cloud Console diseñada para familiarizar a los usuarios con las funciones de la aplicación. En esta versión, puede realizar acciones en un espacio de trabajo durante un período de 30 días. Todas las aplicaciones administradas se ejecutan automáticamente con una licencia de prueba para Kaspersky Security Center Cloud Console, incluido Kaspersky Endpoint Security. Sin embargo, no puede activar Kaspersky Endpoint Security utilizando su propia licencia de prueba cuando caduque la licencia de prueba de Kaspersky Security Center Cloud Console. Para obtener más información sobre las licencias de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center Cloud Console.

> La versión de prueba de Kaspersky Security Center Cloud Console no le permite cambiar posteriormente a una versión comercial. Cualquier espacio de trabajo de prueba se eliminará automáticamente, junto con todo su contenido, una vez que expire el período de 30 días.

Eliminar una clave de licencia

Para eliminar una clave de licencia, debe ejecutar una tarea especial en sus equipos. Puede eliminar una clave de licencia, por ejemplo, para reorganizar las unidades de licencia. Además, cuando caduca la licencia, Kaspersky Endpoint Security se lo notifica. Si ha añadido una clave de licencia con un plazo breve para probar la aplicación (por ejemplo, el complemento EDR Optimum), puede eliminar esta clave de licencia para eliminar las notificaciones y corregir el estado de su equipo.

La tarea *Eliminar clave* permite eliminar cualquier clave de licencia del equipo. Puede eliminar claves de licencia activas y reservar claves de licencia. Además de la clave de licencia de activación de Kaspersky Endpoint Security, puede eliminar claves de licencia individuales de soluciones de Kaspersky Endpoint Detection and Response (por ejemplo, el complemento EDR Optimum).

Cómo eliminar una clave de licencia en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Eliminar clave**.

Paso 2. Selección de una licencia

Seleccione la clave de licencia que desea eliminar. Puede seleccionar una clave de licencia del almacén de claves de Kaspersky Security Center o seleccionar un archivo de clave.

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando el equipo está inactivo.

Paso 5. Definir el nombre de la tarea

Introduzca un nombre para la tarea; por ejemplo, *Eliminar clave para beta*.

Paso 6. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo eliminar una clave de licencia en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.
   Se abre la lista de tareas.
2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Eliminar clave**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Eliminar clave para beta*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea. Ir al paso siguiente.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Selección de una licencia

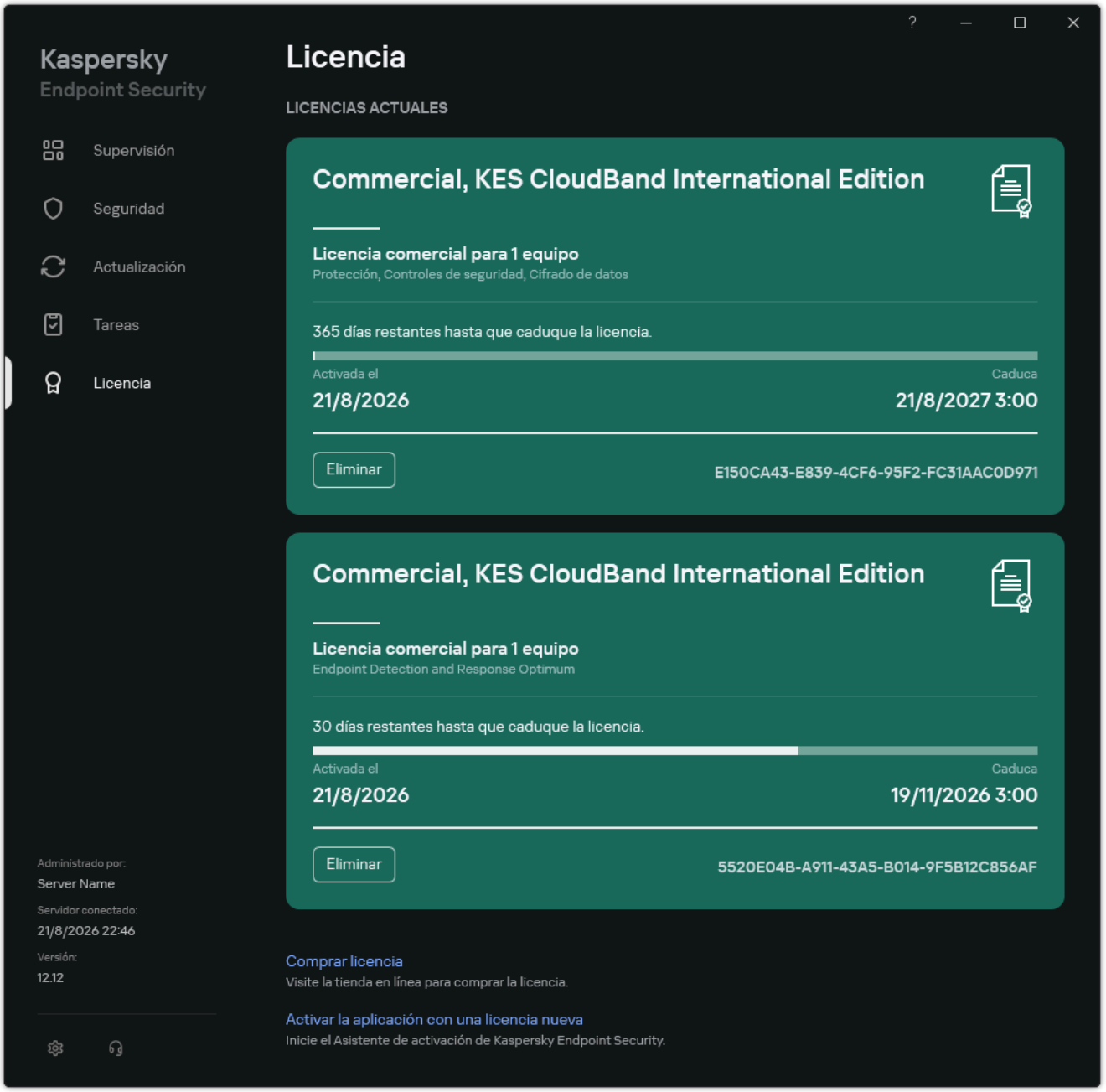
Seleccione la clave de licencia que desea eliminar. Puede seleccionar una clave de licencia del almacén de claves de Kaspersky Security Center o seleccionar un archivo de clave. Ir al paso siguiente.

Paso 4. Conclusión de la creación de tareas

Finalice el asistente haciendo clic en el botón **Finalizar**. La nueva tarea aparecerá en la lista de tareas. Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**.

Cómo eliminar una clave de licencia en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.
2. Seleccione la clave que desea eliminar y haga clic en **Eliminar**.



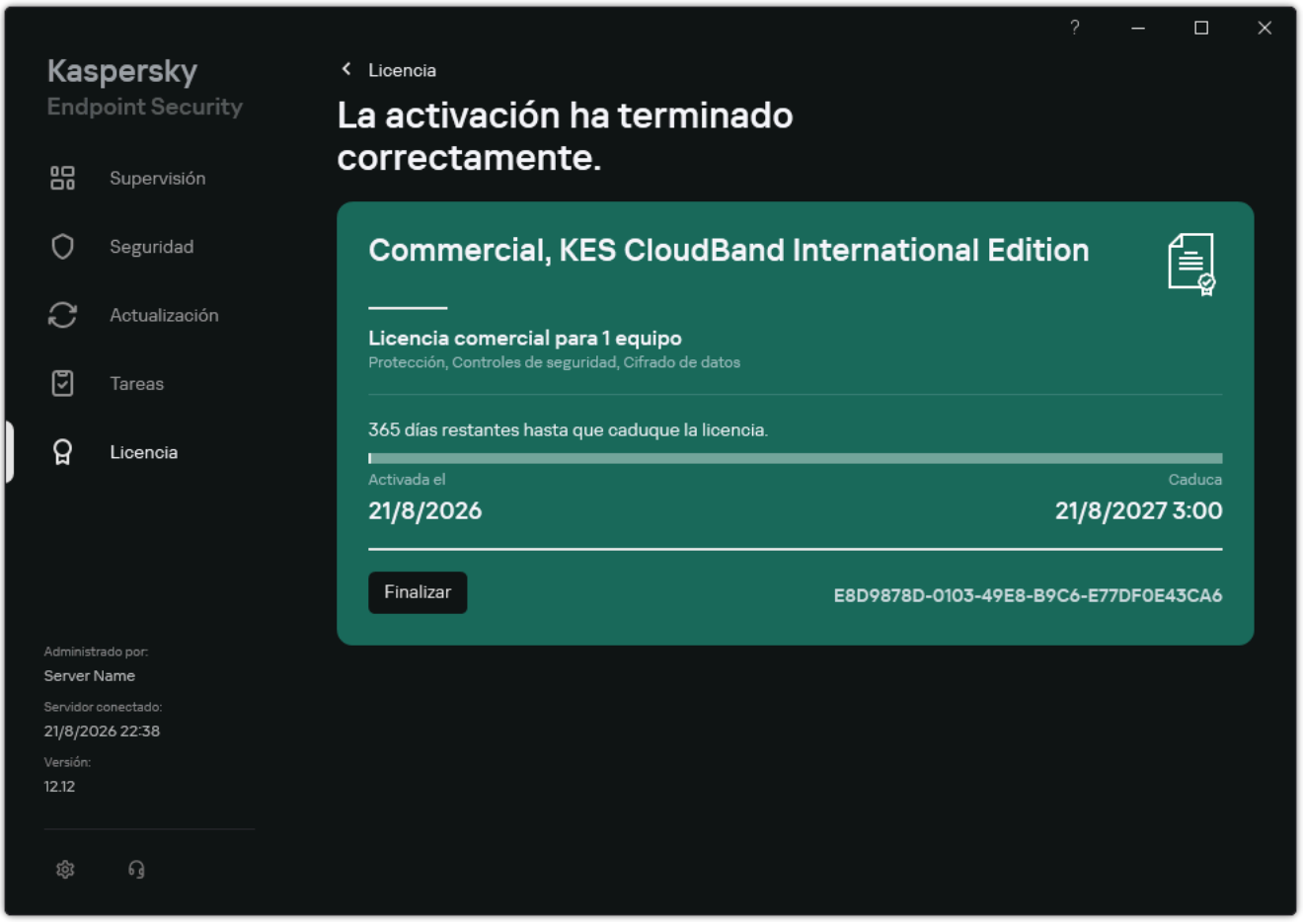
Ventana Licencia

También puede eliminar una clave de licencia en la línea de comandos.

Visualización de información de la licencia

Visualización de información sobre una licencia:

En la ventana principal de la aplicación, vaya a la sección **Licencia** (consulte la figura siguiente).



Ventana Licencia

La sección muestra los siguientes detalles:

- *Estado de la clave*. Puede almacenar más de una clave en el equipo. Existen dos tipos de claves: activa y de reserva. La aplicación solo podrá utilizar una única clave activa. La clave de licencia de reserva puede activarse solo después de que la clave de licencia activa haya caducado o si se elimina la clave de licencia activa al hacer clic en el botón **Eliminar**.
- *Nombre de aplicación*. Nombre completo de la aplicación de Kaspersky adquirida.
- *Tipo de licencia*. Están disponibles los siguientes tipos de licencias: de prueba y comercial.
- *Características*. Funciones de la aplicación que la licencia permite utilizar. Entre las funciones se encuentran Protección, Controles de seguridad, Cifrado de datos, entre otras. La lista de funciones disponibles también se proporciona en el Certificado de licencia.

- *Información adicional sobre la licencia*. Fecha de inicio y fecha de finalización del período de licencia (solo para la clave de licencia activa), duración restante del período de licencia.

  La fecha y hora de caducidad de la licencia se muestra según la zona horaria configurada en el sistema operativo.

- *Clave*. Una clave es una secuencia alfanumérica irrepetible que se genera a partir de un código de activación o de un archivo de clave.

La ventana Licencia también puede usarse para realizar las siguientes acciones:

- **Comprar licencia/Renovar la licencia**. Abre la tienda en línea de Kaspersky, un sitio web donde podrá comprar o renovar una licencia. Para hacer un pedido, deberá escribir los datos de su empresa y realizar el pago.

- **Activar la aplicación con una licencia nueva**. Abre el Asistente de activación de la aplicación. Use el asistente para añadir una clave con un código de activación o un archivo clave. El Asistente de activación de la aplicación le permitirá añadir una clave de licencia activa y un máximo de una clave de licencia de reserva.

Compra de una licencia

Puede comprar una licencia después de instalar la aplicación. Cuando compra una licencia, recibe un código de activación o un archivo clave para activar la aplicación.

Para adquirir una licencia:

1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.
2. Realice una de las siguientes acciones:

   - Si no se ha añadido ninguna clave o se ha añadido una clave de una licencia de evaluación, haga clic en el botón **Comprar licencia**.
   - Si se ha añadido la clave de una licencia comercial, haga clic en el botón **Renovar la licencia**.

   Se abrirá una ventana con el sitio web de la tienda en línea de Kaspersky, en la que podrá comprar una licencia.

Renovación de suscripciones

Cuando utiliza la aplicación mediante suscripción, Kaspersky Endpoint Security se comunica automáticamente con el servidor de activación en intervalos específicos hasta que caduque su suscripción.

Si utiliza la aplicación mediante suscripción ilimitada, Kaspersky Endpoint Security comprueba automáticamente el servidor de activación en busca de claves renovadas en segundo plano. Si hay una clave disponible en el servidor de activación, la aplicación la añade sustituyendo la clave anterior. De esta manera, la suscripción ilimitada de Kaspersky Endpoint Security se renueva sin la participación del usuario.

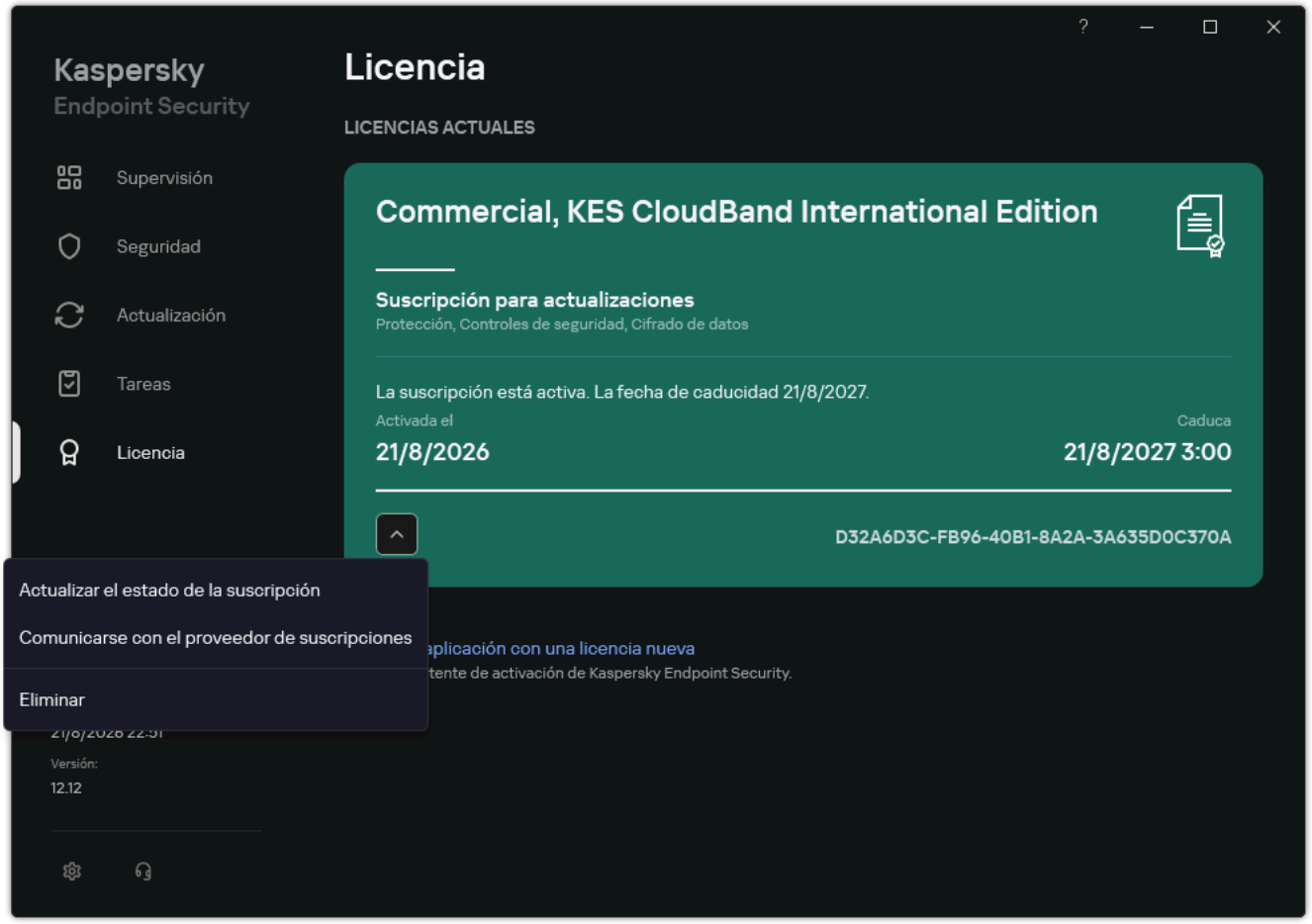
Si usa la aplicación con una suscripción limitada, en la fecha en que caduque la suscripción (o en la fecha de vencimiento del período de gracia de renovación de la suscripción) Kaspersky Endpoint Security le enviará una notificación y dejará de intentar renovar la suscripción automáticamente. En este caso, Kaspersky Endpoint Security se comporta de la misma forma que lo hace cuando caduca una licencia comercial de la aplicación (la aplicación funciona sin actualizaciones y el servicio Kaspersky Security Network no está disponible).

Puede renovar la suscripción en el sitio web del proveedor de servicios.

Para visitar el sitio web del proveedor de servicios en la interfaz de la aplicación:

1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.
2. Haga clic en **Comunicarse con el proveedor de suscripciones**.

Puede actualizar el estado de la suscripción manualmente. Esto puede requerirse si se ha renovado la suscripción después del período de gracia y la aplicación no ha actualizado el estado de la suscripción automáticamente.



Renovación de suscripciones

Primeros pasos

Después de instalar Kaspersky Endpoint Security, puede administrar la aplicación usando las siguientes interfaces:

- Interfaz de la aplicación local.
- Consola de administración de Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Consola de administración de Kaspersky Security Center

Kaspersky Security Center le permite, de forma remota, tanto instalar y desinstalar como iniciar y detener Kaspersky Endpoint Security, configurar la aplicación, cambiar el conjunto de componentes de aplicación disponibles, añadir claves, e iniciar y detener actualizaciones y tareas de análisis.

La aplicación se puede administrar mediante Kaspersky Security Center utilizando el Complemento de administración de Kaspersky Endpoint Security.

Para obtener más información sobre cómo administrar la aplicación a través de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (en adelante, también denominada *Web Console*). Es una interfaz web para administrar un sistema de protección basado en aplicaciones de Kaspersky. Puede trabajar en Kaspersky Security Center Web Console mediante un navegador en cualquier dispositivo. Para obtener más información acerca de Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

Kaspersky Security Center Cloud Console (en adelante también llamado "*Cloud Console*") es una solución basada en la nube para proteger y administrar la red de una organización. Para obtener más información acerca de Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Web Console y Cloud Console le permiten realizar las siguientes acciones:

- Supervisar el estado del sistema de seguridad de su organización.
- Instalar aplicaciones de Kaspersky en los dispositivos conectados a la red.
- Administrar las aplicaciones instaladas.
- Ver informes sobre el estado del sistema de seguridad.

La administración de Kaspersky Endpoint Security a través de Web Console, Cloud Console y la Consola de administración de Kaspersky Security Center ofrece diferentes capacidades de administración. Los componentes y tareas disponibles también varían para las diferentes consolas.

Acerca del Complemento de administración de Kaspersky Endpoint Security para Windows

El Complemento de administración de Kaspersky Endpoint Security para Windows activa la interacción entre Kaspersky Endpoint Security y Kaspersky Security Center. El Complemento de administración permite administrar Kaspersky Endpoint Security utilizando directivas, tareas y la configuración local de la aplicación. El complemento web proporciona la interacción con Kaspersky Security Center Web Console.

La versión del complemento de administración puede diferir de la versión de la aplicación de Kaspersky Endpoint Security instalada en el equipo cliente. Si la versión instalada del complemento de administración tiene menos funcionalidad que la versión instalada de Kaspersky Endpoint Security, la configuración de las funciones ausentes no está regulada por el complemento de administración. El usuario puede modificar dicha configuración en la interfaz local de Kaspersky Endpoint Security.

De manera predeterminada, el complemento web no forma parte de la instalación de Kaspersky Security Center Web Console. El complemento web debe instalarse en un equipo que tenga instalado Kaspersky Security Center Web Console . Las funciones del complemento web quedan entonces disponibles para cualquier administrador que pueda acceder a Web Console con un navegador. Puede ver la lista de complementos web instalados en la interfaz de Web Console: (**Configuración de la consola** → **Complementos web**).

Si utiliza Kaspersky Endpoint Security como parte de la solución Kaspersky Endpoint Detection and Response Optimum, debe instalar el complemento de administración de Kaspersky Endpoint Detection and Response. Necesita el complemento de administración para mostrar los detalles de la alerta. *Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Por lo tanto, para crear tareas de respuesta a amenazas, necesita el complemento de administración de Kaspersky Endpoint Security y, para ver los detalles de la alerta, necesita el complemento de administración de EDR.

Instalación del complemento web

Puede instalar el complemento web de las siguientes maneras:

- Instale el complemento web mediante el Asistente de inicio rápido de Kaspersky Security Center Web Console.

  Web Console le pedirá que ejecute el Asistente de inicio rápido cuando se conecte Web Console al Servidor de administración por primera vez. También puede ejecutar el Asistente de inicio rápido en la interfaz de la Consola web (**Detección y despliegue** → **Despliegue y asignación** → **Asistente de inicio rápido**). El Asistente de inicio rápido le permitirá, asimismo, verificar si los complementos web instalados son los más recientes y descargar las actualizaciones que sean necesarias. Para obtener más información sobre el Asistente de inicio rápido de Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

- Instale el complemento web mediante la lista de paquetes de distribución disponibles en Web Console.

  Para instalar el complemento web, en la interfaz de Web Console, elija el paquete de distribución del complemento web de Kaspersky Endpoint Security: (**Configuración de la consola → Complementos web**). La lista de paquetes de distribución disponibles se actualiza automáticamente cada vez que se publican versiones nuevas de las aplicaciones de Kaspersky.

- Descargando el paquete de distribución a Web Console desde una ubicación externa.

  Para instalar el complemento web, añada el archivo ZIP correspondiente al paquete de distribución del complemento web de Kaspersky Endpoint Security en la interfaz de Web Console: (**Configuración de la consola → Complementos web**). El paquete de distribución del complemento web puede descargarse, por ejemplo, del sitio web de Kaspersky.

A partir de Kaspersky Endpoint Security 12.11 para Windows, el procedimiento de instalación del complemento web ha cambiado. El paquete de distribución ahora incluye dos complementos web: *Kaspersky Endpoint Security para Windows 14.2.0* y *Unified Protection and Management Plug-in*. Esto se debe a la transición a un solo complemento web unificado para administrar las aplicaciones de Kaspersky. El complemento web unificado permite crear una sola directiva para administrar varias aplicaciones de Kaspersky (por ejemplo, Kaspersky Endpoint Security para Windows, macOS y Linux). La transición al complemento web unificado puede requerir varias versiones. Una vez completada la transición, el paquete de distribución incluirá solo el *Unified Protection and Management Plug-in*.

Actualización del complemento de administración

Para actualizar el Complemento de administración de Kaspersky Endpoint Security para Windows, descargue la última versión del complemento (incluido en el kit de distribución) y ejecute el asistente de instalación del complemento.

Si hay una nueva versión del complemento web disponible, Web Console mostrará una notificación de *actualizaciones disponibles para complementos utilizados*. Puede actualizar la versión del complemento web desde esta notificación de Web Console. También puede buscar manualmente nuevas actualizaciones del complemento web en la interfaz de Web Console (**Configuración de la consola → Complementos web**). La versión anterior del complemento web se eliminará automáticamente durante la actualización.

Al actualizarse el complemento web, se guardan los elementos ya existentes (por ejemplo, directivas o tareas). La nueva configuración de elementos que implementa funciones nuevas de Kaspersky Endpoint Security aparecerá en elementos existentes y tendrá los valores predeterminados.

Puede actualizar el complemento web de las siguientes maneras:

- En la lista de complementos web en modo en línea.

  Para actualizar el complemento web, en la interfaz de Web Console, seleccione el paquete de distribución del complemento web de Kaspersky Endpoint Security (**Configuración de la consola → Complementos web**). Web Console busca actualizaciones disponibles en servidores de Kaspersky y descarga las que sean relevantes.

- Desde un archivo.

  Para actualizar el complemento web, en la interfaz de Web Console, elija el archivo ZIP del paquete de distribución del complemento web de Kaspersky Endpoint Security: (**Configuración de la consola → Complementos web**). El paquete de distribución del complemento web puede descargarse, por ejemplo, del sitio web de Kaspersky. Puede actualizar el complemento web de Kaspersky Endpoint Security únicamente a una versión más reciente. El complemento web no se puede actualizar a una versión previa.

Si se abre algún elemento (por ejemplo, una directiva o una tarea), el complemento web comprueba su información de compatibilidad. Si la versión del complemento web es igual o posterior a la especificada en la información de compatibilidad, puede cambiar la configuración de este elemento. De lo contrario, no podrá usar el complemento web para cambiar la configuración del elemento seleccionado. Se recomienda actualizar el complemento web.

Consideraciones especiales cuando se trabaja con distintas versiones de complementos de administración

Puede administrar Kaspersky Endpoint Security a través de Kaspersky Security Center solo si tiene un complemento de administración cuya versión sea igual o posterior a la versión especificada en la información relacionada con la compatibilidad de Kaspersky Endpoint Security con el complemento de administración. Puede ver la versión mínima requerida del complemento de administración en el archivo installer.ini incluido en el kit de distribución.

Si se abre algún elemento (por ejemplo, una directiva o una tarea), el complemento de administración comprueba su información de compatibilidad. Si la versión del complemento de administración es igual o superior a la especificada en la información de compatibilidad, puede cambiar la configuración de este elemento. De lo contrario, no podrá usar el complemento de administración para cambiar la configuración del elemento seleccionado. Se recomienda actualizar el complemento de administración.

Si el Complemento de administración de Kaspersky Endpoint Security está instalado en la Consola de administración, considere lo siguiente al instalar una nueva versión del Complemento de administración:

- La versión anterior del Complemento de administración de Kaspersky Endpoint Security se eliminará.
- La nueva versión del Complemento de administración de Kaspersky Endpoint Security admite la administración de la versión anterior de Kaspersky Endpoint Security para Windows en los equipos de los usuarios.
- Puede utilizar la nueva versión del complemento de administración para cambiar la configuración de directivas, tareas y otros elementos creados con la versión anterior del complemento.
- Para los parámetros nuevos, la nueva versión del complemento de administración asigna los valores predeterminados cuando se guarda una directiva, un perfil de directiva o una tarea por primera vez.

  Después de actualizar el complemento de administración, se recomienda comprobar y guardar los valores de la nueva configuración en directivas y perfiles de directiva. De no hacerlo así, los nuevos grupos de configuración de Kaspersky Endpoint Security en el equipo del usuario utilizarán los valores predeterminados y se podrán modificar (atributo ). Se recomienda comprobar la configuración, empezando por las directivas y los perfiles de directiva en el nivel superior de la jerarquía. También se recomienda utilizar la cuenta de usuario que tenga derechos de acceso a todas las áreas funcionales de Kaspersky Security Center.

  Para informarse sobre las nuevas funcionalidades de la aplicación, consulte las Notas de la versión o la ayuda de aplicación.

- Si se ha añadido un nuevo parámetro a un grupo de configuración en la nueva versión del complemento de administración, no cambiará el estado definido anteriormente para el atributo  de este grupo de configuración.

Consideraciones especiales al utilizar protocolos cifrados para interactuar con servicios externos

Kaspersky Endpoint Security y Kaspersky Security Center utilizan un canal de comunicación cifrado con TLS (Transport Layer Security) para trabajar con servicios externos de Kaspersky. Kaspersky Endpoint Security utiliza servicios externos para las siguientes funciones:

- actualización de las bases de datos y módulos de la aplicación;
- activación de la aplicación con un código de activación (activación 2.0);
- uso de Kaspersky Security Network.

El uso de TLS protege la aplicación al proporcionar las siguientes características:

- Cifrado. Los contenidos de los mensajes son confidenciales y no se divulgan a terceros.
- Integridad. El destinatario del mensaje está seguro de que el contenido del mensaje no se ha modificado desde que el remitente lo reenvió.
- Autenticación. El destinatario está seguro de que la comunicación se establece solo con un servidor de Kaspersky de confianza.

Kaspersky Endpoint Security utiliza certificados de clave pública para la autenticación del servidor. Se requiere una Public Key Infrastructure (PKI) para trabajar con certificados. Una Autoridad de certificación es parte de una PKI. Kaspersky utiliza su propia Autoridad de certificación porque los servicios de Kaspersky son muy técnicos y no públicos. En este caso, cuando se revocan los certificados raíz de Thawte, VeriSign, GlobalTrust y otros, Kaspersky PKI permanece en condiciones de servicio y sin interrupciones.

Kaspersky Endpoint Security considera que los entornos que tienen MITM (herramientas de software y hardware que admiten el análisis del protocolo HTTPS) no son seguros. Es posible que se produzcan errores al trabajar con los servicios de Kaspersky. Por ejemplo, puede haber errores relacionados con el uso de Self-Signed Certificate. Estos errores pueden ocurrir porque una herramienta de inspección HTTPS de su entorno no reconoce a Kaspersky PKI. Para solucionar estos problemas, debe configurar exclusiones para interactuar con servicios externos.

Interfaz de la aplicación



Ventana principal de la aplicación

Supervisión	• **Informes**. Ver eventos que ocurrieron durante el funcionamiento de la aplicación, componentes individuales y tareas. • **Copia de seguridad**. Ver una lista de copias guardadas de archivos infectados que la aplicación ha eliminado. • **Tecnologías de detección de amenazas**. Ver información sobre tecnologías de detección de amenazas y la cantidad de amenazas detectadas por estas tecnologías. • **Kaspersky Security Network**. Estado de la conexión entre Kaspersky Endpoint Security y Kaspersky Security Network, y estadísticas globales de KSN. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, los servicios de KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web que se analicen, así como sobre la categoría y reputación de los archivos analizados. • **Supervisión de la Actividad de Aplicaciones**. Ver información sobre el funcionamiento de las aplicaciones instaladas. El monitor de actividad de aplicaciones realiza un seguimiento del archivo, el registro y los eventos del sistema asociados con una aplicación. • **Monitor de red**. Ver información sobre la actividad de red del equipo en tiempo real. • **Monitor de cifrado**. Supervisa el proceso de cifrado o descifrado del disco en tiempo real. El Monitor de cifrado está disponible si está instalado el componente Cifrado de disco de Kaspersky o el componente Cifrado de unidad BitLocker.
Seguridad	Estado operativo de los componentes instalados. También puede proceder a configurar componentes o ver informes.
Actualización	Administrar las tareas de actualización de Kaspersky Endpoint Security. Puede actualizar las bases de datos antivirus y los módulos de la aplicación y revertir la última actualización. Un administrador puede ocultar la sección al usuario o restringir la gestión de tareas.
Tareas	Administrar las tareas de análisis de Kaspersky Endpoint Security. Puede ejecutar un análisis antimalware y una comprobación de integridad de la aplicación. Un administrador puede ocultar tareas a un usuario o restringir la gestión de tareas.
Licencia	Licencias de la aplicación. Puede adquirir una licencia, activar la aplicación o renovar una suscripción. También puede ver información sobre la licencia actual.

	Configurar parámetros de la aplicación. Un administrador puede prohibir cambios en la configuración de Kaspersky Security Center.
	Información sobre la aplicación: versión actual de Kaspersky Endpoint Security, fecha de publicación de la base de datos, clave y otra información. También puede dirigirse a los recursos informativos de Kaspersky que ofrecen información útil y recomendaciones, además de respuestas a preguntas frecuentes sobre la manera de comprar, instalar y usar la aplicación.
	Mensajes que contienen información sobre actualizaciones disponibles y solicitudes de acceso a archivos y dispositivos cifrados.

Icono de la aplicación en el área de notificaciones de la barra de tareas

Inmediatamente después de la instalación de Kaspersky Endpoint Security, su icono aparece en el área de notificaciones de la barra de tareas de Microsoft Windows.

Si el icono de la aplicación en el área de notificaciones de la barra de tareas está oculto, el administrador ha desactivado la visualización de la interfaz de la aplicación en la directiva.

El icono tiene las siguientes finalidades:

- Indica la actividad de la aplicación.
- Actúa como acceso directo al menú contextual y la ventana principal de la aplicación.

El funcionamiento de la aplicación se representa a través de los siguientes iconos de estado:

- El icono indica que los componentes de protección fundamentales de la aplicación están activados. Kaspersky Endpoint Security mostrará una advertencia si el usuario necesita realizar una acción, por ejemplo, reiniciar el equipo después de actualizar la aplicación.
- El icono indica que los componentes de protección fundamentales de la aplicación están desactivados o han sufrido un error de funcionamiento. Los componentes de protección pueden sufrir un error de funcionamiento, por ejemplo, si la licencia ha caducado o como resultado de un error de la aplicación. Kaspersky Endpoint Security mostrará una advertencia con una descripción del problema en la protección del equipo.

El menú contextual del icono de la aplicación contiene los siguientes elementos:

- **Kaspersky Endpoint Security para Windows**. Abre la ventana principal de la aplicación. En esta ventana puede ajustar el funcionamiento de los componentes y las tareas de la aplicación, así como ver las estadísticas de archivos procesados y amenazas detectadas.
- **Pausar la protección/Reanudar la protección**. Permite poner en pausa todos los componentes de protección y control que no estén marcados con un candado () en la directiva. Recomendamos desactivar la directiva de Kaspersky Security Center antes de realizar esta operación.

  Antes de pausar los componentes de protección y control, la aplicación le pedirá la contraseña de acceso a Kaspersky Endpoint Security (contraseña de cuenta o contraseña temporal). A continuación, podrá seleccionar la duración de la pausa. Los componentes pueden quedar en pausa por un tiempo específico, hasta que ocurra un reinicio o hasta que el usuario decida reanudarlos.

  Este elemento del menú contextual está disponible si la protección con contraseña está habilitada. Para que los componentes de protección y control comiencen a funcionar nuevamente, haga clic en **Reanudar la protección** en el menú contextual de la aplicación.

Pausar los componentes de protección y control no afecta el desempeño de las tareas de actualización y análisis antimalware. Tampoco suspende el uso de Kaspersky Security Network por parte de la aplicación.

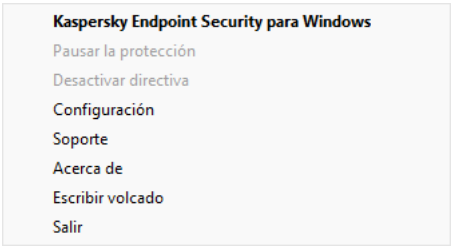
- **Desactivar directiva/Activar directiva**. Desactivar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse. Si la directiva está desactivada, será necesario escribir la contraseña de acceso a Kaspersky Endpoint Security (contraseña de cuenta o contraseña temporal). Este elemento del menú contextual está disponible si la protección con contraseña está habilitada. Para habilitar la directiva, seleccione **Activar directiva** en el menú contextual de la aplicación.

- **Configuración**. Permite abrir la ventana de configuración de la aplicación.

- **Soporte**. Esto abre una ventana que contiene la información necesaria para ponerse en contacto con el Soporte técnico de Kaspersky.

- **Acerca de**. Este elemento abre una ventana de información con detalles sobre la aplicación.

- **Salir**. Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este menú contextual, la aplicación se descarga de la RAM del equipo.



Menú contextual del icono de la aplicación

Interfaz simplificada de la aplicación

Si una directiva de Kaspersky Security Center configurada para visualizar la interfaz simplificada de la aplicación se aplica a un equipo cliente con Kaspersky Endpoint Security instalado, la ventana principal de la aplicación no está disponible en este equipo cliente. Haga clic con el botón secundario para abrir el menú contextual del icono de Kaspersky Endpoint Security (consulte la siguiente figura) que contiene los elementos siguientes:

- **Desactivar directiva/Activar directiva**. Desactivar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse. Si la directiva está desactivada, será necesario escribir la contraseña de acceso a Kaspersky Endpoint Security (contraseña de cuenta o contraseña temporal). Este elemento del menú contextual está disponible si la protección con contraseña está habilitada. Para habilitar la directiva, seleccione **Activar directiva** en el menú contextual de la aplicación.

- **Tareas**. Lista desplegable que contiene los siguientes elementos:

  - **Comprobación de integridad de la aplicación**.

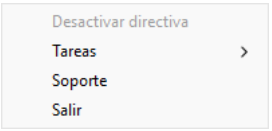
  - **Restauración de las bases de datos a su versión anterior**.

  - **Análisis completo**.

  - **Análisis personalizado**.

- **Análisis de áreas críticas**.
- **Actualización**.

- **Soporte**. Esto abre una ventana que contiene la información necesaria para ponerse en contacto con el Soporte técnico de Kaspersky.
- **Salir**. Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este menú contextual, la aplicación se descarga de la RAM del equipo.



Menú contextual del icono de la aplicación al mostrar la interfaz simplificada

Configuración de la visualización de la interfaz de la aplicación

Puede configurar el modo de visualización de la interfaz de la aplicación para un usuario. El usuario puede interactuar con la aplicación de las siguientes formas:

- **Simplificada**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un icono en el área de notificación de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security en forma limitada a través del menú contextual de este icono. Kaspersky Endpoint Security también muestra únicamente notificaciones que requieren la acción del usuario sobre el icono de la aplicación.
- **Completa**. En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al icono ubicado en el área de notificaciones de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
- **No mostrar interfaz de usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El icono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

Cómo configurar el modo de visualización de la interfaz de la aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Interfaz**.

4. En el bloque **Interacción con el usuario**, configure cómo se mostrará la interfaz de la aplicación:

   - **Mostrar interfaz de usuario**. En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al icono ubicado en el área de notificaciones de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono. Si es necesario, puede activar la funcionalidad **Ocultar la sección del monitor de actividad de la aplicación** para ocultar datos sobre la actividad de la aplicación en el equipo, restringiendo así el acceso del usuario a la herramienta Supervisión de la actividad de aplicaciones.

   - **Mostrar interfaz simplificada**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un icono en el área de notificación de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security en forma limitada a través del menú contextual de este icono. Kaspersky Endpoint Security también muestra únicamente notificaciones que requieren la acción del usuario sobre el icono de la aplicación.

   - **No mostrar interfaz de usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El icono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

5. Guarde los cambios.

Cómo configurar el modo de visualización de la interfaz de la aplicación en la Consola web

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Interacción del usuario**.

5. En el bloque **Visibilidad para usuarios**, configure cómo se mostrará la interfaz de la aplicación:

   - **Mostrar interfaz de usuario**. Si esta función está desactivada, no se muestran signos de funcionamiento de Kaspersky Endpoint Security en un equipo cliente. El icono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

   - **Simplificada**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un icono en el área de notificación de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security en forma limitada a través del menú contextual de este icono. Kaspersky Endpoint Security también muestra únicamente notificaciones que requieren la acción del usuario sobre el icono de la aplicación.

   - **Completa**. En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al icono ubicado en el área de notificaciones de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.

   - **Ocultar la sección del monitor de actividad de la aplicación**. Si desea ocultar la información de la actividad de la aplicación en el equipo de un usuario, puede restringir el acceso del usuario a la herramienta Supervisión de la actividad de aplicaciones.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Preparar la aplicación para su uso

Una vez que se complete la implementación de Kaspersky Endpoint Security en los equipos cliente, deberá realizar las siguientes tareas para poder trabajar con la aplicación desde Kaspersky Security Center Web Console:

- Crear y configurar una directiva.

  Puede usar directivas para aplicar parámetros de Kaspersky Endpoint Security idénticos a todos los equipos cliente de un grupo de administración. El Asistente de inicio rápido de Kaspersky Security Center crea una directiva para Kaspersky Endpoint Security automáticamente.

- Crear las tareas *Actualización de las bases de datos y módulos de la aplicación* y *Análisis antimalware*.

  La tarea *Actualización de las bases de datos y módulos de la aplicación* permite que los equipos siempre cuenten con lo último en protección. Cuando se ejecuta esta tarea, Kaspersky Endpoint Security actualiza sus bases de datos antivirus y sus módulos de software. La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

  La tarea *Análisis antimalware* se requiere para detectar virus y otras clases de malware a tiempo. La tarea *Análisis antimalware* se debe crear manualmente.

  Cómo crear una tarea Análisis antimalware en la Consola de administración (MMC)

  1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

     Se abre la lista de tareas.

  2. Haga clic en **Nueva tarea**.

  El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Análisis antimalware**.

Paso 2. Cobertura del análisis

Crear la lista de objetos que Kaspersky Endpoint Security analizará mientras realiza una tarea de análisis.

Paso 3. Acción de Kaspersky Endpoint Security

Seleccione la acción al detectar una amenaza:

- **Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

- **Desinfectar; informar si falla la desinfección**. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección falla, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.

- **Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.

- **Ejecutar la desinfección avanzada de inmediato**. Cuando esta casilla está activada, Kaspersky Endpoint Security utiliza la tecnología de desinfección avanzada para tratar las amenazas activas durante el análisis.

  El objetivo de *la tecnología de desinfección avanzada* consiste en eliminar del sistema operativo las aplicaciones maliciosas que ya han puesto en marcha sus procesos en la memoria RAM y que impiden que Kaspersky Endpoint Security las elimine por medio de otros métodos. Como consecuencia de ello, se neutraliza la amenaza. Cuando la desinfección avanzada está en curso, se recomienda que no ponga en marcha ningún proceso nuevo ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada emplea un número considerable de recursos del sistema operativo, lo que puede ralentizar el resto de las aplicaciones. Cuando se haya completado la desinfección avanzada, Kaspersky Endpoint Security reiniciará el equipo sin solicitar la confirmación del usuario.

- **Ejecutar solo cuando el equipo está inactivo**. Inicio pospuesto de la tarea cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.

Paso 4. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.

- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.

- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 5. Selección de la cuenta para ejecutar la tarea

Seleccione una cuenta para ejecutar la tarea *Análisis antimalware*. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local. Si la cobertura del análisis incluye unidades de red u otros objetos con acceso restringido, seleccione una cuenta de usuario con los derechos de acceso suficientes.

Paso 6. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o después de descargar bases de datos antivirus al repositorio.

Paso 7. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Análisis completo diario*.

Paso 8. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, la tarea de análisis antimalware se ejecutará en los equipos de usuario según la planificación especificada.

Cómo crear una tarea de Análisis antimalware en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Análisis antimalware**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Análisis semanal*).

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Para configurar la planificación de la tarea, abra las propiedades de la tarea.

   Se recomienda programar la tarea para que se ejecute al menos una vez por semana.

8. Active la casilla ubicada junto a la tarea.

9. Haga clic en **Iniciar**.

   Puede supervisar el estado de la tarea y el número de dispositivos en los que se completó correctamente o con errores.

Como resultado, la tarea de análisis antimalware se ejecutará en los equipos de usuario según la planificación especificada.

- Optimizar el rendimiento de Kaspersky Endpoint Security.

Gestión de directivas

Una *directiva* es un grupo de valores de configuración que se han definido para una aplicación y un grupo de administración específicos. Es posible configurar más de una directiva, cada una con valores distintos, para una misma aplicación. La aplicación puede funcionar con configuraciones distintas asociadas a grupos de administración distintos. Cada grupo puede tener su propia directiva para una aplicación.

Cada configuración de directiva tiene el atributo ("candado"). El estado de este atributo determina si la configuración se transmitirá a los dispositivos administrados del grupo de administración:

- Si el "candado" está abierto (), el valor de esta configuración no se transmitirá a los dispositivos administrados. La configuración se puede modificar en la interfaz local de la aplicación. Tales configuraciones se denominan *desbloqueadas*.

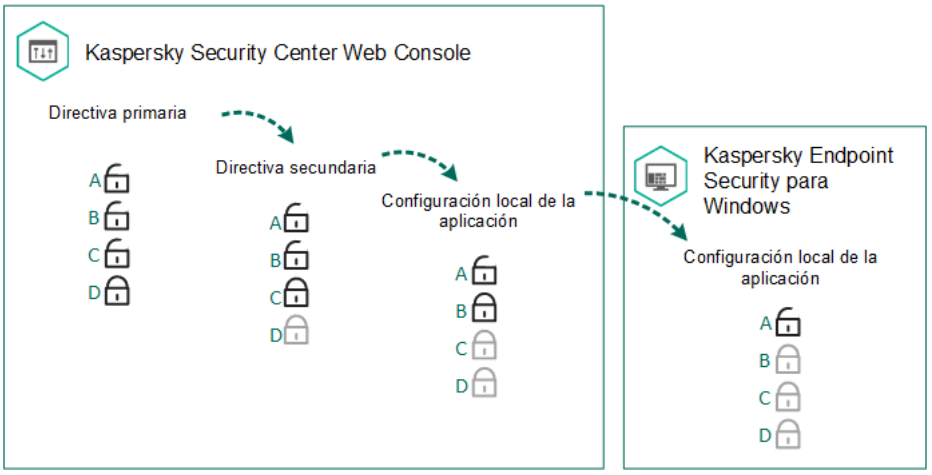
- Si el "candado" está cerrado (), el valor de esta configuración se transmitirá a los dispositivos administrados y se aplicará en ellos. Tales configuraciones se denominan *bloqueadas*. Las configuraciones bloqueadas no se pueden modificar en la interfaz local de la aplicación.

La configuración de una directiva se envía a los equipos cliente a través del Agente de red durante la *sincronización*. De manera predeterminada, el Servidor de administración ejecuta el proceso de sincronización en cuanto se modifica una directiva. El puerto UDP 15000 en el equipo cliente se usa para la sincronización. El Servidor de administración realiza una sincronización cada 15 minutos de forma predeterminada. Si la sincronización falla después de cambiar la configuración de la directiva, el siguiente intento de sincronización se realizará según la planificación configurada.

Herencia de configuración

Las directivas, como los grupos de administración, se organizan en una jerarquía. La *directiva secundaria* es una directiva para niveles de jerarquía anidados, que es una directiva para grupos de administración anidados y servidores de administración secundarios.

De forma predeterminada, una directiva secundaria hereda la configuración de la directiva principal. Si la configuración de la directiva principal tiene el atributo (🔒 "candado cerrado"), el valor de dicha configuración se anulará en directivas secundarias y en las configuraciones de la aplicación local de acuerdo con la directiva principal, y la configuración se bloqueará. Si es necesario, puede deshabilitar la herencia de la configuración de la directiva principal. Este tipo de directiva no afecta a las que se han creado para grupos de administración de otros niveles de la jerarquía.



Herencia de configuración

Los derechos de acceso a la configuración de las directivas (lectura, escritura, ejecución) se especifican para cada usuario que tenga acceso al servidor de administración de Kaspersky Security Center y, por separado, para cada cobertura funcional de Kaspersky Endpoint Security. Para configurar los derechos de acceso a la configuración de la directiva, vaya a la sección **Seguridad** de la ventana de propiedades del Servidor de administración de Kaspersky Security Center (de manera predeterminada, esta sección está oculta en la interfaz de la consola).

Revisiones de directivas

Kaspersky Security Center rastrea las modificaciones de las directivas y crea revisiones. Una *revisión* es un conjunto de parámetros modificados guardados por el usuario. Las revisiones le permiten comparar y revertir los cambios en los parámetros de la directiva. Además del conjunto de parámetros modificados, la revisión incluye información sobre el usuario que realizó los cambios, así como la hora, la dirección IP, comentarios del usuario y otros datos relevantes.

Para ver el registro de revisiones, abra las propiedades de la directiva y vaya a la sección **Historial de revisión**. Para obtener más información sobre cómo trabajar con revisiones, consulte la Ayuda de Kaspersky Security Center.

Creación de una directiva

Al crear una directiva, el asistente sugiere configuraciones relevantes para el modo seleccionado. Por ejemplo, para el modo Light Agent, debe añadir un Servidor de protección (SVM). Al usar la aplicación para proteger un servidor SQL, debe añadir exclusiones de análisis predefinidas para asegurarse de que no se interfiera con el funcionamiento del servidor. El asistente sugiere configuraciones de directiva relevantes después de seleccionar un modo. A continuación, puede editar esta configuración en las propiedades de la directiva.

Cómo crear una directiva en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, seleccione la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Haga clic en **Nueva directiva**.

   El Asistente de directivas se inicia.
5. Siga las instrucciones del Asistente de directivas.

Paso 1. Selección de la aplicación para crear la directiva de grupos

Seleccione la aplicación **Kaspersky Endpoint Security para Windows (14.2)**.

Paso 2. Nombrar la directiva de grupo

Introduzca un nombre para la directiva de grupo; por ejemplo, *Directiva de la oficina*.

También puede crear nuevas directivas basadas en las directivas existentes mediante el Asistente de directivas. Para hacerlo, al especificar el nombre de la directiva de grupo, marque la casilla de verificación **Usar configuración de directivas para una versión anterior de la aplicación**. El asistente también permite crear una directiva de Kaspersky Endpoint Security (KES) basada en una directiva de una solución diferente; por ejemplo, Kaspersky Security for Windows Server (KSWS) o Kaspersky Security for Virtualization Light Agent for Windows

Paso 3. Participación en Kaspersky Security Network

Lea y acepte los términos de la Declaración de Kaspersky Security Network (KSN).

Paso 4. Selección del modo de uso de la aplicación en equipos

Según el uso previsto de Kaspersky Endpoint Security, puede configurar una directiva para los siguientes modos de aplicación:

- Modo estándar para proteger hosts

En este modo, puede seleccionar cómo desea configurar la directiva:

- **Crear una directiva con la configuración predeterminada**. La configuración predeterminada se considera óptima. Los expertos de Kaspersky recomiendan esta configuración. La configuración predeterminada proporciona el nivel de protección recomendado y el uso óptimo de los recursos.

- **Cambiar la configuración de la directiva en el asistente**. Este método permite administrar la configuración de la directiva paso a paso mediante un asistente. También puede administrar la configuración de directivas mediante un archivo de configuración de la aplicación (consulte el siguiente paso).

- Endpoint Detection and Response Agent para protección contra amenazas avanzadas y ataques selectivos.

  Endpoint Detection and Response Agent es una aplicación que se instala en estaciones de trabajo y servidores individuales en la infraestructura de TI de la organización para dar soporte a las soluciones de Detection and Response de Kaspersky: En el siguiente paso, debe seleccionar una solución para la integración de EDR Agent.

- Light Agent para proteger entornos virtuales.

  Para usar la aplicación en modo de Light Agent, debe configurar una conexión con una máquina virtual SVM. Esta configuración es necesaria para que la aplicación funcione en modo Light Agent.

Kaspersky Endpoint Security proporciona una directiva común para todos los modos de aplicación y tipos de sistema operativo. Esto significa que la directiva cubre todo el conjunto de configuraciones. Sin embargo, la aplicación puede ignorar algunas de las configuraciones de la directiva porque Kaspersky Endpoint Security se implementa en un modo en el que algunas funciones no están disponibles. Por ejemplo, al usar la aplicación en el modo Endpoint Detection and Response Agent, solo están disponibles las configuraciones que son relevantes para la integración con las soluciones de Kaspersky Detection and Response y para la integración con KUMA.

Recomendamos usar diferentes directivas para diferentes modos y tipos de sistema operativo.

Paso 5. Importar la configuración

Este paso está disponible si selecciona la configuración manual de la directiva en el paso 4.

Puede crear una directiva basada en la configuración de Kaspersky Endpoint Security desde un archivo de configuración de CFG. El Asistente para nueva directiva no admite archivos de configuración cifrados. Al exportar el archivo de configuración, omita el paso de cifrado del archivo.

Al importar un archivo de configuración CFG de la aplicación, no todos los parámetros de la directiva están disponibles para el asistente. Por ejemplo, la configuración de la aplicación carece de perfiles de la directiva. Si desea transferir todas las configuraciones y perfiles a la directiva, puede importar otra directiva de un archivo KLP.

Al importar un archivo de configuración, Kaspersky Endpoint Security no transfiere contraseñas de contenedores criptográficos. Si utiliza la autenticación bidireccional al conectarse a los servidores, debe especificar las contraseñas del contenedor criptográfico desde cero.

Pasos 6-10. Configuración de la directiva

Este paso está disponible si selecciona la configuración manual de la directiva en el paso 4.

Siga los pasos para administrar la configuración de la directiva.

Paso 11. Configurar la zona de confianza

Configurar la zona de confianza. Puede añadir exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. Las exclusiones de análisis y aplicaciones de confianza predefinidas también pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en modo Light Agent en entornos virtuales Citrix y VMware.

Paso 12. Seleccionar el estado de la directiva

- **Activa**. Después de la siguiente sincronización, la directiva se utilizará como directiva activa en el equipo.

  Los valores de la directiva activa se guardan en los equipos cliente cuando se realiza la sincronización. Un equipo puede estar sujeto a una sola directiva por vez; por ello, solo una directiva puede estar activa por grupo.

- **Inactiva**. Directiva de reserva. Puede convertirse en la directiva activa cuando resulta necesario.

  El número de directivas inactivas que pueden crearse es ilimitado. Estas no afectan la configuración de las aplicaciones instaladas en los equipos de la red. Están pensadas para usarse en situaciones de emergencia, como brotes de virus y otros casos. Por ejemplo, ante un ataque mediante unidades flash, puede activarse una directiva que impida el uso de unidades flash. En tal caso, la directiva activa cambia de estado a inactiva automáticamente.

- **Fuera de la oficina**. La directiva se activa cuando un equipo abandona el perímetro de la red de la organización.

Finalice el asistente.

Cómo crear una directiva en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en **Añadir**.

   El Asistente de directivas se inicia.
3. Seleccione Kaspersky Endpoint Security y haga clic en **Siguiente**.
4. Lea y acepte los términos de la Declaración de Kaspersky Security Network (KSN) y haga clic en **Siguiente**.

5. Seleccione el modo de la aplicación:

   - Modo estándar para proteger estaciones de trabajo y servidores
   - Endpoint Detection and Response Agent para protección contra amenazas avanzadas y ataques selectivos.

     Si selecciona este modo, puede crear una directiva para integrar el equipo con las soluciones de Kaspersky Detection and Response. El asistente le solicita que configure la integración para Kaspersky Managed Detection and Response y, a continuación, Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent para proteger entornos virtuales.

     Si selecciona este modo, en el siguiente paso debe configurar la conexión al Servidor de protección (SVM). Esta configuración es necesaria para que la aplicación funcione en modo Light Agent.

   Kaspersky Endpoint Security proporciona una directiva común para todos los modos de aplicación y tipos de sistema operativo. Esto significa que la directiva cubre todo el conjunto de configuraciones. Sin embargo, la aplicación puede ignorar algunas de las configuraciones de la directiva porque Kaspersky Endpoint Security se implementa en un modo en el que algunas funciones no están disponibles. Por ejemplo, al usar la aplicación en el modo Endpoint Detection and Response Agent, solo están disponibles las configuraciones que son relevantes para la integración con las soluciones de Kaspersky Detection and Response y para la integración con KUMA.

   Recomendamos usar diferentes directivas para diferentes modos y tipos de sistema operativo.

6. Configurar la zona de confianza. Puede añadir exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. Las exclusiones de análisis y aplicaciones de confianza predefinidas también pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en modo Light Agent en entornos virtuales Citrix y VMware.

7. En la pestaña **General**, puede realizar las siguientes acciones:

   - Cambiar el nombre de la directiva.
   - Seleccionar el estado de la directiva:

     - **Activa**. Después de la siguiente sincronización, la directiva se utilizará como directiva activa en el equipo.

       Los valores de la directiva activa se guardan en los equipos cliente cuando se realiza la sincronización. Un equipo puede estar sujeto a una sola directiva por vez; por ello, solo una directiva puede estar activa por grupo.
     - **Inactiva**. Directiva de reserva. Puede convertirse en la directiva activa cuando resulta necesario.

       El número de directivas inactivas que pueden crearse es ilimitado. Estas no afectan la configuración de las aplicaciones instaladas en los equipos de la red. Están pensadas para usarse en situaciones de emergencia, como brotes de virus y otros casos. Por ejemplo, ante un ataque mediante unidades flash, puede activarse una directiva que impida el uso de unidades flash. En tal caso, la directiva activa cambia de estado a inactiva automáticamente.
     - **Fuera de la oficina**. La directiva se activa cuando un equipo abandona el perímetro de la red de la organización.

- Configurar la herencia de configuración:

  - **Heredar configuración de la directiva principal**. Si activa este interruptor, los valores de configuración de la directiva se tomarán de la directiva de mayor nivel jerárquico. La configuración de la directiva no se puede editar si está establecida para la directiva principal.

  - **Forzar la herencia de la configuración en las directivas secundarias**. Si el botón de alternancia está activado, los valores de la configuración de directiva se propagan a las directivas secundarias. En las propiedades de la directiva secundaria, el interruptor **Heredar configuración de la directiva principal** se activará automáticamente y no se podrá desactivar. La configuración de directiva secundaria se hereda de la directiva primaria, excepto para los ajustes marcados con . Los ajustes de la directiva secundaria no se pueden modificar si está configurado para la directiva principal.

8. En la pestaña **Configuración de la aplicación** puede modificar la configuración de la directiva de Kaspersky Endpoint Security.

9. Finalice el asistente.

La configuración de Kaspersky Endpoint Security se aplicará en los equipos cliente cuando se realice la siguiente sincronización. Puede ver información sobre la directiva que se aplica al equipo en la interfaz de Kaspersky Endpoint Security haciendo clic en el botón en la pantalla principal (por ejemplo, el nombre de la directiva). Para hacerlo, en la configuración de la directiva del Agente de red, tiene que activar la recepción de datos de directiva ampliados. Para obtener más información sobre una directiva del Agente de red, consulte la Ayuda de Kaspersky Security Center.

Exportar e importar una directiva

Kaspersky Endpoint Security permite exportar una directiva con su configuración y perfiles a un archivo KLP. A continuación, puede utilizar la función de exportación/importación de directivas para hacer una copia de seguridad de las directivas, migrar las directivas a otro servidor o, por ejemplo, para migrar directivas de Kaspersky Security Center Windows a Kaspersky Security Center Linux. Para obtener más información sobre la administración de directivas, consulte la Ayuda de Kaspersky Security Center.

Cómo exportar e importar una directiva en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

3. En el espacio de trabajo, seleccione la pestaña **Directivas**.

4. Para exportar una directiva:

   a. Haga clic en la directiva que desea exportar.

   b. Haga clic en el vínculo **Exportar directiva al archivo** en la parte derecha de la ventana.

   c. En la ventana que se abre, especifique el nombre del archivo KLP al que desee exportar la directiva y seleccione la carpeta en la que guardar el archivo.

   d. Guarde el archivo.

5. Para importar una directiva:

    a. Haga clic en **Importar directiva desde archivo**.

    b. En la ventana que se abre, seleccione la el archivo de directiva de KLP que desea importar.

    c. Abra el archivo.

    Esto agrega una nueva directiva con el estado *Directiva inactiva*.

Cómo exportar e importar la directiva en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Para exportar una directiva:

    a. Seleccione la casilla de verificación que hay junto a la directiva que desea exportar.

    b. Haga clic en el botón **Exportar**.

    c. En la ventana que se abre, especifique el nombre del archivo KLP al que desee exportar la directiva y seleccione la carpeta en la que guardar el archivo.

    d. Guarde el archivo.

3. Para importar una directiva:

    a. Haga clic en **Importar**.

    b. Seleccione el archivo de directiva de KLP que desea importar.

    c. Una vez que la directiva se haya procesado correctamente, seleccione el grupo de administración al que desea aplicarla.

    d. Haga clic en el botón **Completar** para terminar de importar la directiva.

    Esto agrega una nueva directiva con el estado *Inactiva*.

Indicador de nivel de seguridad

El indicador de nivel de seguridad se muestra en la parte superior de la ventana de propiedades de la directiva. El indicador puede tener uno de estos valores:

- **Nivel de protección alto**. El indicador toma este valor y se pone verde si todos los componentes de las siguientes categorías están activados:
    - **Crítico**. Esta categoría incluye los componentes siguientes:
        - Protección frente a amenazas en archivos.
        - Detección de comportamiento.
        - Prevención de exploits.

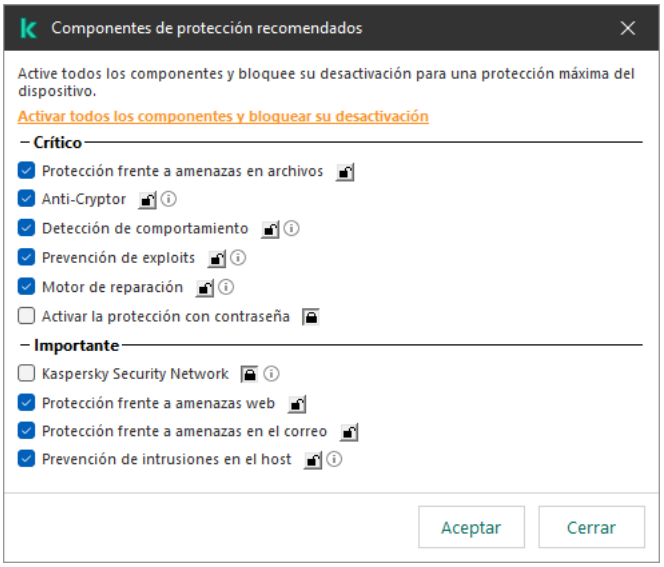
- Motor de reparación.
- Protección de los servicios de la aplicación contra la administración externa.

- **Importante**. Esta categoría incluye los componentes siguientes:
  - Kaspersky Security Network.
  - Protección frente a amenazas web.
  - Protección frente a amenazas en el correo.
  - Prevención de intrusiones en el host.
  - Protección con contraseña.

- **Nivel de protección medio**. El indicador toma este valor y se pone amarillo si uno de los componentes de importantes está desactivado.
- **Nivel de protección bajo**. El indicador toma este valor y se pone rojo en uno de los casos siguientes:
  - Un componente crítico (o varios) está(n) desactivado(s).
  - Dos componentes importantes (o más) están desactivados.

Si el indicador tiene el valor **Nivel de protección medio** o **Nivel de protección bajo**, a la derecha del indicador aparece un enlace, que abre la ventana **Componentes de protección recomendados**. En esta ventana puede activar cualquiera de los componentes de protección recomendados.

Después de actualizar la aplicación, el indicador del nivel de protección puede indicar un nivel de protección más bajo que antes de la actualización. Esto sucede porque la versión más reciente de la aplicación introduce nuevos componentes o funciones que son importantes para la seguridad del equipo. Después de actualizar la aplicación, debe administrar la nueva configuración para asegurarse de que el nivel de protección siga siendo alto.



Indicador de nivel de seguridad de la directiva

Gestión de tareas

Puede crear los siguientes tipos de tareas para administrar Kaspersky Endpoint Security mediante Kaspersky Security Center:

- Tareas locales configuradas para un equipo cliente individual.
- Tareas de grupo configuradas para equipos cliente incluidos en grupos de administración.
- Tareas para una selección de equipos.

Puede crear cualquier cantidad de tareas de grupo, tareas para una selección de equipos o tareas locales. Para más información sobre cómo trabajar con grupos de administración y selecciones de equipos, consulte la Ayuda en línea de Kaspersky Security Center.

Kaspersky Endpoint Security admite las siguientes tareas:

- **Análisis antimalware**. Kaspersky Endpoint Security analiza las áreas del equipo que se han especificado en la configuración de tareas para virus y otras amenazas. La tarea *Análisis antimalware*, necesaria para usar Kaspersky Endpoint Security, se crea al utilizar el Asistente de inicio rápido. Se recomienda programar la tarea para que se ejecute al menos una vez por semana.
- **Añadir clave**. Kaspersky Endpoint Security añade una clave que le permite activarse, así como una clave adicional. Antes de ejecutar la tarea, asegúrese de que el número de equipos en los que la tarea vaya a ejecutarse no supere el número permitido por la licencia.
- **Cambiar componentes de la aplicación**. Kaspersky Endpoint Security instala o elimina componentes en equipos cliente según la lista de componentes especificados en la configuración de la tarea. El componente Protección frente a amenazas en archivos no puede eliminarse. La óptima elección de componentes de Kaspersky Endpoint Security ayuda a hacer un buen uso de los recursos del equipo.
- **Inventario**. Kaspersky Endpoint Security recibe información sobre todos los archivos ejecutables de aplicaciones almacenados en los equipos. La tarea *Inventario* se ejecuta usando el componente Control de aplicaciones. Si Control de aplicaciones no está instalado, la tarea finaliza con un error.
- **Actualización de las bases de datos y módulos de la aplicación**. Kaspersky Endpoint Security actualiza sus bases de datos y módulos. La tarea *Actualización de las bases de datos y módulos de la aplicación*, necesaria para usar Kaspersky Endpoint Security, se crea al utilizar el Asistente de inicio rápido. Recomendamos definir una planificación para que la tarea se ejecute al menos una vez al día.
- **Eliminación de datos**. Kaspersky Endpoint Security elimina archivos y carpetas de los equipos de los usuarios en forma inmediata o cuando no ha habido conexión con Kaspersky Security Center en mucho tiempo.
- **Revertir actualización**. Kaspersky Endpoint Security revierte la última actualización de sus bases de datos y módulos. Esto puede ser necesario, por ejemplo, cuando las bases de datos nuevas contienen datos incorrectos y Kaspersky Endpoint Security bloquea una aplicación segura en consecuencia.

- **Comprobación de integridad de la aplicación**. Kaspersky Endpoint Security analiza los archivos que forman parte de la aplicación, comprueba si tienen daños o modificaciones y verifica sus firmas digitales.

- **Administrar cuentas del Agente de autenticación**. Kaspersky Endpoint Security configura los ajustes de la cuenta del Agente de autenticación. Se necesita un Agente de autenticación para trabajar con unidades cifradas. Antes de que se cargue el sistema operativo, el usuario debe completar la autenticación con el Agente.

Si la aplicación funciona como parte de la solución Endpoint Detection and Response de Kaspersky, puede ejecutar tareas adicionales como acciones de respuesta de detección (responses). Por ejemplo, puede finalizar procesos de forma remota mediante la tarea *Terminar proceso*.

Las tareas se ejecutarán en un equipo únicamente si Kaspersky Endpoint Security está en funcionamiento.

Crear una tarea

Cómo crear una tarea en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. Seleccione la carpeta **Tareas** en el árbol de la consola de administración.
3. Haga clic en **Nueva tarea**.

   El Asistente de tareas comienza.
4. Siga las instrucciones del Asistente de tareas.

Cómo crear una tarea en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.
3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione el tipo de tarea que desea ejecutar en los equipos de los usuarios.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

La nueva tarea aparecerá en la lista de tareas. La tarea tendrá la configuración predeterminada. Para modificar la configuración, abra las propiedades de la tarea. Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**. Una vez iniciada la tarea, puede suspenderla y reanudarla más tarde.

Puede utilizar la lista de tareas para llevar un control de sus resultados, ver el estado en que se encuentran, acceder a estadísticas sobre las tareas que se han ejecutado en los equipos y más. Para el mismo fin puede crear una selección de eventos (**Supervisión → Selecciones de eventos**). Para obtener más información sobre la selección de eventos, consulte la Ayuda de Kaspersky Security Center. Los resultados de la ejecución de tareas también se guardan localmente en el registro de eventos de Windows y en los informes de Kaspersky Endpoint Security.

Administrar el acceso a las tareas

Los derechos de acceso a las tareas de Kaspersky Endpoint Security (lectura, escritura, ejecución) se especifican para cada usuario que tenga acceso al Servidor de administración de Kaspersky Security Center a través de la configuración del acceso a las áreas funcionales de Kaspersky Endpoint Security. Para configurar el acceso a las áreas funcionales de Kaspersky Endpoint Security, vaya a la sección **Seguridad** de la ventana de propiedades del servidor de administración de Kaspersky Security Center. Para obtener más información sobre la gestión de tareas a través de Kaspersky Security Center, consulte la Guía de ayuda de Kaspersky Security Center.

Puede configurar los derechos de los usuarios para acceder a las tareas utilizando una directiva (*modo de gestión de tareas*). Por ejemplo, puede ocultar tareas de grupo en la interfaz de Kaspersky Endpoint Security.

Cómo configurar el modo de gestión de tareas en la interfaz de Kaspersky Endpoint Security a través de la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Tareas locales → Gestión de tareas**.

4. Configure el modo de administración de tareas (consulte la tabla a continuación).

5. Guarde los cambios.

Cómo configurar el modo de gestión de tareas en la interfaz de Kaspersky Endpoint Security a través de Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general → Interacción del usuario**.

5. En **Acciones permitidas**, configure el modo de administración de tareas (consulte la tabla a continuación).

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Parámetros de gestión de tareas

Parámetro	Descripción
Acceso a las tareas locales	Si se selecciona la casilla de verificación, se muestran tareas locales en la interfaz local de Kaspersky Endpoint Security. Cuando no existen restricciones adicionales de directivas, el usuario puede configurar y ejecutar tareas. Sin embargo, el usuario no puede programar la configuración y la ejecución de las tareas. El usuario puede ejecutar tareas solo manualmente. Si esta casilla está desmarcada, las tareas locales se ocultan en la interfaz de la aplicación. De este modo, las tareas locales no se ejecutan según la planificación. Las tareas no se pueden iniciar ni configurar en la interfaz local de Kaspersky Endpoint Security, ni con la línea de comandos. Aun así, un usuario puede iniciar un análisis de un archivo o una carpeta eligiendo la opción **Buscar virus** en el menú contextual del archivo o de la carpeta. La tarea de análisis se inicia con los valores de configuración predeterminados de la tarea de análisis personalizado.
Ver tareas de grupo	Si se selecciona la casilla de verificación, se muestran tareas de grupo en la interfaz local de Kaspersky Endpoint Security. El usuario puede ver la lista de todas las tareas en la interfaz de la aplicación. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security muestra una lista de tareas vacía.
Gestionar tareas de grupo	Si se selecciona, los usuarios pueden iniciar y detener las tareas de grupo especificadas en la consola de Kaspersky Security Center. Los usuarios pueden iniciar y detener las tareas en la interfaz de la aplicación o en la interfaz de la aplicación simplificada. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no inicia las tareas planificadas automáticamente, o el administrador inicia las tareas manualmente en la consola de Kaspersky Security Center.

Configuración de los ajustes locales de la aplicación

En Kaspersky Security Center, puede configurar los ajustes de Kaspersky Endpoint Security en un equipo determinado. Tales parámetros se denominan *configuración local de la aplicación*. No siempre es posible modificar todos los parámetros. Los parámetros que no pueden modificarse tienen el atributo de bloqueo en las propiedades de la directiva.

Cómo configurar los ajustes locales de la aplicación en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.

4. Haga doble clic para abrir la ventana de propiedades del equipo.

5. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.

6. En la lista de aplicaciones de Kaspersky que están instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.2)** y haga doble clic para abrir las propiedades de la aplicación.

7. En la sección **Configuración general**, configure Kaspersky Endpoint Security, además de Informes y Almacenes.

   El resto de las secciones de la ventana de propiedades de la aplicación son estándar para Kaspersky Security Center. Se ofrece una descripción de estas secciones en la ayuda de Kaspersky Security Center.

Si una aplicación está sujeta a una directiva que prohíbe cambiar parámetros específicos, no podrá modificarlos al configurar los parámetros de la aplicación en la sección **Configuración general**.

8. Guarde los cambios.

Cómo configurar los ajustes locales de la aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.
   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows 14.2**.
   Se abre la configuración local de la aplicación.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Haga los cambios que necesite en la configuración local de la aplicación.
7. Guarde los cambios.

Los ajustes locales de la aplicación son los mismos que los de la directiva, excepto los ajustes de cifrado.

Inicio y detención de Kaspersky Endpoint Security

Cuando termina de instalarse en el equipo de un usuario, Kaspersky Endpoint Security se abre automáticamente. De forma predeterminada, Kaspersky Endpoint Security se inicia después del inicio del sistema operativo. No se puede configurar el inicio automático de la aplicación en la configuración del sistema operativo.

La descarga de las bases de datos de Kaspersky Endpoint Security después de que se inicie el sistema operativo puede requerir hasta dos minutos según la capacidad del equipo. Durante este período, el nivel de protección del equipo se reduce. Cuando Kaspersky Endpoint Security se inicia en un sistema operativo que ya está en funcionamiento, descargar las bases de datos no afecta el nivel de protección.

Cómo configurar el inicio de Kaspersky Endpoint Security en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.
4. Use la casilla **Ejecutar la aplicación al iniciar el equipo (recomendado)** para configurar el inicio de la aplicación.
5. Guarde los cambios.

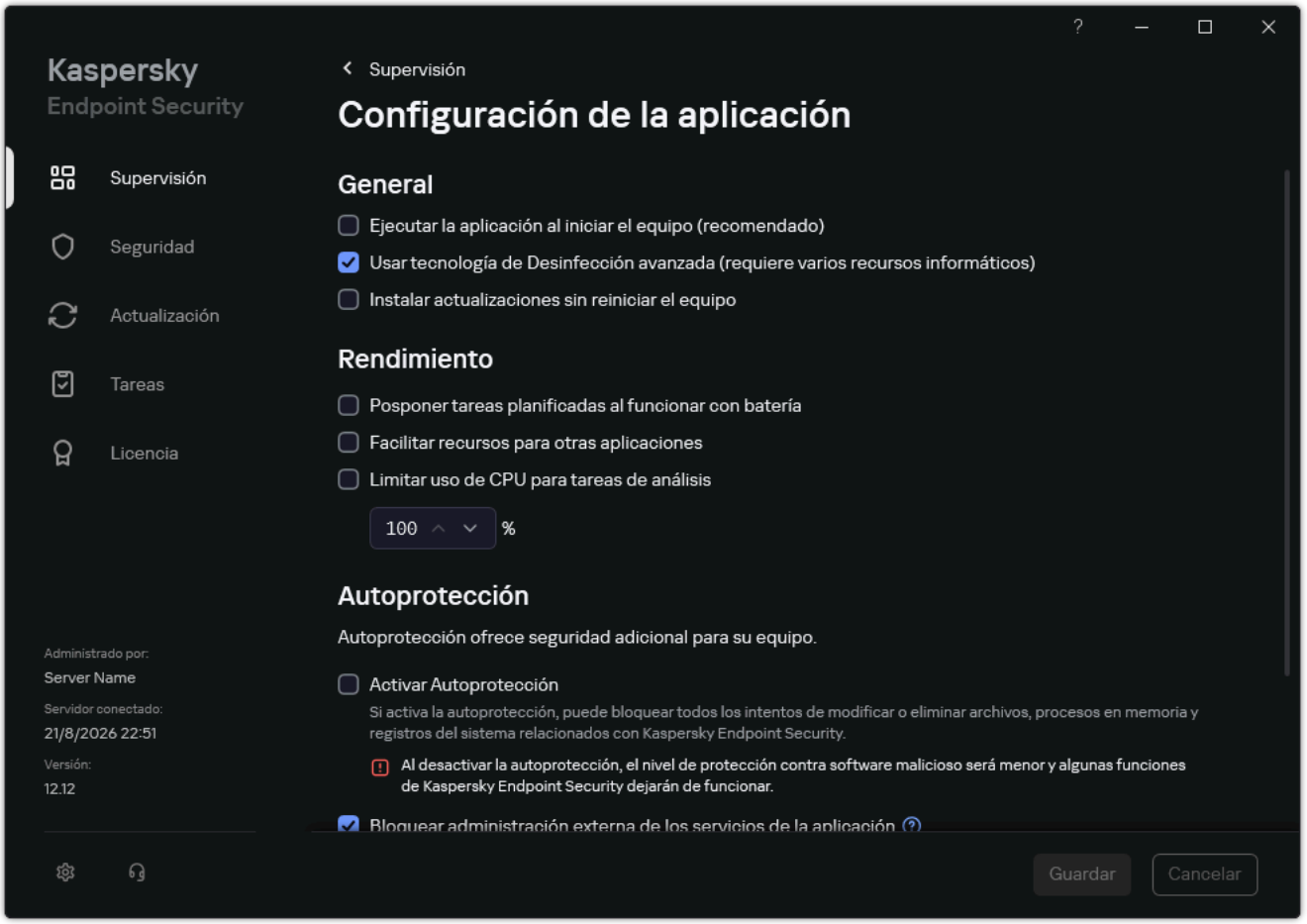
Cómo configurar el inicio de Kaspersky Endpoint Security en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Interacción del usuario**.
5. Use la casilla **Iniciar Kaspersky Endpoint Security en el arranque del ordenador (recomendado)** para configurar el inicio de la aplicación.
6. Guarde los cambios.

Cómo configurar el inicio de Kaspersky Endpoint Security en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. Use la casilla **Ejecutar la aplicación al iniciar el equipo (recomendado)** para configurar el inicio de la aplicación.

4. Guarde los cambios.

Los expertos de Kaspersky no recomiendan detener manualmente Kaspersky Endpoint Security ya que, de hacerlo, el equipo y sus datos personales quedan expuestos a amenazas. Si fuera necesario, puede suspender la protección del equipo durante el tiempo que necesite, sin detener la aplicación.

Puede controlar el estado de la aplicación utilizando el widget **Estado de la protección**.

Cómo iniciar o detener Kaspersky Endpoint Security en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.

4. Haga doble clic para abrir la ventana de propiedades del equipo.

5. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.

6. En la lista de aplicaciones de Kaspersky que están instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.2)** y haga doble clic para abrir las propiedades de la aplicación.

7. Realice una de las siguientes acciones:

   - Para iniciar la aplicación, haga clic en el botón  situado a la derecha de la lista de aplicaciones de Kaspersky.

   - Para detener la aplicación, haga clic en el botón  situado a la derecha de la lista de aplicaciones de Kaspersky.

Cómo iniciar o detener Kaspersky Endpoint Security en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.

2. Haga clic en el nombre del equipo en el que desea iniciar o detener Kaspersky Endpoint Security.

   Se abre la ventana de propiedades del equipo.

3. Seleccione la pestaña **Aplicaciones**.

4. Active la casilla junto a **Kaspersky Endpoint Security para Windows**.

5. Haga clic en los botones **Iniciar** o **Detener**.

Cómo iniciar o detener Kaspersky Endpoint Security a través de la línea de comandos

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.

2. Vaya a la carpeta donde se encuentra el archivo ejecutable klpsm.exe.

3. Para iniciar la aplicación desde la línea de comandos, introduzca `klpsm.exe start_avp_service`.

4. Para detener la aplicación desde la línea de comandos, introduzca `klpsm.exe stop_avp_service`.

Para que la aplicación se pueda detener desde la línea de comandos, active la administración externa de los servicios del sistema.



Iniciar y detener la aplicación desde la línea de comandos

Suspensión y reanudación de Protección y control del equipo

La suspensión de la protección y el control del equipo implica la desactivación de todos los componentes de protección y control de Kaspersky Endpoint Security durante un tiempo.

El estado de la aplicación se muestra mediante el icono de la aplicación en el área de notificaciones de la barra de tareas.

- El icono indica que Protección y control del equipo se ha suspendido.
- El icono indica que Protección y control del equipo están activados.

La suspensión o reanudación de Protección y control del equipo no afecta a las tareas de análisis o actualización.

Si se establece alguna conexión de red al mismo tiempo que suspende o reanuda Protección y control del equipo, se muestra una notificación para indicar la finalización de dichas conexiones de red.

Para pausar Protección y control del equipo:

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.

2. En el menú contextual, seleccione **Pausar la protección** (vea la figura a continuación).

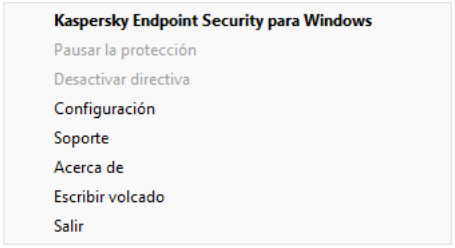
   Este elemento del menú contextual está disponible si la protección con contraseña está habilitada.

3. Seleccione una de las siguientes opciones:

   - **Pausar durante <período de tiempo>**: la protección y el control del equipo se reanudarán una vez que haya transcurrido la cantidad de tiempo especificada en la siguiente lista desplegable.
   - **Pausar hasta el reinicio de la aplicación**: la protección y el control del equipo se reanudarán después de reiniciar la aplicación o el sistema operativo. Debe activarse el inicio automático de la aplicación para utilizar esta opción.
   - **Pausar**: protección y control del equipo se reanudará cuando decida volver a activarlo.

4. Haga clic en **Pausar la protección**.

Kaspersky Endpoint Security pone en pausa todos los componentes de protección y control que no estén marcados con un candado (🔒) en la directiva. Recomendamos desactivar la directiva de Kaspersky Security Center antes de realizar esta operación.



Menú contextual del icono de la aplicación

Para reanudar Protección y control del equipo:

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En el menú contextual, seleccione **Reanudar la protección**.

Puede reanudar la protección y el control del equipo en cualquier momento, independientemente de la opción de suspensión de protección y control del equipo que haya seleccionado anteriormente.

Crear y utilizar un archivo de configuración

Un archivo de configuración con los ajustes de Kaspersky Endpoint Security le permite llevar a cabo las tareas siguientes:

- Realice la instalación local de Kaspersky Endpoint Security mediante la línea de comandos con la configuración predefinida.
- Realice la instalación remota de Kaspersky Endpoint Security mediante Kaspersky Security Center con la configuración predefinida.
- Transferir la configuración de la aplicación a una directiva.
- Migre la configuración de Kaspersky Endpoint Security de un equipo al otro (consulte las instrucciones más adelante).

Exportar un archivo de configuración

A partir de la versión 14.2 de Kaspersky Endpoint Security, el archivo de configuración exportado se puede cifrar. Como el archivo de configuración puede contener credenciales, recomendamos cifrarlo. No puede editar un archivo cifrado. Cualquier intento de modificar un archivo de configuración lo dañará.

El cifrado de archivos de configuración tiene las siguientes características especiales:

- Kaspersky Endpoint Security permite importar archivos cifrados únicamente desde la interfaz de usuario de la aplicación o mediante la línea de comandos. No puede usar un archivo de este tipo en una consola de Kaspersky Security Center para configurar una directiva ni instalar la aplicación de forma remota. Si tiene previsto añadir el archivo a una directiva o a un paquete de instalación, omita el paso de cifrado del archivo.
- No es posible recuperar la contraseña de un archivo cifrado.
- Las versiones de Kaspersky Endpoint Security anteriores a la 14.1 no admiten la importación de archivos de configuración cifrados. Si tiene previsto importar el archivo en una versión anterior de la aplicación, omita el paso de cifrado del archivo.

Para crear un archivo de configuración:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Administrar configuración**.
3. Haga clic en **Exportar**.
4. Para guardar el archivo de configuración, la Protección con contraseña debe estar activada. El usuario debe tener el permiso **Exportar configuración**.
5. En la ventana que se abre, especifique la ruta en la cual desea guardar el archivo de configuración e introduzca su nombre.

   Si desea usar el archivo de configuración para la instalación local o remota de Kaspersky Endpoint Security, lo debe denominar install.cfg.

6. Si es necesario, active el conmutador **Cifrar el archivo exportado** e introduzca la contraseña de cifrado del archivo de configuración.

   Guarde la contraseña en un almacén seguro. No es posible recuperar esta contraseña.

7. Guarde el archivo.

Como resultado, la aplicación crea un archivo de configuración.

Importar un archivo de configuración

Al importar un archivo de configuración, Kaspersky Endpoint Security no transfiere contraseñas de contenedores criptográficos. Si utiliza la autenticación bidireccional al conectarse a los servidores, debe especificar las contraseñas del contenedor criptográfico desde cero.

Para importar la configuración de Kaspersky Endpoint Security desde un archivo de configuración:

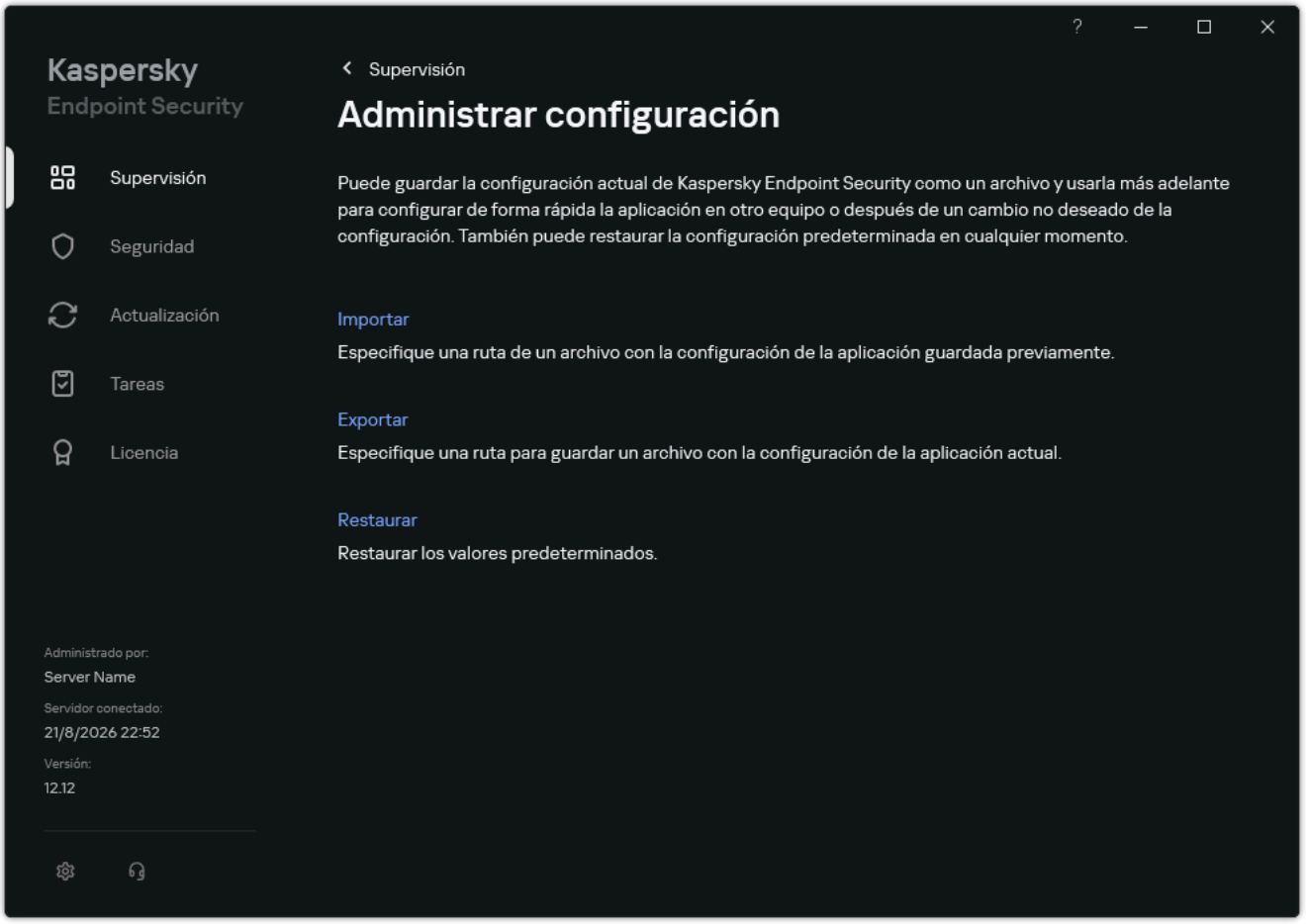
1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Administrar configuración**.
3. Haga clic en **Importar**.
4. En la ventana que se abre, introduzca la ruta del archivo de configuración.

5. Si el archivo de configuración está cifrado, introduzca la contraseña que especificó al exportarlo.

> Si ha olvidado la contraseña de cifrado del archivo de configuración, no podrá recuperarla. En este caso, debe repetir los pasos para exportar el archivo de configuración.

6. Abra el archivo.

Todos los valores de la configuración de Kaspersky Endpoint Security se definirán según el archivo de configuración seleccionado.



Administrar la configuración de la aplicación

Restaurar las configuración predeterminada de la aplicación

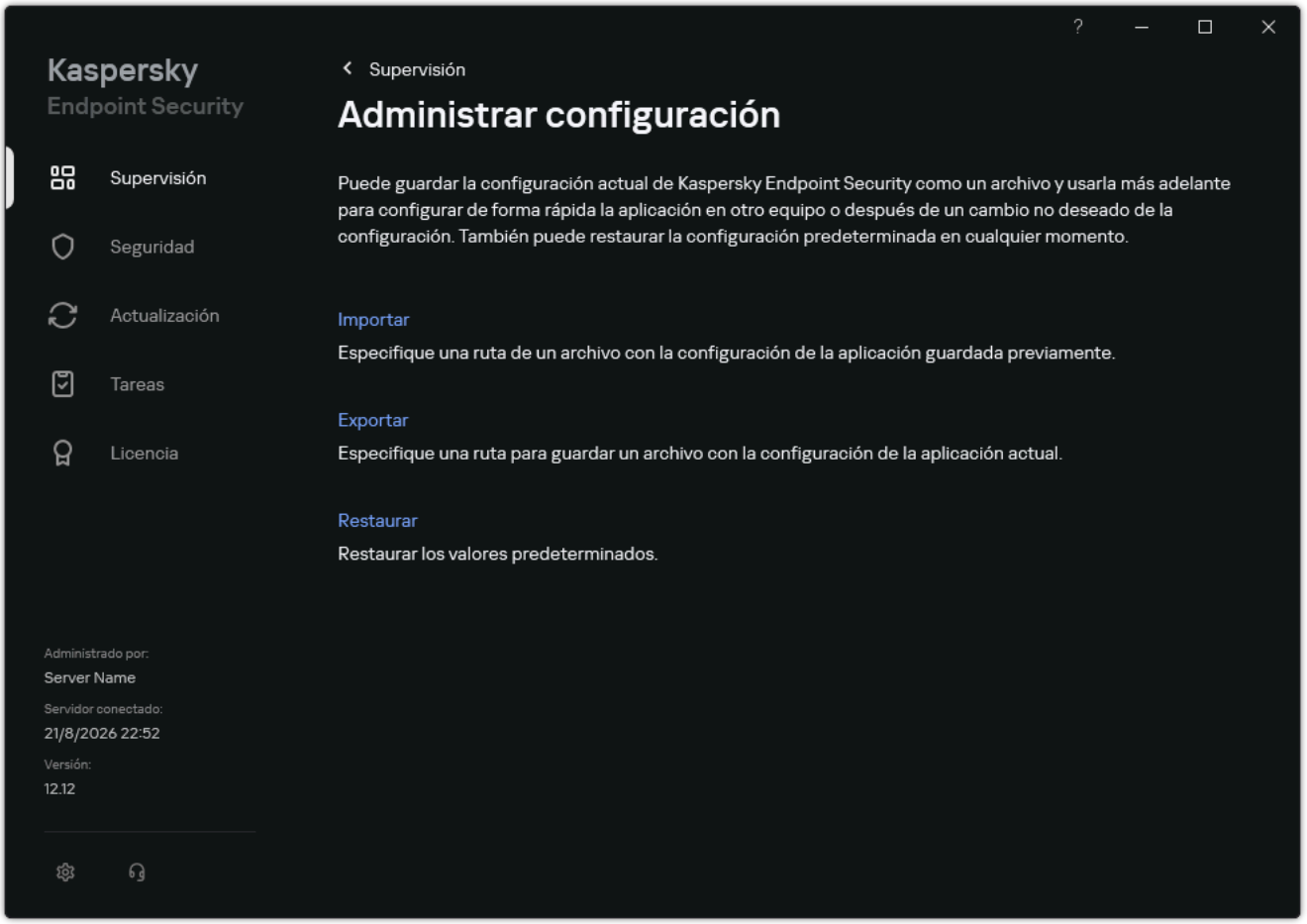
Puede restaurar la configuración de la aplicación recomendada por Kaspersky en cualquier momento. Cuando se restablece la configuración, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección.

Para restaurar la configuración predeterminada de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Administrar configuración**.

3. Haga clic en **Restaurar**.

4. Guarde los cambios.



Administrar la configuración de la aplicación

Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones

El rendimiento de Kaspersky Endpoint Security se refiere al número de tipos de objetos que puedan dañar el equipo que son detectables, así como al consumo de energía y uso de los recursos del equipo.

Selección de los tipos de objetos detectables

Kaspersky Endpoint Security le permite ajustar la protección de su equipo y seleccionar los tipos de objetos que la aplicación detecta durante su funcionamiento. Kaspersky Endpoint Security el sistema operativo en busca de virus, gusanos y troyanos. No puede desactivar el análisis de estos tipos de objetos. Este tipo de software malicioso (malware) puede provocar daños significativos en el equipo. Para lograr una mayor protección en su equipo, puede ampliar la gama de tipos de objetos detectables si activa el control de software legal que pueden usar los delincuentes para dañar su equipo o sus datos personales.

Uso del modo de ahorro de energía

El consumo de energía que hacen las aplicaciones es un aspecto básico para los equipos portátiles. Por lo general, las tareas planificadas de Kaspersky Endpoint Security consumen una gran cantidad de recursos. Cuando un equipo se está ejecutando con alimentación de la batería, puede usar el modo de ahorro de energía para moderar su consumo.

En el modo de ahorro de energía, se posponen automáticamente las siguientes tareas planificadas:

- Tarea de Análisis completo;
- Tarea de Análisis de áreas críticas;
- Tarea de análisis personalizado;
- Tarea de Comprobación de integridad.

Independientemente de si el modo de ahorro de energía está activado o no, Kaspersky Endpoint Security suspende las tareas de cifrado cuando el portátil cambia al funcionamiento con batería. La aplicación reanuda las tareas de cifrado cuando el portátil cambia del funcionamiento con batería al funcionamiento por red eléctrica.

Concesión de recursos del equipo a otras aplicaciones

El consumo de recursos informáticos al analizar un equipo puede aumentar la carga en los subsistemas de la CPU y el disco duro. Para solucionar el problema del funcionamiento simultáneo durante el aumento de la carga en los subsistemas del disco duro y la CPU, Kaspersky Endpoint Security puede conceder recursos para otras aplicaciones.

Uso de tecnología de desinfección avanzada

Las aplicaciones maliciosas actuales pueden penetrar en los niveles más bajos del sistema operativo, lo que las hace prácticamente imposibles de eliminar. Tras la detección de actividad maliciosa en el sistema operativo, Kaspersky Endpoint Security lleva a cabo un proceso de desinfección exhaustiva por medio de la tecnología de desinfección avanzada. El objetivo de *la tecnología de desinfección avanzada* consiste en eliminar del sistema operativo las aplicaciones maliciosas que ya han puesto en marcha sus procesos en la memoria RAM y que impiden que Kaspersky Endpoint Security las elimine por medio de otros métodos. Como consecuencia de ello, se neutraliza la amenaza. Cuando la desinfección avanzada está en curso, se recomienda que no ponga en marcha ningún proceso nuevo ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada emplea un número considerable de recursos del sistema operativo, lo que puede ralentizar el resto de las aplicaciones.

Después de que la desinfección avanzada haya finalizado en un equipo que ejecuta con Microsoft Windows para estaciones de trabajo, Kaspersky Endpoint Security solicita el permiso del usuario para reiniciar el equipo. Después del reinicio del sistema, Kaspersky Endpoint Security elimina los archivos de malware e inicia un "pequeño" análisis completo del equipo.

Resulta imposible que se solicite el reinicio en un equipo que se ejecuta con Microsoft Windows para servidores debido a las especificaciones de Kaspersky Endpoint Security. El reinicio de un servidor de archivos no planificado puede conllevar problemas que impliquen la no disponibilidad temporal de los datos del servidor de archivos o la pérdida de datos no guardados. Se recomienda reiniciar el servidor de archivos únicamente de acuerdo con la planificación. Esta es la razón por la cual la tecnología de desinfección avanzada está desactivada de forma predeterminada para los servidores de archivos.

Si se detecta una infección activa en un servidor de archivos, se envía a Kaspersky Security Center un evento con información que indica que se debe realizar la desinfección avanzada. Para desinfectar la infección activa de un servidor, active la tecnología de desinfección avanzada para servidores e inicie una tarea de grupo de *Análisis antimalware* en el momento que resulte adecuado para los usuarios del servidor.

Activación o desactivación del modo de ahorro de energía

El *Modo de ahorro de energía* es una funcionalidad que reduce la carga de recursos del equipo portátil y extiende la vida útil de la batería sin comprometer significativamente el nivel de seguridad. En el modo de ahorro de energía, la aplicación limita el inicio de tareas programadas. De esta forma, el modo de ahorro de energía garantiza un equilibrio entre el nivel de seguridad y la duración de la batería del portátil.

Cuando se activa el modo de ahorro de energía y el equipo funciona con la energía de la batería, las tareas siguientes no se ejecutan aunque estén planificadas:

- *Análisis completo*.
- *Análisis de áreas críticas*.
- *Análisis personalizado*.
- *Comprobación de integridad de la aplicación*.
- *Análisis de IOC*.
- *Actualización de las bases de datos y módulos de la aplicación* (solo parches)

La aplicación omite las actualizaciones programadas de las bases de datos solo cuando el equipo portátil funciona con batería y el nivel de carga es inferior al 30 % (valor predeterminado). Puede cambiar el nivel mínimo de carga de la batería a partir del cual la aplicación comienza a omitir las actualizaciones programadas de la base de datos antivirus editando el registro (consulte las instrucciones siguientes). En todos los demás casos, Kaspersky Endpoint Security actualiza las bases de datos según lo programado, independientemente de si el equipo portátil está conectado o funciona con batería, o si la aplicación está en modo de ahorro de energía.

Cómo activar o desactivar el modo de ahorro de energía en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de la aplicación**.

5. En el bloque **Rendimiento**, use la casilla de verificación **Posponer tareas planificadas al funcionar con batería** para activar o desactivar el modo de ahorro de energía.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el modo de ahorro de energía en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Rendimiento**.

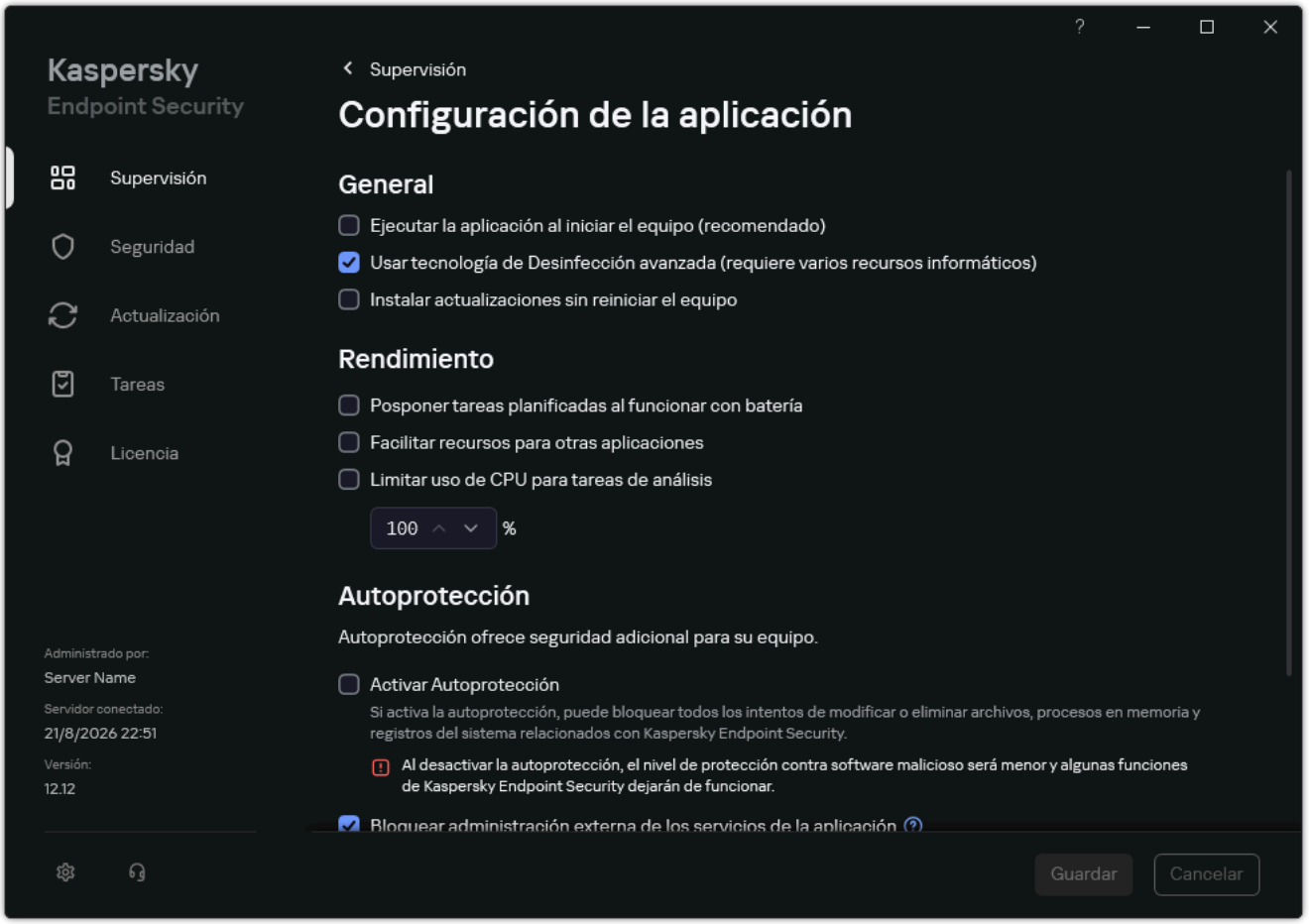
5. En el bloque **Posponer u omitir tareas planificadas al funcionar con batería**, use la casilla de verificación **Posponer u omitir tareas planificadas al funcionar con batería (depende del sistema operativo)** para activar o desactivar el modo de ahorro de energía.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el modo de ahorro de energía en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. En el bloque **Rendimiento**, use la casilla de verificación **Posponer tareas planificadas al funcionar con batería** para activar o desactivar el modo de ahorro de energía.

4. Guarde los cambios.

Cómo cambiar el nivel mínimo de carga a partir del cual la aplicación comienza a omitir las actualizaciones programadas de la base de datos antivirus

1. Abra el editor de registro en el equipo.

2. En el editor de registro, vaya a la siguiente sección:

   - Para sistemas operativos de 64 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`

   - Para sistemas operativos de 32 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. Abra `UpdaterAccumulatorThreshold` para editarlo.

4. Especifique el nivel mínimo de carga a partir del cual la aplicación comienza a omitir las actualizaciones programadas de la base de datos antivirus.

Activación o desactivación de la concesión de recursos a otras aplicaciones

El consumo de recursos informáticos de Kaspersky Endpoint Security al analizar el equipo puede aumentar la carga en los subsistemas de la CPU y el disco duro. Esto puede ralentizar otras aplicaciones. Para optimizar el rendimiento, Kaspersky Endpoint Security proporciona un *modo de transferencia de recursos a otras aplicaciones*. En este modo, el sistema operativo puede reducir la prioridad de los hilos de la tarea de análisis de Kaspersky Endpoint Security si la carga de la CPU es alta. Esto permite redistribuir recursos del sistema operativo a otras aplicaciones. Por tanto, las tareas de análisis recibirán menos tiempo de CPU. Como resultado, Kaspersky Endpoint Security tardará más en analizar el equipo. De forma predeterminada, la aplicación está configurada para ceder recursos a otras aplicaciones.

Cómo activar o desactivar la concesión de recursos a otras aplicaciones en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.

4. En el bloque **Rendimiento**, use la casilla de verificación **Facilitar recursos para otras aplicaciones** para activar o desactivar la concesión de recursos a otras aplicaciones.

5. Guarde los cambios.

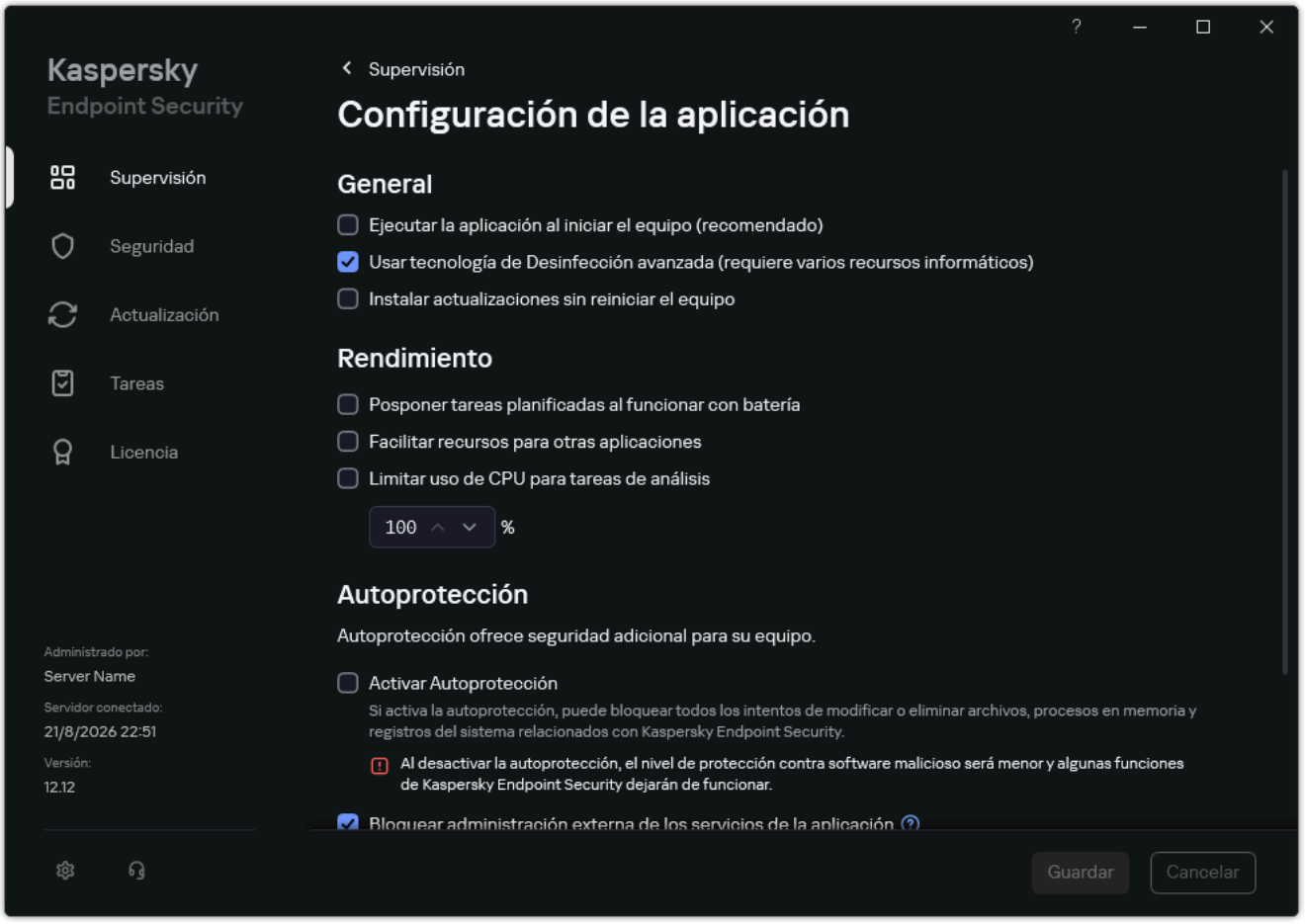
Cómo activar o desactivar la concesión de recursos a otras aplicaciones en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Rendimiento**.
5. En el bloque **Facilitar recursos para otras aplicaciones**, use el interruptor **Facilitar recursos para otras aplicaciones** para activar o desactivar la concesión de recursos a otras aplicaciones.
6. Guarde los cambios.

Cómo activar o desactivar la concesión de recursos a otras aplicaciones en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. En el bloque **Rendimiento**, use la casilla de verificación **Facilitar recursos para otras aplicaciones** para activar o desactivar la concesión de recursos a otras aplicaciones.
4. Guarde los cambios.

Prácticas recomendadas para optimizar el rendimiento de Kaspersky Endpoint Security

Al implementar Kaspersky Endpoint Security para Windows, puede utilizar las siguientes recomendaciones para configurar la protección del equipo y optimizar el rendimiento. Para obtener más información sobre cómo lidiar con problemas de productividad del equipo, consulte la Base de conocimientos de soporte técnico.

General

Defina la configuración general de la aplicación de acuerdo con las siguientes recomendaciones:

1. Actualice Kaspersky Endpoint Security a la versión más reciente.

   En las versiones más recientes de la aplicación se han corregido los errores, mejorado la estabilidad y optimizado en rendimiento.

2. Active los componentes de protección con la configuración predeterminada.

   La configuración predeterminada se considera óptima. Los expertos de Kaspersky recomiendan esta configuración. La configuración predeterminada proporciona el nivel de protección recomendado y el uso óptimo de los recursos. Si es necesario, puede restaurar la configuración predeterminada de la aplicación.

3. Active las funciones de optimización del rendimiento de la aplicación.

   La aplicación tiene funciones de optimización del rendimiento: modo de conservación de energía y concesión de recursos a otras aplicaciones. Asegúrese de que estas opciones estén activadas.

Análisis antimalware en estaciones de trabajo

Se recomienda activar Análisis en segundo plano para el análisis antimalware de estaciones de trabajo. El *Análisis en segundo plano* es uno de los modos de análisis disponibles en Kaspersky Endpoint Security. Cuando se realiza un análisis de este tipo, la aplicación no le muestra ninguna notificación al usuario. En comparación con otros tipos de análisis, como el análisis completo, un análisis en segundo plano tiene menos impacto en los recursos del equipo. En este modo, Kaspersky Endpoint Security analiza los objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema. La configuración del análisis en segundo plano se considera óptima. Los expertos de Kaspersky recomiendan esta configuración. Por lo tanto, para realizar un análisis antimalware del equipo, puede usar solo el modo de análisis en segundo plano sin usar otras tareas de análisis.

Si el análisis en segundo plano no se adapta a sus necesidades, configure la tarea *Análisis antimalware* de acuerdo con las siguientes recomendaciones:

1. Establezca un límite en el consumo de recursos de la CPU al analizar el equipo.

   Puede limitar el uso de CPU al ejecutar la tarea *Análisis antimalware*. Para hacerlo, en la configuración de la aplicación, especifique el porcentaje máximo de carga de la CPU para todos los núcleos que se pueden utilizar al analizar el equipo. Esto puede aumentar el tiempo que lleva analizar su equipo.

2. Configurar el cronograma óptimo de análisis del equipo.

Puede configurar la tarea para que se ejecute cuando el equipo esté funcionando con una carga mínima. Por ejemplo, puede configurar la tarea para que se ejecute por la noche o los fines de semana.

Si los usuarios apagan el equipo fuera del horario laboral, puede activar la función Wake-on-LAN. La función Wake-on-LAN permite encender el equipo de forma remota mediante el envío de una señal especial a través de la red local. Para utilizar esta función, debe activar Wake-on-LAN en la configuración del BIOS. También puede hacer que el equipo se apague automáticamente cuando finalice el análisis.

Si no pudo configurar un programa de análisis óptimo, configure las tareas para que se ejecuten solo cuando el equipo esté inactivo. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió.

3. Definir una cobertura del análisis.

   Seleccione los siguientes objetos para analizar (conjunto mínimo de cobertura del análisis):

   - Memoria del núcleo
   - Procesos en ejecución y objetos de arranque
   - Sectores de arranque
   - %systemroot% (sin incluir subcarpetas)
   - %systemroot%\System (sin incluir subcarpetas)
   - %systemroot%\System32 (sin incluir subcarpetas)
   - %systemroot%\System32\drivers (sin incluir subcarpetas)
   - %systemroot%\SysWOW64 (sin incluir subcarpetas)
   - %systemroot%\SysWOW64\drivers (sin incluir subcarpetas)

4. Active las tecnologías iSwift e iChecker.

   - Tecnología iSwift.

     Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

   - Tecnología iChecker.

     Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

Solo puede activar las tecnologías iSwift e iChecker en la Consola de administración (MMC) y la interfaz de Kaspersky Endpoint Security. No puede activar estas tecnologías en Kaspersky Security Center Web Console.

5. Desactivar el análisis de archivos protegidos con contraseña.

   Si el análisis de archivos comprimidos protegidos con contraseña está activado, se muestra una solicitud de contraseña antes de analizar el archivo. Debido a que se recomienda programar la tarea fuera del horario de oficina, el usuario no puede introducir la contraseña. Puede analizar archivos protegidos con contraseña manualmente.

6. Desactivar el inicio simultáneo de varias tareas de análisis.

   Kaspersky Endpoint Security colocará en cola las nuevas tareas de análisis si el análisis actual continúa. Esto ayuda a optimizar la carga en el equipo.

Análisis antimalware en los servidores

Configure la tarea *Análisis antimalware* de acuerdo con las siguientes recomendaciones:

1. Establezca un límite en el consumo de recursos de la CPU al analizar el equipo.

   Puede limitar el uso de CPU al ejecutar la tarea *Análisis antimalware*. Para hacerlo, en la configuración de la aplicación, especifique el porcentaje máximo de carga de la CPU para todos los núcleos que se pueden utilizar al analizar el equipo. Esto puede aumentar el tiempo que lleva analizar su equipo.

2. Configurar el cronograma óptimo de análisis del equipo.

   Puede configurar la tarea para que se ejecute cuando el equipo esté funcionando con una carga mínima. Por ejemplo, puede configurar la tarea para que se ejecute por la noche o los fines de semana.

3. Active las tecnologías iSwift e iChecker.

   - Tecnología iSwift.

     Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

   - Tecnología iChecker.

     Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

   Solo puede activar las tecnologías iSwift e iChecker en la Consola de administración (MMC) y la interfaz de Kaspersky Endpoint Security. No puede activar estas tecnologías en Kaspersky Security Center Web Console.

4. Desactivar el análisis de archivos protegidos con contraseña.

   Si el análisis de archivos comprimidos protegidos con contraseña está activado, se muestra una solicitud de contraseña antes de analizar el archivo. Debido a que se recomienda programar la tarea fuera del horario de oficina, el usuario no puede introducir la contraseña. Puede analizar archivos protegidos con contraseña manualmente.

5. Desactivar el inicio simultáneo de varias tareas de análisis.

   Kaspersky Endpoint Security colocará en cola las nuevas tareas de análisis si el análisis actual continúa. Esto ayuda a optimizar la carga en el equipo.

Kaspersky Security Network

A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, los servicios de KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web que se analicen, así como sobre la categoría y reputación de los archivos analizados.

Edite la configuración de Kaspersky Security Network de acuerdo con las siguientes recomendaciones:

1. Desactivar el modo ampliado de KSN.

   El *modo KSN ampliado* es un modo en el que Kaspersky Endpoint Security envía información adicional a Kaspersky.

2. Configure Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos.

3. Activar modo nube.

   Modo nube es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky.

Análisis antimalware

Un análisis antimalware es fundamental para la seguridad del equipo. Realice análisis antimalware de forma periódica para ayudar a descartar la posibilidad de que se extienda el software malicioso (malware) que los componentes de protección no han detectado debido a una configuración de nivel de seguridad baja o a otros motivos.

Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive, y crea entradas de registro que indican que estos archivos no se han analizado.

Análisis completo

Análisis en profundidad de todo el equipo. Kaspersky Endpoint Security analiza los siguientes objetos:

- Memoria del núcleo
- Objetos cargados en el inicio del sistema operativo
- Sectores de arranque
- Copia de seguridad del sistema operativo
- Todas las unidades de disco duro y unidades extraíbles

Los expertos de Kaspersky recomiendan que no cambie la cobertura del análisis de la tarea *Análisis completo*.

Para reducir el impacto en los recursos del equipo, recomendamos realizar un análisis en segundo plano en lugar de una tarea de análisis completo. El nivel de seguridad del equipo no se verá afectado.

Análisis de áreas críticas

De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.

Los expertos de Kaspersky recomiendan que no cambie la cobertura del análisis de la tarea *Análisis de áreas críticas*.

Análisis personalizado

Kaspersky Endpoint Security analiza los objetos seleccionados por el usuario. Puede analizar cualquier objeto de la siguiente lista:

- Memoria del sistema
- Objetos cargados en el inicio del sistema operativo
- Copia de seguridad del sistema operativo
- Unidades de disco duro, unidades extraíbles y unidades de red
- Cualquier archivo seleccionado

Análisis en segundo plano

El *Análisis en segundo plano* es uno de los modos de análisis disponibles en Kaspersky Endpoint Security. Cuando se realiza un análisis de este tipo, la aplicación no le muestra ninguna notificación al usuario. En comparación con otros tipos de análisis, como el análisis completo, un análisis en segundo plano tiene menos impacto en los recursos del equipo. En este modo, Kaspersky Endpoint Security analiza los objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema.

Comprobación de integridad de la aplicación

Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en busca de datos corruptos o modificaciones.

Análisis del equipo

Un análisis es fundamental para la seguridad del equipo. Realice análisis antimalware de forma periódica para ayudar a descartar la posibilidad de que se extienda el software malicioso (malware) que los componentes de protección no han detectado debido a una configuración de nivel de seguridad baja o a otros motivos. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

Kaspersky Endpoint Security tiene las siguientes tareas estándar predefinidas: *Análisis completo*, *Análisis de áreas críticas*, *Análisis personalizado*. Si su organización tiene el sistema de administración de Kaspersky Security Center desplegado, puede crear una tarea de *Análisis antimalware* y configurar el análisis.

Cómo ejecutar una tarea de análisis en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.

   Si es necesario, cree la tarea de *Análisis antimalware*.
4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
5. Configure la tarea de análisis (consulte la tabla a continuación).

   Si necesario, configure la programación de la tarea de análisis.
6. Guarde los cambios.
7. Ejecutar la tarea de análisis.

Kaspersky Endpoint Security comenzará a escanear el equipo. Si el usuario ha interrumpido la ejecución de la tarea (por ejemplo, al apagar el equipo), Kaspersky Endpoint Security ejecuta automáticamente la tarea, continuando desde el punto donde se interrumpió el análisis.

Cómo ejecutar una tarea de análisis en la Consola web

1. En la ventana principal de Web Console, seleccione **Administración de activos → Tareas**.

   Se abre la lista de tareas.
2. Haga clic en la tarea de análisis.

   Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Configure la tarea de análisis (consulte la tabla a continuación).

   Si necesario, configure la programación de la tarea de análisis.
5. Guarde los cambios.
6. Ejecutar la tarea de análisis.

Kaspersky Endpoint Security comenzará a escanear el equipo. Si el usuario ha interrumpido la ejecución de la tarea (por ejemplo, al apagar el equipo), Kaspersky Endpoint Security ejecuta automáticamente la tarea, continuando desde el punto donde se interrumpió el análisis.

Cómo ejecutar una tarea de análisis en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.

Si no se muestra la tarea de análisis, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

En la interfaz de la aplicación, solo puede configurar tareas de análisis locales: *Análisis completo*, *Análisis de áreas críticas*, *Análisis personalizado*. No es posible configurar en la interfaz de la aplicación las tareas de grupo añadidas mediante la Consola de Kaspersky Security Center. El botón ⚙ no se muestra para las tareas de grupo.

3. Configure la tarea de análisis (consulte la tabla a continuación).

   Si necesario, configure la programación de la tarea de análisis.

4. Guarde los cambios.

5. Ejecutar la tarea de análisis.

   Kaspersky Endpoint Security comenzará a escanear el equipo. La aplicación mostrará el progreso del análisis, la cantidad de archivos analizados y el tiempo de análisis restante. Puede detener la tarea en cualquier momento haciendo clic en el botón **Detener**.

Para optimizar el rendimiento de Kaspersky Endpoint Security al analizar el equipo, puede administrar la configuración avanzada de la tarea *Análisis completo* y limitar el uso de recursos de la CPU.

En Kaspersky Security Center, también puede utilizar la tarea *Análisis en segundo plano* en lugar de la tarea *Análisis completo* para optimizar el rendimiento de la aplicación. El nivel de seguridad del equipo no se verá afectado. No se puede configurar el análisis en segundo plano.

Como resultado, Kaspersky Endpoint Security analiza el equipo y, si detecta una amenaza, ejecuta la acción configurada en la configuración de la aplicación. Normalmente, la aplicación intenta desinfectar los archivos infectados. Como resultado, los archivos infectados pueden recibir los siguientes estados:

- **Pospuesto**. El archivo infectado no se ha podido desinfectar. La aplicación elimina el archivo infectado después de reiniciar el equipo.
- **Registrado**. El archivo infectado no se ha podido desinfectar. La aplicación agrega información sobre los archivos infectados detectados a la lista de amenazas activas.
- **Escritura no aceptada** o **Error de escritura**. El archivo infectado no se ha podido desinfectar. La aplicación no tiene acceso de escritura.
- **Ya se ha procesado**. La aplicación detectó un archivo infectado anteriormente. La aplicación desinfecta o elimina el archivo infectado después de reiniciar el equipo.

Configuración del análisis

Parámetro	Descripción
Nivel de seguridad	Kaspersky Endpoint Security puede usar diferentes grupos de parámetros para ejecutar un análisis. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*. • **Alto**. Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, la aplicación analiza archivos, paquetes de distribución, archivos de formatos de Office, pero no analiza archivos protegidos con contraseña. Cuando se establece este nivel de seguridad, la aplicación utiliza el análisis heurístico con el nivel de detalle **Análisis profundo**. • **Recomendado**. Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, la aplicación analiza archivos, paquetes de distribución, archivos de formatos de Office, pero no analiza archivos protegidos con contraseña. Cuando se establece este nivel de seguridad, la aplicación utiliza el análisis heurístico con el nivel de detalle **Análisis medio**. • **Bajo**. Kaspersky Endpoint Security analiza solo los formatos de archivo especificados. Al analizar archivos compuestos, la aplicación analiza archivos, paquetes de distribución, archivos de formatos de Office, pero no analiza archivos protegidos con contraseña. Cuando se establece este nivel de seguridad, la aplicación utiliza el análisis heurístico con el nivel de detalle **Análisis superficial**. Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración recomendada del nivel de seguridad.

Parámetro	Descripción
Acción al detectar una amenaza	**Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo. **Desinfectar; informar si falla la desinfección**. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección falla, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas. **Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos. Antes de intentar desinfectar o eliminar un archivo infectado, la aplicación crea una copia de seguridad del archivo en caso de que necesite restaurarlo o que sea posible desinfectarlo en el futuro. Al detectar archivos infectados que son parte de la aplicación Windows Store, Kaspersky Endpoint Security intenta eliminar los archivos.
Ejecutar la desinfección avanzada de inmediato *(disponible solo en la Consola de Kaspersky Security Center)*	Se realiza una desinfección avanzada durante una tarea de análisis antivirus en un equipo solo si la característica Desinfección avanzada está activada en las propiedades de la directiva aplicada a este equipo. Si se selecciona la casilla de verificación, Kaspersky Endpoint Security desinfecta la infección activa inmediatamente después de que se detecta durante la ejecución de la tarea de análisis antivirus. Una vez que se desinfecta la infección activa, Kaspersky Endpoint Security reinicia el equipo sin preguntarle al usuario. Si la casilla de verificación está desactivada, Kaspersky Endpoint Security no desinfecta la infección activa inmediatamente después de que se detecta durante la ejecución de la tarea de análisis antivirus. Kaspersky Endpoint Security genera eventos de infección activos en informes de aplicaciones locales y en el lado de Kaspersky Security Center. La infección activa se puede desinfectar cuando se vuelve a ejecutar la tarea de análisis antivirus con la función Desinfección avanzada activada. De esta forma, el administrador del sistema puede elegir el momento adecuado para realizar la Desinfección avanzada y, posteriormente, reiniciar los equipos automáticamente.
Cobertura del análisis	Lista de objetos que Kaspersky Endpoint Security analiza mientras realiza una tarea de análisis. Los objetos dentro de la cobertura del análisis pueden ser la memoria del núcleo, los procesos en ejecución, los sectores de arranque, el almacenamiento de respaldo del sistema, las unidades de disco duro, las extraíbles o las de red, una carpeta o un archivo. En Kaspersky Endpoint Security para Windows 12.12, el correo electrónico está excluido de la cobertura del análisis de la aplicación. El análisis de los mensajes de correo electrónico entrantes y salientes lo realiza el componente Protección frente a amenazas en el correo. Si está utilizando una versión anterior del complemento de administración, la aplicación excluye el correo electrónico del alcance del análisis, incluso si la directiva lo incluye.
Programación de análisis	**Manual**. Modo de ejecución en el que puede comenzar a analizar manualmente en el momento que sea conveniente para usted. **Según programación**. En este modo de ejecución de la tarea de análisis, la aplicación comienza el análisis en función de la programación especificada. Si está seleccionado este modo de ejecución de la tarea de análisis, también puede iniciar la tarea de análisis manualmente.
Posponer ejecución después del inicio de la aplicación durante N minutos	Inicio pospuesto de la tarea de análisis después del inicio de la aplicación. Dado que se ejecutan varios procesos al iniciar el sistema operativo, es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después del inicio de Kaspersky Endpoint Security.
Ejecutar tareas omitidas	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security iniciará la tarea omitida lo antes posible. La tarea se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programado de la tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas omitidas, las ejecuta de manera aleatoria dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no iniciará las tareas omitidas. En lugar de ello, lleva a cabo la siguiente tarea de acuerdo con la planificación actual.

Parámetro	Descripción
Ejecutar solo cuando el equipo está inactivo	Inicio pospuesto de la tarea cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.
Ejecutar el análisis como	Por defecto, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. La cobertura de la protección puede incluir unidades de red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que tenga los permisos adecuados en la configuración de la aplicación y realizar la tarea de análisis con esta cuenta de usuario.
Tipos de archivos Kaspersky Endpoint Security considera los archivos sin extensión como ejecutables. La aplicación siempre analiza los archivos ejecutables independientemente de los tipos de archivos que elija para analizar. **Todos los archivos**. Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones). **Archivos analizados por formato**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares. **Archivos analizados por extensión**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. El formato de archivo se determina en función de su extensión. De forma predeterminada, Kaspersky Endpoint Security analiza archivos según su formato. El análisis de archivos por extensión es menos seguro porque un archivo malicioso puede tener una extensión que no está en la lista de potencialmente infectable (por ejemplo, `.123`).	
Analizar solamente archivos nuevos y modificados	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
Omitir archivo cuyo análisis dure más de N segundo(s)	Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.
No ejecute varias tareas de análisis al mismo tiempo	Posponga las tareas de análisis planificadas si aún se está ejecutando un análisis planificado iniciado anteriormente. Kaspersky Endpoint Security pondrá en cola las tareas de análisis planificadas si el análisis actual sigue en curso. Esto ayuda a optimizar la carga en el equipo. Por ejemplo, ha planificado tareas de análisis para que se ejecuten a las 6:00 p. m. y a las 8:00 p. m. Kaspersky Endpoint Security pospondrá la tarea de análisis de las 8:00 p. m. si la tarea de análisis planificada para las 6:00 p. m. aún se está ejecutando. La aplicación ejecutará un análisis cuando finalice la tarea iniciada a las 6:00 p. m. Sin embargo, Kaspersky Endpoint Security inicia inmediatamente una tarea de análisis aunque una de las siguientes tareas de análisis esté en ejecución: • Análisis de unidades extraíbles cuando se conectan. • Analizar desde el menú contextual. • Análisis de áreas críticas que se inició al detectar un indicador de compromiso (IoC). Si esta casilla de verificación no está marcada, Kaspersky Endpoint Security le permite ejecutar varias tareas de análisis al mismo tiempo. La ejecución de varias tareas de análisis requiere más recursos informáticos.
Analizar archivos	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos en formatos de Microsoft Office	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.

Parámetro	Descripción
Analizar archivos de formatos de correo electrónico	Análisis de archivos en formato de correo electrónico y la base de datos de correo electrónico. La aplicación analiza los archivos PST y OST utilizados por los clientes de correo MS Outlook y Windows Mail, así como los archivos EML. Kaspersky Endpoint Security no es compatible con la versión de 64 bits del cliente de correo electrónico Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de 64 bits de Microsoft Outlook (archivos PST y OST) si hay una versión de 64 bits de Microsoft Outook instalada en el equipo, aunque el correo esté incluido en la cobertura del análisis. Si se selecciona la casilla de verificación, Kaspersky Endpoint Security fracciona el archivo de formato de correo en sus componentes (encabezado, cuerpo y archivos adjuntos) y los analiza en busca de amenazas. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza el archivo de formato de correo como un único archivo. Cuando se descubre un objeto malicioso en archivos PST u OST, Kaspersky Endpoint Security lo transforma en inofensivo de acuerdo con la acción seleccionada (por ejemplo, desinfección o eliminación del archivo). Si se detectan objetos maliciosos en archivos de otros clientes de correo electrónico (por ejemplo, Mozilla Thunderbird), Kaspersky Endpoint Security no desinfecta ni elimina esos archivos para evitar que sus mensajes de correo electrónico se eliminen involuntariamente. Kaspersky Endpoint Security solo añade información sobre los objetos detectados a la lista de amenazas activas. Debe eliminar los mensajes de correo electrónico que tengan archivos maliciosos adjuntos desde la interfaz de usuario de su cliente de correo. Si por algún motivo no es posible eliminar en ese momento los mensajes que contienen objetos maliciosos, puede procesar esas amenazas en la interfaz de usuario de Kaspersky Endpoint Security mediante la opción de añadir los objetos detectados a la lista de exclusiones del análisis.
Analizar archivos protegidos por contraseña	Si la casilla de verificación está marcada, la aplicación analiza los archivos protegidos con contraseña. Antes de que se puedan analizar los archivos de un archivador, se le solicitará que introduzca la contraseña. Si la casilla de verificación no está marcada, la aplicación omite el análisis de los archivos protegidos con contraseña.
No descomprimir archivos compuestos grandes	Si esta casilla de verificación está marcada, la aplicación no analiza archivos compuestos cuyo tamaño exceda el valor especificado. Si esta casilla de verificación no está marcada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.
Aprendizaje automático y análisis de firmas	El método de aprendizaje automático y análisis de firmas utiliza la base de datos de Kaspersky Endpoint Security, que contiene descripciones de las amenazas conocidas y métodos para erradicarlas. La protección que utiliza este método proporciona el nivel de seguridad mínimo aceptable. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.
Análisis heurístico	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
Tecnología iSwift *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
Tecnología iChecker *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

Análisis de unidades extraíbles cuando se conectan al equipo

Kaspersky Endpoint Security analiza todos los archivos que ejecuta o copia, inclusive si el archivo está ubicado en una unidad extraíble (el componente Protección frente a amenazas en archivos). A fin de evitar la propagación de virus u otro malware, puede configurar análisis automáticos de unidades extraíbles cuando estén conectadas al equipo. Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos. El componente mantiene seguro el equipo mediante la ejecución de análisis que implementan aprendizaje automático, análisis heurístico (nivel alto) y análisis de firma. Kaspersky Endpoint Security también utiliza las tecnologías de optimización de análisis iSwift e iChecker. Estas tecnologías están siempre activas y no se pueden desactivar.

Cómo configurar la ejecución del Análisis de unidades extraíbles en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Tareas locales** → **Análisis de unidades extraíbles**.
4. En la lista desplegable **Acción al conectar una unidad extraíble**, seleccione **Análisis detallado** o **Análisis rápido**.
5. Configure las opciones avanzadas para el análisis de unidades extraíbles (consulte la tabla a continuación).
6. Guarde los cambios.

Cómo configurar la ejecución del Análisis de unidades extraíbles en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Análisis de unidades extraíbles**.
5. Utilice interruptor **Análisis de unidades extraíbles ACTIVADO** para activar o desactivar el componente.
6. En el bloque **Tipo de análisis**, seleccione **Análisis detallado** o **Análisis rápido**.
7. Configure las opciones avanzadas para el análisis de unidades extraíbles (consulte la tabla a continuación).
8. Guarde los cambios.

Cómo configurar la ejecución del Análisis de unidades extraíbles en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.

3. Utilice interruptor **Análisis de unidades extraíbles** para activar o desactivar el análisis de unidades extraíbles al conectarse al equipo.

4. Configure las opciones avanzadas para el análisis de unidades extraíbles (consulte la tabla a continuación).

5. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security ejecuta un análisis de unidades extraíbles para unidades extraíbles que no superen el tamaño máximo especificado. Si no se muestra la tarea *Análisis de unidades extraíbles*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Configuración de los parámetros de análisis de unidades extraíbles

Parámetro	Descripción
Tipo de análisis	**Análisis detallado**. Si se selecciona esta opción, Kaspersky Endpoint Security analiza todos los archivos en la unidad extraíble, incluidos los archivos dentro de objetos compuestos, archivos, paquetes de distribución y archivos en formatos de Office. Kaspersky Endpoint Security no analiza archivos en formatos de correo ni archivos protegidos con contraseña. **Análisis rápido**. Si se selecciona esta opción, cuando se conecte una unidad extraíble, Kaspersky Endpoint Security analizará solo los archivos que sean de algunos formatos específicos, por ser los más propensos a estar infectados. Los objetos compuestos no se desempaquetarán.
Tamaño máximo de la unidad (MB)	Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security lleva a cabo la acción sobre las unidades extraíbles con un tamaño no superior al tamaño máximo especificado para la unidad. Si el tamaño de la unidad extraíble supera el valor configurado, Kaspersky Endpoint Security omite el análisis. Si la casilla está desactivada, Kaspersky Endpoint Security realiza la acción seleccionada en unidades extraíbles de cualquier tamaño.
Ocultar barra de progreso del análisis	Si la casilla está seleccionada, Kaspersky Endpoint Security mostrará el progreso de los análisis de unidades extraíbles en la sección **Tareas** y en una ventana separada. Si la casilla no está seleccionada, Kaspersky Endpoint Security analizará las unidades extraíbles en segundo plano.
Evitar que los usuarios detengan el análisis	Si esta casilla está seleccionada, para la tarea de análisis de unidades extraíbles en la interfaz local de Kaspersky Endpoint Security, ni el botón **Detener** en la sección **Tareas** ni el botón **Detener** en la ventana de análisis de unidades extraíbles estarán disponibles.

Análisis en segundo plano

El *Análisis en segundo plano* es uno de los modos de análisis disponibles en Kaspersky Endpoint Security. Cuando se realiza un análisis de este tipo, la aplicación no le muestra ninguna notificación al usuario. En comparación con otros tipos de análisis, como el análisis completo, un análisis en segundo plano tiene menos impacto en los recursos del equipo. En este modo, Kaspersky Endpoint Security analiza los objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema.

Para reducir el impacto en los recursos del equipo, recomendamos realizar un análisis en segundo plano en lugar de una tarea de análisis completo. El nivel de seguridad del equipo no se verá afectado. Estas tareas tienen la misma cobertura del análisis. Para optimizar la carga en el equipo, la aplicación no ejecuta una tarea de Análisis completo y una tarea de Análisis en segundo plano al mismo tiempo. Si ya ha ejecutado una tarea de Análisis completo, Kaspersky Endpoint Security no iniciará una tarea de Análisis en segundo plano en los siete días posteriores a la finalización de la tarea de Análisis completo.

La aplicación inicia un análisis en segundo plano en los siguientes casos:

- Las bases de datos antivirus se han actualizado hace poco.
- Kaspersky Endpoint Security se ha estado ejecutando por 30 minutos.

- Cada seis horas.
- Cuando el equipo está inactivo durante cinco minutos o más (el equipo está bloqueado o el protector de pantalla está encendido).

El análisis en segundo plano cuando el equipo está inactivo se interrumpe cuando se cumple alguna de las siguientes condiciones:

- El equipo entró en modo activo.

  > Si el análisis en segundo plano no se ha ejecutado desde hace más de diez días, el análisis no se interrumpe.

- El equipo (portátil) ha cambiado al modo batería.

> Cuando se realiza un análisis en segundo plano, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.

Cómo activar el análisis en segundo plano en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Tareas locales** → **Análisis en segundo plano**.
4. Utilice la casilla de verificación **Activar análisis en segundo plano** para activar o desactivar los análisis en segundo plano.
5. Guarde los cambios.

Cómo activar los análisis en segundo plano en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Protección frente a amenazas en archivos**.
5. En **Análisis en segundo plano**, use el interruptor **Análisis en segundo plano ACTIVADO** para activar o desactivar el análisis en segundo plano.
6. Guarde los cambios.

Cómo activar los análisis en segundo plano en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.

3. Utilice el interruptor **Análisis en segundo plano** para activar o desactivar los análisis en segundo plano.

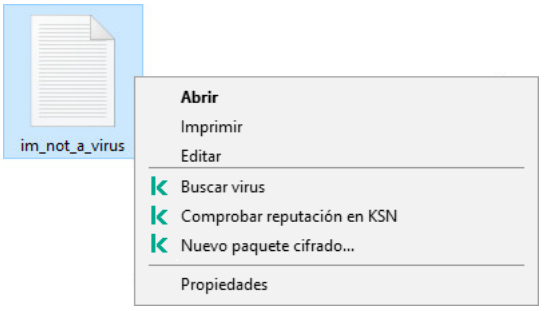
4. Guarde los cambios.

Si el *Análisis en segundo plano* no se muestra, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Analizar desde el menú contextual

Kaspersky Endpoint Security permite analizar archivos individuales en busca de virus y otras clases de malware desde el menú contextual (vea la siguiente imagen).

Cuando se realiza un análisis desde el menú contextual, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.



Analizar desde el menú contextual

Cómo configurar Analizar desde el menú contextual en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Tareas locales** → **Análisis desde el menú contextual**.

4. Configure Analizar desde el menú contextual (consulte la tabla a continuación).

5. Guarde los cambios.

Cómo configurar Analizar desde el menú contextual en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host** → **Protección frente a amenazas en archivos**.

5. En **Análisis desde el menú contextual**, configure Analizar desde el menú contextual (consulte la tabla a continuación).

6. Guarde los cambios.

Cómo configurar Analizar desde el menú contextual en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.

2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.

3. Configure Analizar desde el menú contextual (consulte la tabla a continuación).

4. Guarde los cambios.

Si no se muestra la tarea *Análisis desde el menú contextual*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Configuración de la tarea Analizar desde el menú contextual

Parámetro	Descripción
Nivel de seguridad	Kaspersky Endpoint Security puede usar diferentes grupos de parámetros para ejecutar un análisis. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*. • **Alto**. Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, la aplicación analiza archivos, paquetes de distribución, archivos de formatos de Office, pero no analiza archivos protegidos con contraseña. Cuando se establece este nivel de seguridad, la aplicación utiliza el análisis heurístico con el nivel de detalle **Análisis profundo**. • **Recomendado**. Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, la aplicación analiza archivos, paquetes de distribución, archivos de formatos de Office, pero no analiza archivos protegidos con contraseña. Cuando se establece este nivel de seguridad, la aplicación utiliza el análisis heurístico con el nivel de detalle **Análisis medio**. • **Bajo**. Kaspersky Endpoint Security analiza solo los formatos de archivo especificados. Al analizar archivos compuestos, la aplicación analiza archivos, paquetes de distribución, archivos de formatos de Office, pero no analiza archivos protegidos con contraseña. Cuando se establece este nivel de seguridad, la aplicación utiliza el análisis heurístico con el nivel de detalle **Análisis superficial**.
Acción al detectar una amenaza	**Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo. **Desinfectar; informar si falla la desinfección**. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección falla, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas. **Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.
Tipos de archivos	Kaspersky Endpoint Security considera los archivos sin extensión como ejecutables. La aplicación siempre analiza los archivos ejecutables independientemente de los tipos de archivos que elija para analizar. **Todos los archivos**. Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones). **Archivos analizados por formato**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares. **Archivos analizados por extensión**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. El formato de archivo se determina en función de su extensión. De forma predeterminada, Kaspersky Endpoint Security analiza archivos según su formato. El análisis de archivos por extensión es menos seguro porque un archivo malicioso puede tener una extensión que no está en la lista de potencialmente infectable (por ejemplo, `.123`).
Analizar solamente archivos nuevos y modificados	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
Omitir archivo cuyo análisis dure más de N segundo(s)	Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

Parámetro	Descripción
Analizar archivos	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar paquetes de distribución	La casilla de verificación activa o desactiva el análisis de los paquetes de distribución.
Analizar archivos en formatos de Microsoft Office	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
Analizar archivos de formatos de correo electrónico	Análisis de archivos en formato de correo electrónico y la base de datos de correo electrónico. La aplicación analiza los archivos PST y OST utilizados por los clientes de correo MS Outlook y Windows Mail, así como los archivos EML. Kaspersky Endpoint Security no es compatible con la versión de 64 bits del cliente de correo electrónico Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de 64 bits de Microsoft Outlook (archivos PST y OST) si hay una versión de 64 bits de Microsoft Outook instalada en el equipo, aunque el correo esté incluido en la cobertura del análisis. Si se selecciona la casilla de verificación, Kaspersky Endpoint Security fracciona el archivo de formato de correo en sus componentes (encabezado, cuerpo y archivos adjuntos) y los analiza en busca de amenazas. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza el archivo de formato de correo como un único archivo. Cuando se descubre un objeto malicioso en archivos PST u OST, Kaspersky Endpoint Security lo transforma en inofensivo de acuerdo con la acción seleccionada (por ejemplo, desinfección o eliminación del archivo). Si se detectan objetos maliciosos en archivos de otros clientes de correo electrónico (por ejemplo, Mozilla Thunderbird), Kaspersky Endpoint Security no desinfecta ni elimina esos archivos para evitar que sus mensajes de correo electrónico se eliminen involuntariamente. Kaspersky Endpoint Security solo añade información sobre los objetos detectados a la lista de amenazas activas. Debe eliminar los mensajes de correo electrónico que tengan archivos maliciosos adjuntos desde la interfaz de usuario de su cliente de correo. Si por algún motivo no es posible eliminar en ese momento los mensajes que contienen objetos maliciosos, puede procesar esas amenazas en la interfaz de usuario de Kaspersky Endpoint Security mediante la opción de añadir los objetos detectados a la lista de exclusiones del análisis.
Analizar archivos protegidos por contraseña	Si la casilla de verificación está marcada, la aplicación analiza los archivos protegidos con contraseña. Antes de que se puedan analizar los archivos de un archivador, se le solicitará que introduzca la contraseña. Si la casilla de verificación no está marcada, la aplicación omite el análisis de los archivos protegidos con contraseña.
No descomprimir archivos compuestos grandes	Si esta casilla de verificación está marcada, la aplicación no analiza archivos compuestos cuyo tamaño exceda el valor especificado. Si esta casilla de verificación no está marcada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.
Aprendizaje automático y análisis de firmas	El método de aprendizaje automático y análisis de firmas utiliza la base de datos de Kaspersky Endpoint Security, que contiene descripciones de las amenazas conocidas y métodos para erradicarlas. La protección que utiliza este método proporciona el nivel de seguridad mínimo aceptable. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.
Análisis heurístico	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
Tecnología iSwift	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
Tecnología iChecker	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

Comprobación de integridad de la aplicación

Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en busca de datos corruptos o modificaciones. Si detecta, por ejemplo, que una de las bibliotecas no tiene la firma digital correcta, considera que la biblioteca está dañada. Los archivos de la aplicación se comprueban a través de la tarea *Comprobación de integridad de la aplicación*. Recomendamos que ejecute la tarea *Comprobación de integridad de la aplicación* si observa que Kaspersky Endpoint Security detecta, pero no neutraliza, un objeto malicioso.

Puede crear la tarea *Comprobación de integridad de la aplicación* en Kaspersky Security Center Web Console y en la Consola de administración. No se puede crear una tarea en Kaspersky Security Center Cloud Console.

Las siguientes situaciones pueden comprometer la integridad de la aplicación:

- Un objeto malicioso modifica los archivos de Kaspersky Endpoint Security. Ante esta situación, siga el procedimiento para restaurar Kaspersky Endpoint Security con las herramientas del sistema operativo. Cuando concluya la restauración, realice un análisis completo del equipo y ejecute nuevamente la comprobación de integridad.

- La firma digital llega a su fecha de caducidad. Ante esta situación, actualice Kaspersky Endpoint Security.

Cómo ejecutar una comprobación de integridad de aplicación mediante la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Comprobación de integridad de la aplicación**.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando se detecte un brote de virus.

Paso 4. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Comprobación de integridad después de que se haya infectado el equipo*.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique de forma programada (consulte la tabla a continuación).

Cómo ejecutar una comprobación de integridad de aplicación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Comprobación de integridad de la aplicación**.

c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Comprobar la integridad de la aplicación tras una infección*).

d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Active la casilla ubicada junto a la tarea.

Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique de forma programada (consulte la tabla a continuación).

Cómo ejecutar una comprobación de integridad en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.

2. Esto abre la lista de tareas. Seleccione la tarea *Comprobación de integridad de la aplicación* y haga clic en **Ejecutar**.

Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique de forma programada (consulte la tabla a continuación). Si no se muestra la tarea *Comprobación de integridad de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Configuración de la tarea de Comprobación de integridad

Parámetro	Descripción
Programación de análisis	**Manualmente**. Modo de ejecución en el que puede comenzar a analizar manualmente en el momento que sea conveniente para usted. **Según programación**. En este modo de ejecución de la tarea de análisis, la aplicación comienza el análisis en función de la programación especificada. Si está seleccionado este modo de ejecución de la tarea de análisis, también puede iniciar la tarea de análisis manualmente.
Ejecutar tareas omitidas	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security iniciará la tarea omitida lo antes posible. La tarea se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programado de la tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas omitidas, las ejecuta de manera aleatoria dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no iniciará las tareas omitidas. En lugar de ello, lleva a cabo la siguiente tarea de acuerdo con la planificación actual.
Ejecutar solo cuando el equipo está inactivo	Inicio pospuesto de la tarea cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.

Edición de la cobertura del análisis

La *Cobertura del análisis* es una lista de rutas a carpetas y rutas que Kaspersky Endpoint Security analiza al ejecutar la tarea. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

Para editar la cobertura del análisis, recomendamos usar la tarea de *Análisis personalizado*. Los expertos de Kaspersky recomiendan que no cambie la cobertura del análisis de las tareas de *Análisis completo* y *Análisis de áreas críticas*.

Kaspersky Endpoint Security tiene los siguientes objetos predefinidos como parte de la cobertura del análisis:

- **Memoria del sistema**.
- **Procesos en ejecución y objetos de arranque**.

  Memoria ocupada por procesos y archivos ejecutables de aplicaciones que se ejecutan al iniciar el sistema.
- **Sectores de arranque del disco**.

  Sectores de arranque del disco duro y del disco extraíble.
- **Copia de seguridad del sistema**.

  Contenido de la carpeta System Volume Information.
- **Todos los dispositivos externos**.
- **Todos los discos duros**.
- **Todas las unidades de red**.

  En Kaspersky Endpoint Security para Windows 12.12, el correo electrónico está excluido de la cobertura del análisis de la aplicación. El análisis de los mensajes de correo electrónico entrantes y salientes lo realiza el componente Protección frente a amenazas en el correo. Si está utilizando una versión anterior del complemento de administración, la aplicación excluye el correo electrónico del alcance del análisis, incluso si la directiva lo incluye.

  Recomendamos crear una tarea de análisis separada para analizar unidades de red o carpetas compartidas. En los ajustes de la tarea *Análisis antimalware*, especifique un usuario que tenga acceso de escritura a esta unidad; esto es necesario para mitigar las amenazas detectadas. Si el servidor donde se encuentra la unidad de red tiene sus propias herramientas de seguridad, no ejecute la tarea de análisis para esa unidad. De esta forma, puede evitar comprobar el objeto dos veces, y mejorar así el rendimiento del servidor.

Para excluir carpetas o archivos de la cobertura del análisis, añada la carpeta o el archivo a la zona de confianza.

Cómo editar una cobertura del análisis en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.
   Si es necesario, cree la tarea de *Análisis antimalware*.
4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
5. En la sección **Cobertura del análisis**, haga clic en **Configuración**.
6. En la ventana que se abre, seleccione los objetos que desea añadir o excluir de la cobertura del análisis.
7. Si desea añadir un nuevo objeto a la cobertura del análisis:
   a. Haga clic en **Añadir**.
   b. En el campo **Objeto**, introduzca la ruta a la carpeta o archivo.
      Usar máscaras:
      - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
      - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
      - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

      Puede utilizar máscaras en cualquier parte de la ruta de un archivo o carpeta. Por ejemplo, si desea que la cobertura del análisis incluya la carpeta descargas para todas las cuentas de usuario del equipo, ingrese la máscara `C:\Users\*\Downloads\`.

      El objeto **Este equipo** de la lista de recursos de archivos del equipo incluye los siguientes objetos: **Todos los discos duros**, **Todas las unidades de red** y **Todas las unidades extraíbles**.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura del análisis. Para hacerlo, desactive la casilla de verificación junto al objeto.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo editar una cobertura del análisis en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Tareas**.
   Se abre la lista de tareas.

2. Haga clic en la tarea de análisis.

   Se abre la ventana propiedades de la tarea. Si es necesario, cree la tarea de *Análisis antimalware*.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. En la sección **Cobertura del análisis**, seleccione los objetos que desea añadir o excluir de la cobertura del análisis.

5. Si desea añadir un nuevo objeto a la cobertura del análisis:

   a. Haga clic en **Añadir**.

   b. Ingrese la ruta para la carpeta o el archivo.

      Usar máscaras:

      - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

      - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

      - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

      Puede utilizar máscaras en cualquier parte de la ruta de un archivo o carpeta. Por ejemplo, si desea que la cobertura del análisis incluya la carpeta descargas para todas las cuentas de usuario del equipo, ingrese la máscara `C:\Users\*\Downloads\`.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura del análisis. Para hacerlo, coloque el interruptor junto a él en la posición de apagado.

6. Guarde los cambios.

Cómo editar una cobertura del análisis en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.

2. Esto abre la lista de tareas. Seleccione la tarea *Análisis personalizado* y haga clic en **Seleccionar**.

   También puede editar la cobertura del análisis para otras tareas. Los expertos de Kaspersky recomiendan que no cambie la cobertura del análisis de las tareas de *Análisis completo* y *Análisis de áreas críticas*.

3. En la ventana que se abre, seleccione los objetos que desea añadir a la cobertura del análisis.

4. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Análisis programado en ejecución

Buscar malware con la tarea *Análisis antimalware* puede llevar mucho tiempo y aumentar el uso que Kaspersky Endpoint Security hace de los recursos del equipo. Por lo tanto, se recomienda seleccionar un momento óptimo para ejecutar la tarea, de modo que se minimice el impacto en el rendimiento de otras aplicaciones.

Por ejemplo, si los empleados de su organización trabajan en un horario fijo, puede configurar la ejecución de un análisis de los equipos por la noche o los fines de semana. Si no es posible iniciar la tarea por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se inicie automáticamente lo antes posible. Esta función debe usarse con precaución, ya que puede ralentizar las aplicaciones en el equipo del usuario cuando este se enciende por la mañana.

Si no puede determinar una programación de análisis óptima que se ajuste a sus necesidades, puede configurar la ejecución del análisis cuando se cumpla una de las siguientes condiciones especiales:

- Después de una actualización de las bases de datos.

  Kaspersky Endpoint Security ejecuta el análisis del equipo con las bases de datos de firmas actualizadas.

- Después de iniciar la aplicación.

  Kaspersky Endpoint Security ejecuta un análisis del equipo tras un período específico de tiempo después de iniciar la aplicación. Dado que se ejecutan varios procesos al iniciar el sistema operativo, es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después del inicio de Kaspersky Endpoint Security.

- Función Wake-on-LAN.

  Kaspersky Endpoint Security ejecuta un análisis del equipo según lo programado, incluso si el equipo está apagado. Para hacerlo, la aplicación utiliza la función Wake-on-LAN del sistema operativo. La función Wake-on-LAN permite encender el equipo de forma remota mediante el envío de una señal especial a través de la red local. Para utilizar esta función, debe activar Wake-on-LAN en la configuración del BIOS.

  Puede configurar la ejecución del análisis mediante Wake-on-LAN solo para la tarea de *Análisis antimalware* en Kaspersky Security Center. No puede activar Wake-on-LAN para analizar el equipo en la interfaz de la aplicación.

- Cuando el equipo está inactivo.

  Kaspersky Endpoint Security ejecuta un análisis del equipo según lo programado cuando el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security suspende el análisis. En este caso, el análisis completo puede tardar varios días en completarse.

- Cuando se ha omitido la tarea.

  Kaspersky Endpoint Security ejecuta la tarea omitida en cuanto es posible. La tarea se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programado de la tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas omitidas, las ejecuta de manera aleatoria dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo.

Cómo configurar la programación del análisis en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en la tarea de análisis.

   Se abre la ventana propiedades de la tarea.

3. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.

4. Configure la programación de la tarea de análisis.

5. Según la frecuencia seleccionada, ajuste la configuración avanzada que especifica la planificación de la ejecución de la tarea (ver la tabla a continuación).

6. Guarde los cambios.

Cómo configurar la programación del análisis en la interfaz de la aplicación

Puede configurar la programación del análisis solo si no se aplica una directiva al equipo. Para equipos con una directiva, puede configurar la programación de la tarea de *Análisis antimalware* en Kaspersky Security Center.

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.

2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.

   Puede configurar una programación para ejecutar un análisis completo, un análisis de áreas críticas o una comprobación de integridad. Solo puede ejecutar un análisis personalizado manualmente.

3. Haga clic en **Programación de análisis**.

4. En la ventana que se abre, configure el programa de ejecución de la tarea de análisis.

5. Según la frecuencia seleccionada, ajuste la configuración avanzada que especifica la planificación de la ejecución de la tarea (ver la tabla a continuación).

6. Guarde los cambios.

Configuración de la programación del análisis

Parámetro	Descripción
Programación de análisis	**Manualmente**. Modo de ejecución en el que puede comenzar a analizar manualmente en el momento que sea conveniente para usted. **Según programación**. En este modo de ejecución de la tarea de análisis, la aplicación comienza el análisis en función de la programación especificada. Si está seleccionado este modo de ejecución de la tarea de análisis, también puede iniciar la tarea de análisis manualmente.
Posponer ejecución después del inicio de la aplicación durante N minutos	Inicio pospuesto de la tarea de análisis después del inicio de la aplicación. Dado que se ejecutan varios procesos al iniciar el sistema operativo, es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después del inicio de Kaspersky Endpoint Security.
Ejecutar tareas omitidas	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security iniciará la tarea omitida lo antes posible. La tarea se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programado de la tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas omitidas, las ejecuta de manera aleatoria dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no iniciará las tareas omitidas. En lugar de ello, lleva a cabo la siguiente tarea de acuerdo con la planificación actual.
Ejecutar solo cuando el equipo está inactivo	Inicio pospuesto de la tarea cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.

Parámetro	Descripción
Usar un retraso aleatorio automático para el inicio de las tareas *(disponible solo en la Consola de Kaspersky Security Center)*	Si se selecciona la casilla de verificación, la tarea no se ejecuta estrictamente según lo programado, sino aleatoriamente dentro de un intervalo determinado, es decir, se distribuyen las horas de inicio de la tarea. Las horas de inicio aleatorias ayudan a evitar que una gran cantidad de equipos accedan simultáneamente al Servidor de administración cuando la tarea se ejecuta según lo programado. El intervalo de horas de inicio aleatorias se calcula automáticamente cuando se crea la tarea, según la cantidad de equipos que tienen la tarea asignada. Posteriormente, la tarea siempre se ejecuta a la hora de inicio calculada. Sin embargo, siempre que se modifique la configuración de la tarea o la tarea se ejecute manualmente, la hora de inicio calculada cambia. Si la casilla de verificación está desactivada, la tarea se ejecuta exactamente a la hora programada.
Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)	Si esta casilla de verificación está seleccionada, la tarea se ejecuta en los equipos a una hora aleatoria dentro de un período de tiempo determinado. Las horas de inicio aleatorias ayudan a evitar que una gran cantidad de equipos accedan simultáneamente al Servidor de administración cuando la tarea se ejecuta según lo programado. Si la casilla de verificación está desactivada, la tarea se ejecuta exactamente a la hora programada.
Detener la tarea si tarda más de (min) *(disponible solo en la Consola de Kaspersky Security Center)*	Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado. Para reducir el tiempo de ejecución de la tarea, puede, por ejemplo, configurar el alcance del análisis u optimizar el análisis.
Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea (min) *(disponible solo en la Consola de Kaspersky Security Center)*	Si se selecciona la casilla de verificación, el sistema operativo del equipo recibe un tiempo de espera especificado para completar el inicio antes de que se ejecute la tarea. El tiempo de espera predeterminado es de 5 minutos. Seleccione la casilla de verificación si desea ejecutar la tarea en todos los equipos, incluidos los que están apagados.
Apagar los dispositivos después de completar la tarea *(disponible solo en la Consola de Kaspersky Security Center)*	Si esta casilla de verificación está seleccionada, el equipo se apagará una vez completada la tarea. Por ejemplo, puede habilitar esta funcionalidad para analizar el equipo los viernes después del horario laboral. Cuando finaliza la tarea, la aplicación apaga el equipo durante el fin de semana.
Suspender tarea	Puede especificar un intervalo de tiempo durante el cual se pausará la ejecución de una tarea programada anteriormente. Una vez que finalice el período de tiempo especificado, la tarea se reanudará. Esto puede ser necesario, por ejemplo, para minimizar el impacto de Kaspersky Endpoint Security en el rendimiento de su equipo durante los períodos de máximo uso.
Desactivar planificación desde	Si la casilla está seleccionada, Kaspersky Endpoint Security dejará de ejecutar la tarea programada a partir de la fecha especificada. La tarea se establecerá en el modo **Manual**.

Ejecutar un análisis como un usuario diferente

Por defecto, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. La cobertura de la protección puede incluir unidades de red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que tenga los permisos adecuados en la configuración de la aplicación y realizar la tarea de análisis con esta cuenta de usuario.

Puede ejecutar los siguientes análisis como un usuario diferente:

- Análisis de áreas críticas.
- Análisis completo.
- Análisis personalizado.
- Analizar desde el menú contextual.

No puede configurar los derechos de usuario para ejecutar un Análisis de unidades extraíbles, un Análisis en segundo plano ni una Comprobación de integridad.

Cómo ejecutar un análisis como un usuario diferente en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Tareas**.
4. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.
5. En la ventana de propiedades de la tarea, seleccione la sección **Cuenta**.
6. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar una tarea de análisis.
7. Guarde los cambios.

Cómo ejecutar un análisis como un usuario diferente en Web Console o Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en la tarea de análisis.

   Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Configuración**.
4. En el bloque **Cuenta**, haga clic en el botón **Configuración**.
5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar una tarea de análisis.
6. Guarde los cambios.

Cómo ejecutar un análisis como un usuario diferente en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.
3. En las propiedades de la tarea, seleccione **Configuración avanzada** → **Ejecutar el análisis como**.
4. En la ventana que se abre, introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar una tarea de análisis.
5. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Optimización del análisis

Limitar el uso de la CPU al analizar el equipo

Puede limitar el uso de CPU al ejecutar la tarea *Análisis antimalware*. Esto puede aumentar el tiempo que lleva analizar su equipo.

Cómo limitar el uso de la CPU al analizar el equipo en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de la aplicación**.
4. En **Rendimiento**, seleccione la casilla de verificación **Limitar uso de CPU para tareas de análisis** e introduzca el valor medio del consumo de recursos de la CPU en porcentaje.
5. Guarde los cambios.

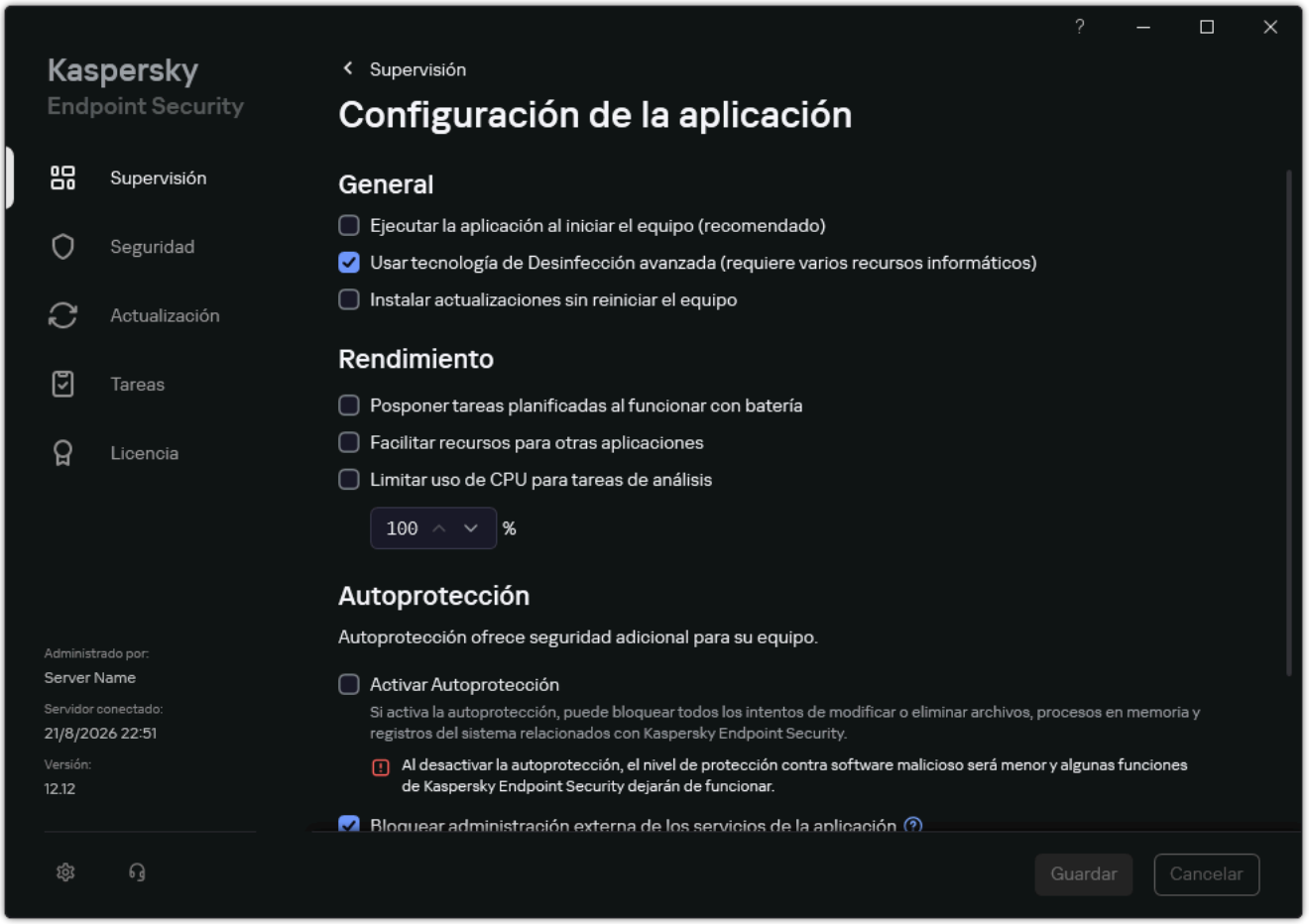
Cómo limitar el uso de la CPU al analizar el equipo en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Rendimiento**.
5. En **Limitar uso de CPU para tareas de análisis**, sitúe el interruptor en **Limitar uso de CPU para tareas de análisis** e introduzca el valor medio del consumo de recursos de la CPU en porcentaje.
6. Guarde los cambios.

Cómo limitar el uso de la CPU al analizar el equipo en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. En **Rendimiento**, seleccione la casilla de verificación **Limitar uso de CPU para tareas de análisis** e introduzca el valor medio del consumo de recursos de la CPU en porcentaje.

4. Guarde los cambios.

Configurar parámetros de la tarea avanzados para Análisis antimalware.

Puede optimizar el análisis de archivos: reduzca el tiempo de análisis y aumente la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede conseguir si analiza solamente los archivos nuevos y los que se hayan modificado desde el último análisis. Este modo se aplica tanto a archivos simples como a compuestos. También puede establecer un límite para la duración del análisis de un único archivo. Cuando se supera el intervalo de tiempo especificado, Kaspersky Endpoint Security excluye el archivo del análisis actual (excepto los archivos y objetos que incluyen varios archivos).

Una técnica común para ocultar virus y otro tipo de software malicioso (malware) consiste en implantarlos en archivos compuestos, como archivos comprimidos o bases de datos. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

También puede activar las tecnologías iChecker e iSwift. Las tecnologías iChecker e iSwift optimizan la velocidad del análisis de archivos ya que excluyen archivos que no han sido modificados desde el análisis más reciente.

Cómo optimizar el análisis en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.

   Si es necesario, cree la tarea de *Análisis antimalware*.
4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
5. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.

   Esto abre la ventana de configuración de la tarea de análisis.
6. En el bloque **Optimización**, establezca la configuración del análisis:

   - **Analizar solamente archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.

     También puede configurar el análisis de archivos nuevos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo archivos comprimidos nuevos y archivos de formato Office.

   - **Omitir archivos analizados durante más de N s**. Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

   - **No ejecute varias tareas de análisis al mismo tiempo**. Posponga las tareas de análisis planificadas si aún se está ejecutando un análisis planificado iniciado anteriormente. Kaspersky Endpoint Security pondrá en cola las tareas de análisis planificadas si el análisis actual sigue en curso. Esto ayuda a optimizar la carga en el equipo. Por ejemplo, ha planificado tareas de análisis para que se ejecuten a las 6:00 p. m. y a las 8:00 p. m. Kaspersky Endpoint Security pospondrá la tarea de análisis de las 8:00 p. m. si la tarea de análisis planificada para las 6:00 p. m. aún se está ejecutando. La aplicación ejecutará un análisis cuando finalice la tarea iniciada a las 6:00 p. m.
7. Haga clic en **Adicional**.

   Esto abre la ventana de configuración de análisis de archivos compuestos.
8. En el bloque **Límite de tamaño**, seleccione la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**. Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

   Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.
9. Haga clic en **Aceptar**.
10. Vaya a la pestaña **Adicional**.

11. En el bloque **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar durante un análisis:

    - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

    - **Tecnología iChecker**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

12. Guarde los cambios.

Cómo optimizar el análisis en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Tareas**.

   Se abre la lista de tareas.

2. Haga clic en la tarea de análisis.

   Se abre la ventana propiedades de la tarea. Si es necesario, cree la tarea de *Análisis antimalware*.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. En el bloque **Acción al detectar una amenaza**, seleccione la casilla de verificación **Analizar solamente archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.

   También puede configurar el análisis de archivos nuevos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo archivos comprimidos nuevos y archivos de formato Office.

5. En el bloque **Optimización de análisis**, seleccione la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**. Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

   Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

6. Seleccione la casilla **No ejecute varias tareas de análisis al mismo tiempo**. Posponga las tareas de análisis planificadas si aún se está ejecutando un análisis planificado iniciado anteriormente. Kaspersky Endpoint Security pondrá en cola las tareas de análisis planificadas si el análisis actual sigue en curso. Esto ayuda a optimizar la carga en el equipo. Por ejemplo, ha planificado tareas de análisis para que se ejecuten a las 6:00 p. m. y a las 8:00 p. m. Kaspersky Endpoint Security pospondrá la tarea de análisis de las 8:00 p. m. si la tarea de análisis planificada para las 6:00 p. m. aún se está ejecutando. La aplicación ejecutará un análisis cuando finalice la tarea iniciada a las 6:00 p. m.

7. En el bloque **Configuración avanzada**, seleccione la casilla de verificación **Omitir archivo cuyo análisis dure más de (seg)**. Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

8. Guarde los cambios.

Cómo optimizar el análisis en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.

2. En la lista de tareas, seleccione la tarea de análisis y haga clic en ⚙.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Optimización**, establezca la configuración del análisis:

   - **Analizar solamente archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.

     También puede configurar el análisis de archivos nuevos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo archivos comprimidos nuevos y archivos de formato Office.

   - **Omitir archivo cuyo análisis dure más de N segundo(s)**. Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

   - **No ejecute varias tareas de análisis al mismo tiempo**. Posponga las tareas de análisis planificadas si aún se está ejecutando un análisis planificado iniciado anteriormente. Kaspersky Endpoint Security pondrá en cola las tareas de análisis planificadas si el análisis actual sigue en curso. Esto ayuda a optimizar la carga en el equipo. Por ejemplo, ha planificado tareas de análisis para que se ejecuten a las 6:00 p. m. y a las 8:00 p. m. Kaspersky Endpoint Security pospondrá la tarea de análisis de las 8:00 p. m. si la tarea de análisis planificada para las 6:00 p. m. aún se está ejecutando. La aplicación ejecutará un análisis cuando finalice la tarea iniciada a las 6:00 p. m.

5. En el bloque **Límite de tamaño**, seleccione la casilla de verificación **No descomprimir archivos compuestos grandes**. Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.

   Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos grandes**.

6. En el bloque **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar durante un análisis:

   - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

   - **Tecnología iChecker**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

7. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

Actualización de las bases de datos y módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antivirus y de la base de código) y la función de KSN pueden dejar de estar disponibles en la aplicación en el territorio de EE. UU.

Las actualizaciones regulares requieren una licencia efectiva. Si no hay ninguna licencia actual, solamente podrá realizar una actualización una vez.

Su equipo debe estar conectado a Internet para descargar satisfactoriamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. De forma predeterminada, los parámetros de conexión a Internet se determinan automáticamente. Si utiliza un servidor proxy, debe ajustar la configuración del servidor proxy.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTPS.

Mientras se lleva a cabo la actualización, se descargan e instalan los siguientes objetos en su equipo:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se proporciona por medio de bases de datos que contienen firmas de virus y otras amenazas, así como información sobre la forma de neutralizarlas. Los componentes de protección emplean esta información a la hora de buscar y neutralizar archivos infectados en el equipo. Las bases de datos se actualizan constantemente con registros de nuevas amenazas y métodos para combatirlas. Por tanto, es recomendable que actualice la base de datos con regularidad.

  Además de las bases de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de protección interceptar el tráfico de la red.

- Módulos de la aplicación. Aparte de las bases de datos de Kaspersky Endpoint Security, también puede actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación sirve para solucionar vulnerabilidades en Kaspersky Endpoint Security, añade nuevas funciones o mejora las existentes.

Durante una actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con los de la versión actualizada en el origen de actualizaciones. Si los módulos de la aplicación y las bases de datos actuales son diferentes de sus respectivas versiones actualizadas, la parte de las actualizaciones que falte se instala en su equipo.

Si las bases de datos no están actualizadas, puede que el tamaño del paquete de actualización sea considerable, lo que provocaría un tráfico de internet adicional (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en la ventana principal de la aplicación o en la información sobre herramientas que ve cuando pasa el cursor sobre el icono de la aplicación en el área de notificación.

La información sobre los resultados de la actualización y sobre todos los eventos se producen durante la ejecución de la tarea de actualización se registra en el informe de Kaspersky Endpoint Security.

Si la aplicación funciona en modo Light Agent, hay consideraciones especiales que afectan a la actualización de las bases de datos y los módulos de la aplicación.

Escenarios de actualización de las bases de datos y los módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

Los objetos que se actualizan en los equipos de los usuarios son los siguientes:

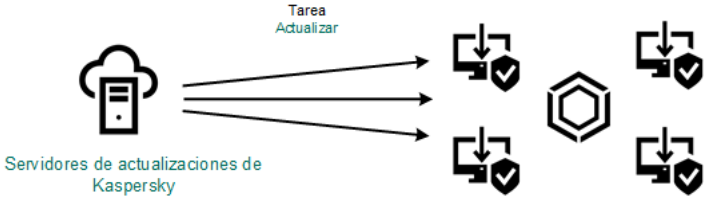
- Bases de datos antivirus. Las bases de datos antivirus contienen bases de datos con firmas de malware, descripciones de ataques de red, bases de datos de direcciones web fraudulentas y maliciosas, bases de datos de banners, bases de datos de spam y otras clases de información.

- Módulos de la aplicación. Las actualizaciones de módulos están diseñadas para eliminar vulnerabilidades de la aplicación y mejorar los métodos con los que se protegen los equipos. Cuando se actualizan los módulos, la aplicación puede sumar nuevas funciones y modificar el comportamiento de sus componentes.

Las bases de datos y los módulos de Kaspersky Endpoint Security pueden actualizarse de las siguientes maneras:

- Actualización con los servidores de Kaspersky.

  Los servidores de actualización de Kaspersky están ubicados en varios países del mundo. Gracias a ello, el proceso de actualización es altamente fiable. Cuando Kaspersky Endpoint Security no puede descargar las actualizaciones de un servidor, cambia a uno distinto.



Actualización con los servidores de Kaspersky

- Actualización centralizada.

  La actualización centralizada reduce el tráfico de Internet externo y facilita el control del proceso.

  La actualización centralizada consta de los siguientes pasos:

  1. Descargar el paquete de actualización a un repositorio ubicado en la red de la organización.

     Para descargar el paquete de actualización, se utiliza la tarea del Servidor de administración llamada *Descargar actualizaciones en el repositorio del Servidor de administración*.

  2. Descargar el paquete de actualización a una carpeta compartida (opcional).

Para descargar el paquete de actualización a una carpeta compartida, puede usar los siguientes métodos:

- Uso de la tarea *Actualización de las bases de datos y módulos de la aplicación* de Kaspersky Endpoint Security. Esta tarea está destinada a uno de los equipos en la red de la compañía local.

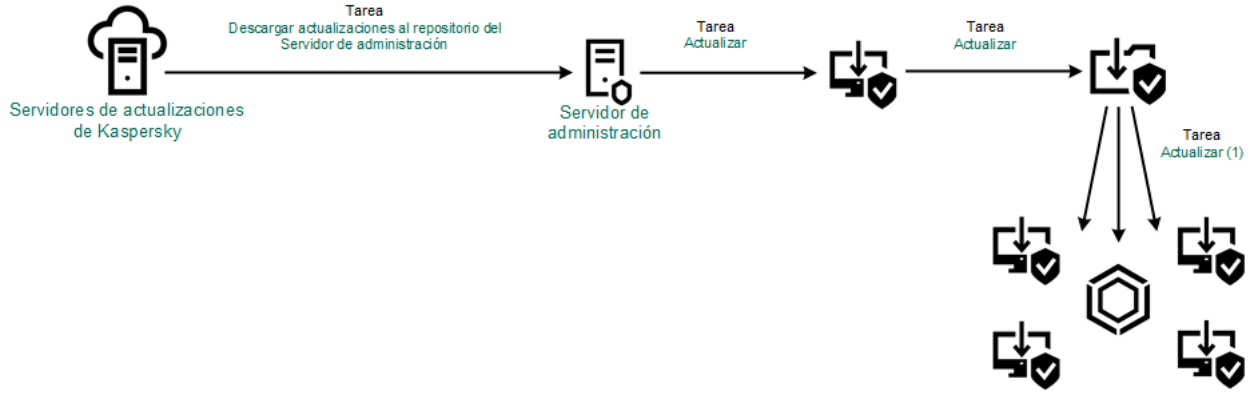
- Usar la herramienta Kaspersky Update Utility. Para obtener información detallada sobre el uso de Kaspersky Update Utility, consulte la Base de conocimientos de Kaspersky.

3. Distribuir el paquete de actualización a los equipos cliente.

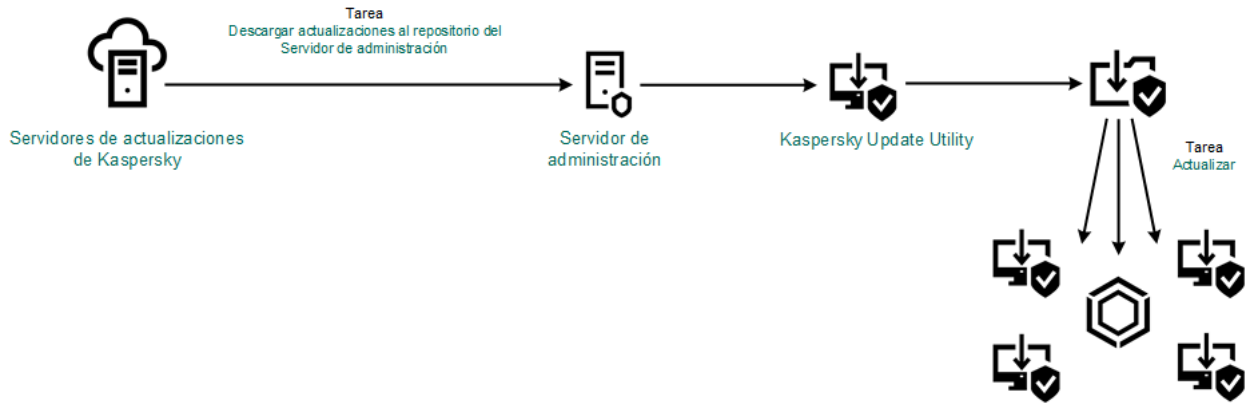
   Para distribuir el paquete a los equipos cliente, utilice la tarea *Actualización de las bases de datos y módulos de la aplicación* de Kaspersky Endpoint Security. Podrá crear cuantas tareas de actualización necesite para cada grupo de administración.



Actualización con un repositorio de servidor



Actualización con una carpeta compartida



Actualización con Kaspersky Update Utility

Para Kaspersky Security Center, la lista predeterminada de orígenes de actualizaciones contiene los servidores de actualización del Servidor de administración de Kaspersky Security Center y de Kaspersky. Para Kaspersky Security Center Cloud Console, la lista predeterminada de orígenes de actualizaciones contiene los servidores de actualización de Kaspersky y los puntos de distribución. Para obtener más información sobre puntos de distribución, consulte la Ayuda de Kaspersky Security Center Cloud Console. Puede agregar a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones. Cuando Kaspersky Endpoint Security no puede descargar las actualizaciones de un origen, cambia a uno distinto.

Las actualizaciones se descargan de los servidores de actualizaciones de Kaspersky, o de otros servidores FTP o HTTP, usando protocolos de red estándar. Si la conexión al origen de actualizaciones debe establecerse a través de un servidor proxy, especifique los parámetros de conexión pertinentes en los ajustes de directiva de Kaspersky Endpoint Security.

Actualización con un repositorio de servidor

Para reducir el tráfico de Internet, los equipos conectados a la LAN de la organización pueden obtener las actualizaciones de las bases de datos y de los módulos de la aplicación de un repositorio de servidor. En esta modalidad, Kaspersky Security Center descarga un paquete de actualización de los servidores de actualizaciones de Kaspersky y lo guarda en un repositorio (un servidor FTP o HTTP, una carpeta de red o una carpeta local). Los demás equipos conectados a la LAN obtienen de allí el paquete de actualización.

Si desea utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. Configurar la descarga de un paquete de actualización al repositorio del Servidor de administración (tarea *Descargar actualizaciones en el repositorio del Servidor de administración*).

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*; solo puede existir un ejemplar de esta tarea. De forma predeterminada, Kaspersky Security Center copia el paquete de actualización en la carpeta `\\<server name>\KLSHARE\Updates`. Para obtener más información sobre la descarga de actualizaciones al repositorio del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

2. Configurar el proceso de actualización para que los demás equipos de la LAN de la organización obtengan las bases de datos y los módulos de la aplicación más recientes del repositorio especificado (tarea *Actualización de las bases de datos y módulos de la aplicación*).

   Cómo configurar la actualización de Kaspersky Endpoint Security desde el almacenamiento del servidor especificado en la Consola de administración (MMC)

   1. Abra la Consola de administración de Kaspersky Security Center.

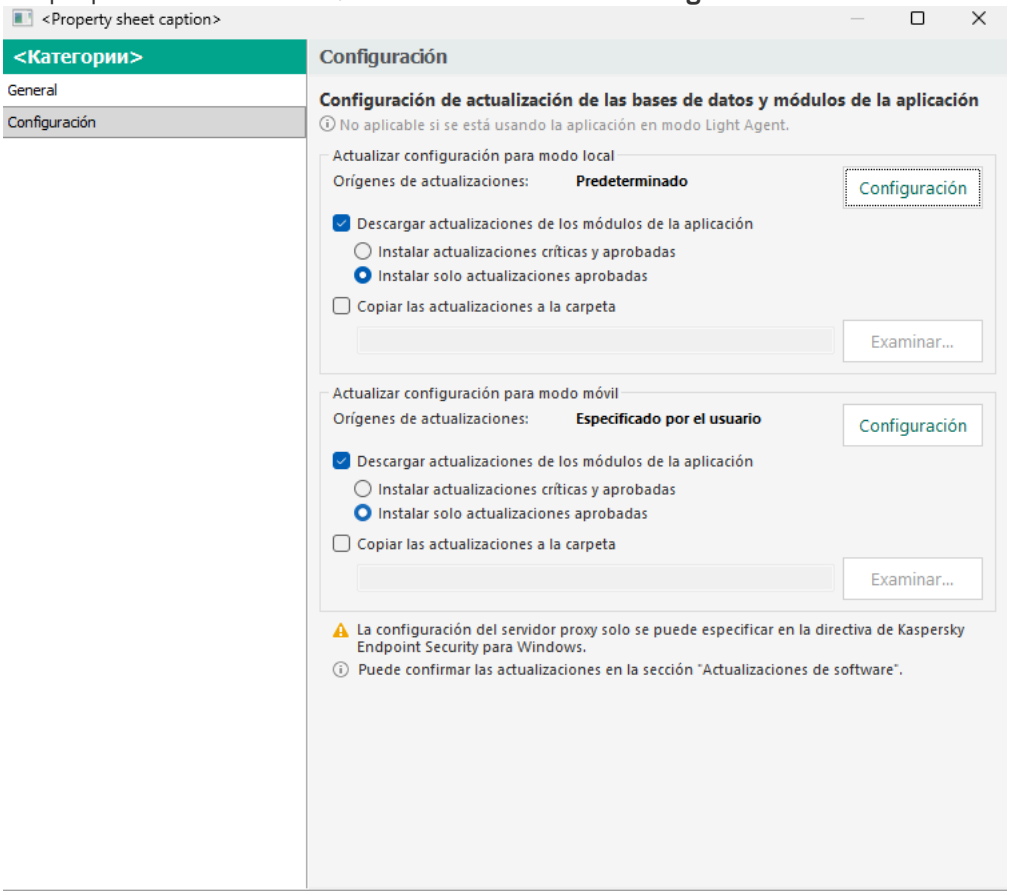
      En el árbol de la consola, seleccione **Tareas**.

   2. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

      Se abre la ventana propiedades de la tarea.

      La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de las bases de datos y módulos de la aplicación

4. En el bloque **Actualizar configuración para modo local**, haga clic en el botón **Configuración**.

5. En la lista de fuentes de actualización, asegúrese de que la actualización de la fuente de **Kaspersky Security Center** está activada. Además, la fuente de **Kaspersky Security Center** debe tener la prioridad más alta.

6. Si es necesario, añada las fuentes de actualización:

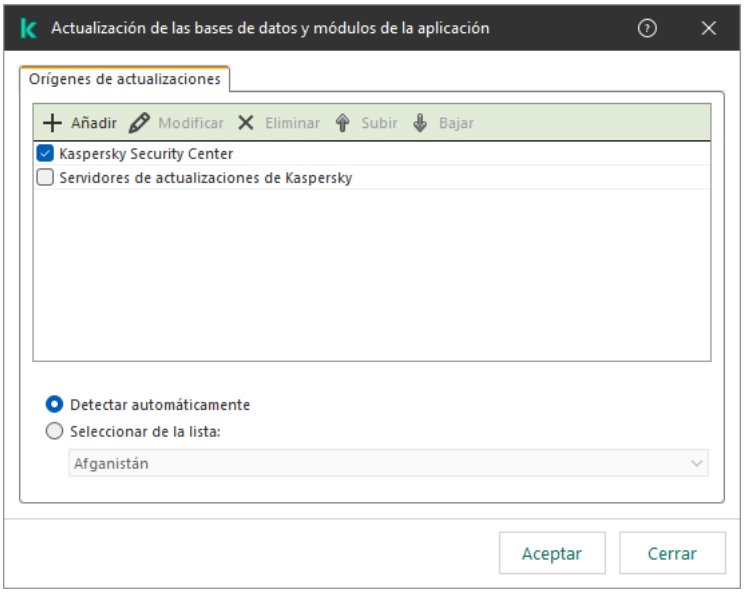
   a. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.

   b. En el campo **Orígenes de actualizaciones**, escriba la dirección del servidor FTP/HTTP, carpeta local o carpeta de red en donde Kaspersky Security Center guardará el paquete de actualización que reciba de los servidores de Kaspersky.

      La dirección de la fuente de actualización debe coincidir con la dirección que especificó en el campo **Carpeta para almacenar actualizaciones** cuando configuró la descarga de actualizaciones en el almacenamiento del servidor (tarea *Descargar actualizaciones en el repositorio del Servidor de administración*).

   c. Haga clic en **Aceptar**.

Puede excluir la fuente de actualización sin eliminarla de la lista de fuentes de actualización. Para hacerlo, desactive la casilla de verificación junto al objeto.



Fuentes de actualización

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

8. En la ventana de propiedades de la tarea, seleccione la sección **Programación** y configure el modo de ejecución de la tarea.

9. De forma predeterminada, Kaspersky Endpoint Security ejecuta la tarea en modo manual.

10. Guarde los cambios.

Cómo configurar la actualización de Kaspersky Endpoint Security desde el almacenamiento del servidor especificado en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. Seleccione la pestaña **Configuración de la aplicación → Modo local**.

4. En la lista de fuentes de actualización, asegúrese de que la actualización de la fuente de **Kaspersky Security Center** está activada. Además, la fuente de **Kaspersky Security Center** debe tener la prioridad más alta.

5. Si es necesario, añada las fuentes de actualización:

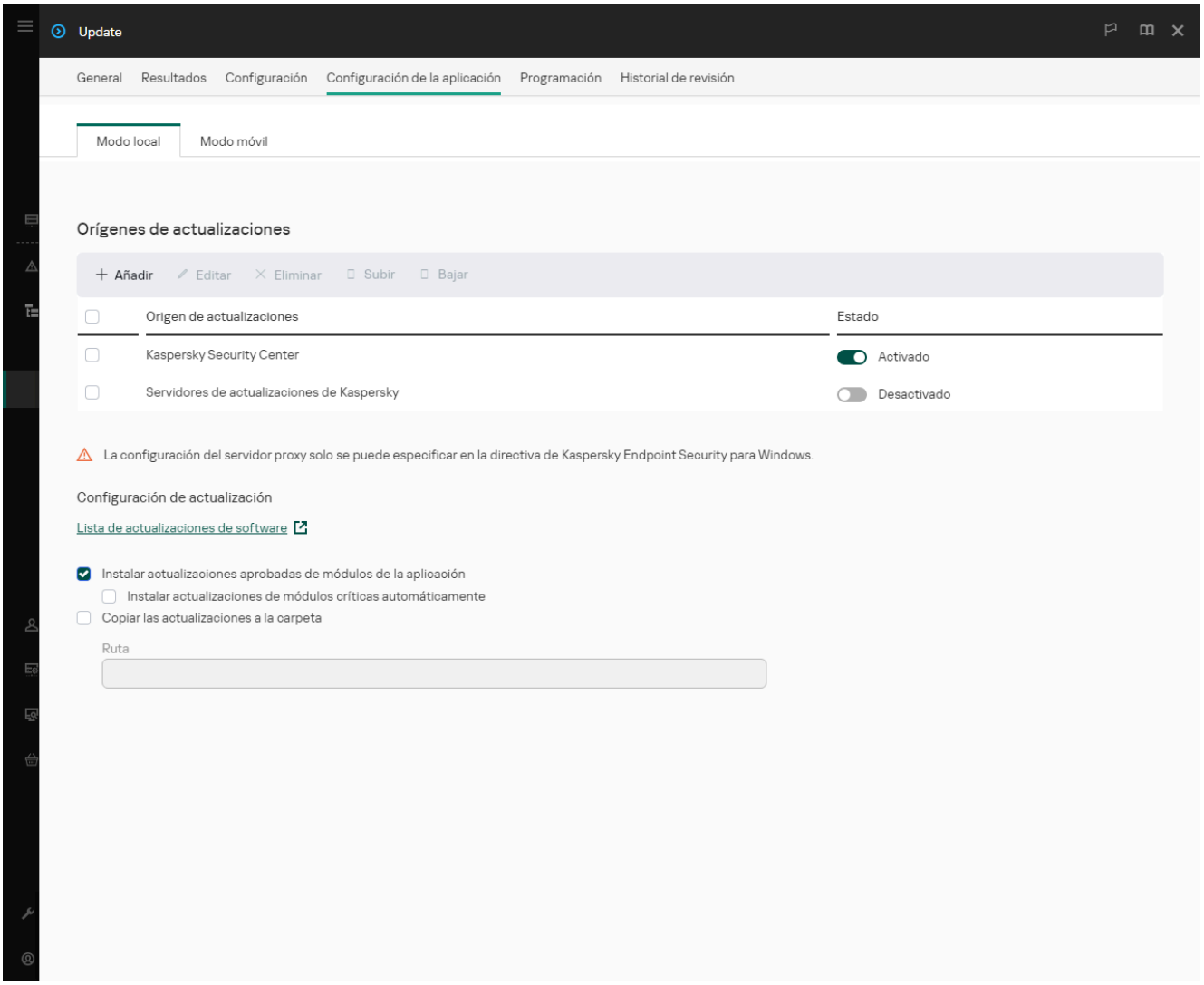
   a. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.

   b. En el campo **Orígenes de actualizaciones**, escriba la dirección del servidor FTP/HTTP, carpeta local o carpeta de red en donde Kaspersky Security Center guardará el paquete de actualización que reciba de los servidores de Kaspersky.

      La dirección de la fuente de actualización debe coincidir con la dirección que especificó en el campo **Carpeta para almacenar actualizaciones** cuando configuró la descarga de actualizaciones en el almacenamiento del servidor (tarea *Descargar actualizaciones en el repositorio del Servidor de administración*).

   c. Haga clic en **Guardar**.

Puede excluir la fuente de actualización sin eliminarla de la lista de fuentes de actualización. Para hacerlo, coloque el interruptor junto a él en la posición de apagado.



Fuentes de actualización

6. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

7. En la ventana de propiedades de la tarea, seleccione la sección **Programación** y configure el modo de ejecución de la tarea.

8. De forma predeterminada, Kaspersky Endpoint Security ejecuta la tarea en modo manual.

9. Guarde los cambios.

Cómo configurar la actualización de Kaspersky Endpoint Security desde el almacenamiento del servidor especificado en la interfaz de la aplicación

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

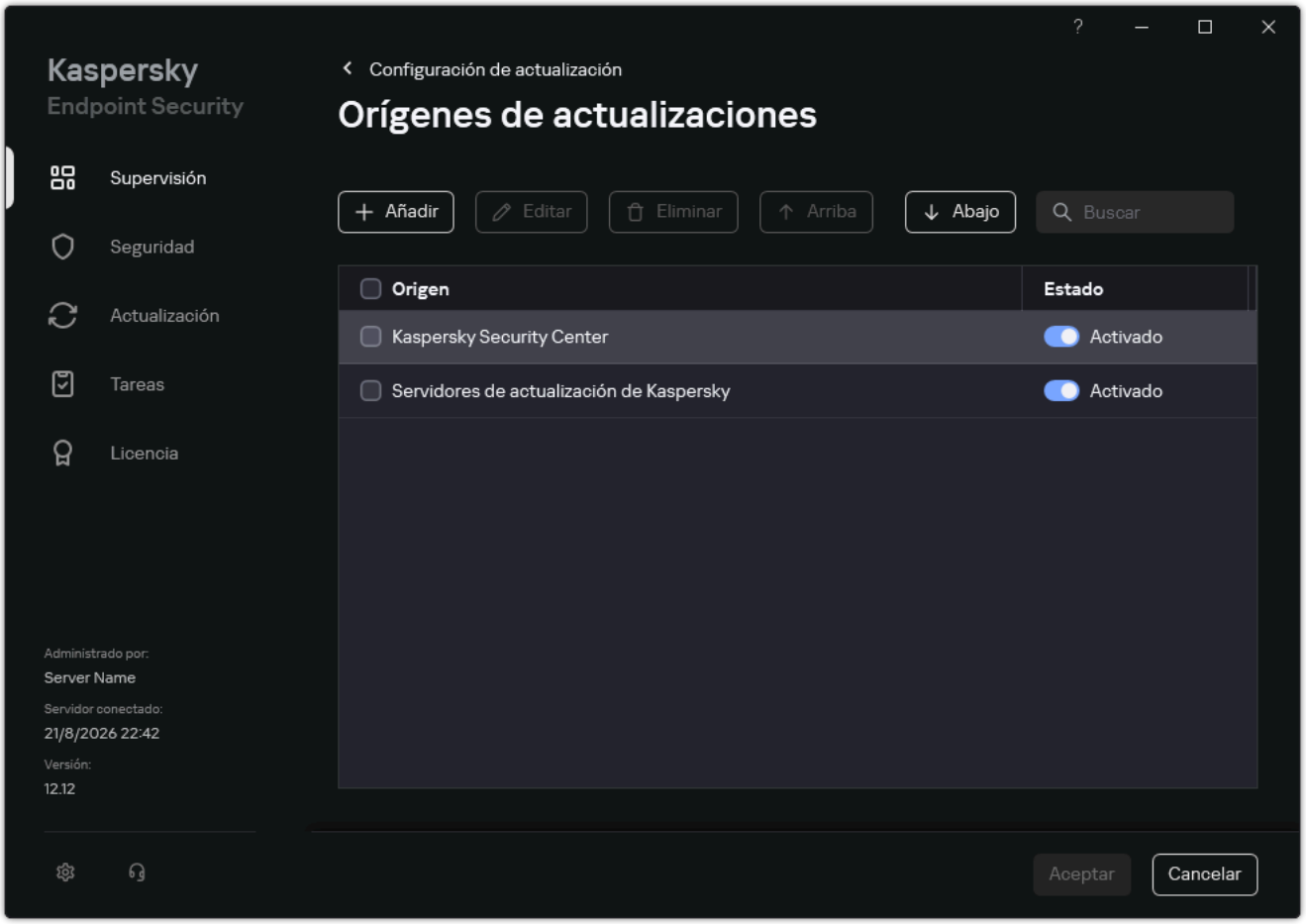
   Se abre la ventana propiedades de la tarea.

3. En la ventana de propiedades de la tarea, haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la lista de fuentes de actualización, asegúrese de que la actualización de la fuente de **Kaspersky Security Center** está activada. Además, la fuente de **Kaspersky Security Center** debe tener la prioridad más alta.

5. Si es necesario, añada las fuentes de actualización:

   a. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.



Fuentes de actualización

   a. Especifique la dirección del servidor FTP/HTTP, la carpeta de red o la carpeta local en donde Kaspersky Security Center copiará el paquete de actualización que reciba de los servidores de Kaspersky.

      La dirección de la fuente de actualización debe coincidir con la dirección que especificó en el campo **Carpeta para almacenar actualizaciones** cuando configuró la descarga de actualizaciones en el almacenamiento del servidor (tarea *Descargar actualizaciones en el repositorio del Servidor de administración*).

   b. Haga clic en **Seleccionar**.

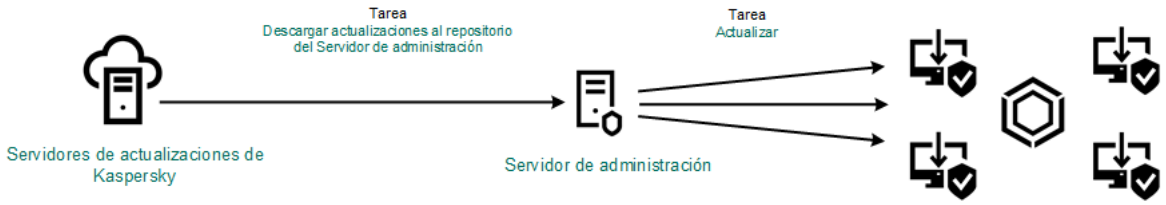
   Puede excluir la fuente de actualización sin eliminarla de la lista de fuentes de actualización. Para hacerlo, coloque el interruptor junto a él en la posición de apagado.

6. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

Si un equipo es administrado por Kaspersky Security Center, no es posible configurar el modo de ejecución para la tarea *Actualización de las bases de datos y módulos de la aplicación*. Solo puede ejecutar la tarea manualmente.

7. Guarde los cambios.



Actualización con un repositorio de servidor

Actualización con una carpeta compartida

Para reducir el tráfico de Internet, los equipos conectados a la LAN de la organización pueden obtener las actualizaciones de las bases de datos y de los módulos de la aplicación de una carpeta compartida. En esta modalidad, uno de los equipos de la LAN se encarga de recibir los paquetes de actualización del Servidor de administración de Kaspersky Security Center o de los servidores de actualizaciones de Kaspersky y los copia a una carpeta compartida. Los demás equipos conectados a la LAN obtienen el paquete de actualización de esa carpeta.

La versión y localización de la aplicación Kaspersky Endpoint Security que copia el paquete de actualización a una carpeta compartida debe coincidir con la versión y localización de la aplicación que actualiza las bases de datos desde la carpeta compartida. Si las versiones o localizaciones de las aplicaciones no coinciden, la actualización de la base de datos puede terminar con un error.

Si desea utilizar una carpeta compartida para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. Utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación.

2. Activar la copia de un paquete de actualización en una carpeta compartida en uno de los equipos de la red de área local.

   Cómo activar la copia del paquete de actualización en la carpeta compartida en la Consola de administración (MMC)

   1. Abra la Consola de administración de Kaspersky Security Center.

   2. En el árbol de la consola, seleccione **Tareas**.

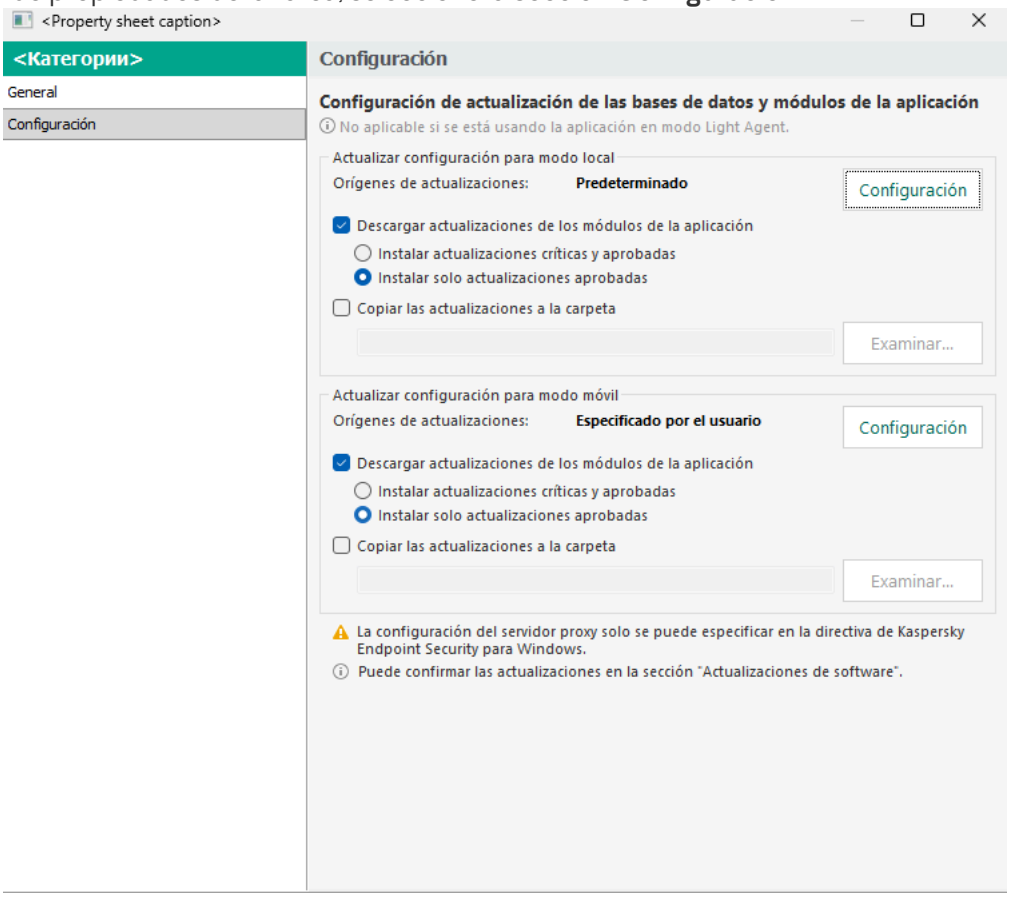
      La tarea *Actualización de las bases de datos y módulos de la aplicación* debe asignarse al equipo que actuará como origen de actualizaciones.

   3. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

      Se abre la ventana propiedades de la tarea.

La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de las bases de datos y módulos de la aplicación

5. En el bloque **Actualizar configuración para modo local**, haga clic en el botón **Configuración**.

6. Configure los orígenes de las actualizaciones.

   Las actualizaciones pueden obtenerse de los servidores de actualizaciones de Kaspersky, del Servidor de administración de Kaspersky Security Center, de otros servidores FTP o HTTP, o de carpetas locales o de red.

7. Seleccione la casilla **Copiar las actualizaciones a la carpeta**.

8. En el campo **Ruta de la carpeta**, introduzca la ruta UNC a la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

   Si el campo queda en blanco, Kaspersky Endpoint Security copiará el paquete de actualización a la carpeta `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Guarde los cambios.

Cómo activar la copia del paquete de actualización en la carpeta compartida en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

La tarea *Actualización* debe asignarse al equipo que actuará como origen de actualizaciones.

2. Seleccione la tarea **Actualización** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. Seleccione la pestaña **Configuración de la aplicación** → **Modo local**.

4. Configure los orígenes de las actualizaciones.

   Las actualizaciones pueden obtenerse de los servidores de actualizaciones de Kaspersky, del Servidor de administración de Kaspersky Security Center, de otros servidores FTP o HTTP, o de carpetas locales o de red.

5. Seleccione la casilla **Copiar las actualizaciones a la carpeta**.

6. En el campo **Ruta**, introduzca la ruta UNC a la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

   Si el campo queda en blanco, Kaspersky Endpoint Security copiará el paquete de actualización a la carpeta `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Guarde los cambios.

Cómo activar la copia del paquete de actualización en la carpeta compartida en la interfaz de la aplicación

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. En el bloque **Distribución de actualizaciones**, seleccione la casilla de verificación **Copiar las actualizaciones a la carpeta**.

4. Introduzca la ruta UNC a la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

5. Guarde los cambios.

3. Configuración del proceso de actualización para que los demás equipos de la LAN de la organización obtengan las bases de datos y los módulos de la aplicación más recientes de la carpeta compartida.

Cómo configurar actualizaciones desde la carpeta compartida en la Consola de administración (MMC)

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Actualización de las bases de datos y módulos de la aplicación**.

4. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

5. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Actualización de las bases de datos y módulos de la aplicación**.

Paso 2. Selección de orígenes de actualizaciones

Agregue un nuevo origen de actualizaciones: una carpeta compartida. La dirección del origen debe ser la misma que haya especificado en el campo **Ruta de la carpeta** al configurar la copia del paquete de actualización a la carpeta compartida. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

La tarea *Actualización de las bases de datos y módulos de la aplicación* debe asignarse a los equipos conectados a la LAN de la organización, salvo al que actúa como origen de actualizaciones.

Paso 4. Selección de la cuenta para ejecutar la tarea

Seleccione una cuenta para ejecutar la tarea *Actualización de las bases de datos y módulos de la aplicación*. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

Paso 5. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o después de descargar bases de datos antivirus al repositorio.

Paso 6. Definir el nombre de la tarea

Introduzca el nombre de la tarea; por ejemplo, *Actualización desde una carpeta compartida*.

Paso 7. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, la tarea de actualización se ejecutará en los equipos de usuario según la planificación especificada.

Cómo configurar actualizaciones desde la carpeta compartida en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Actualización**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Actualización desde una carpeta compartida*).

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

   > La tarea *Actualización* debe asignarse a los equipos conectados a la LAN de la organización, salvo al que actúa como origen de actualizaciones.

4. Seleccione dispositivos de acuerdo con la opción de cobertura de la tarea que haya elegido y vaya al paso siguiente.

5. Finalice el asistente.

   La nueva tarea aparecerá en la tabla de tareas.

6. Haga clic en la tarea *Actualización* recién creada.

   Se abre la ventana propiedades de la tarea.

7. Seleccione la pestaña **Configuración de la aplicación** → **Modo local**.

8. En el bloque **Orígenes de actualizaciones**, haga clic en el botón **Añadir**.

9. En la ventana que se abre, introduzca la ruta de la carpeta compartida.

   > La dirección del origen debe ser la misma que haya especificado en el campo **Ruta** al configurar la copia del paquete de actualización a la carpeta compartida (consulte las instrucciones de más arriba).

10. Haga clic en **Aceptar**.

11. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

12. Guarde los cambios.

Cómo configurar actualizaciones desde la carpeta compartida en la interfaz de la aplicación

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. Haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la ventana que se abre, haga clic en el botón **Añadir**.

5. En la ventana que se abre, introduzca la ruta de la carpeta compartida.

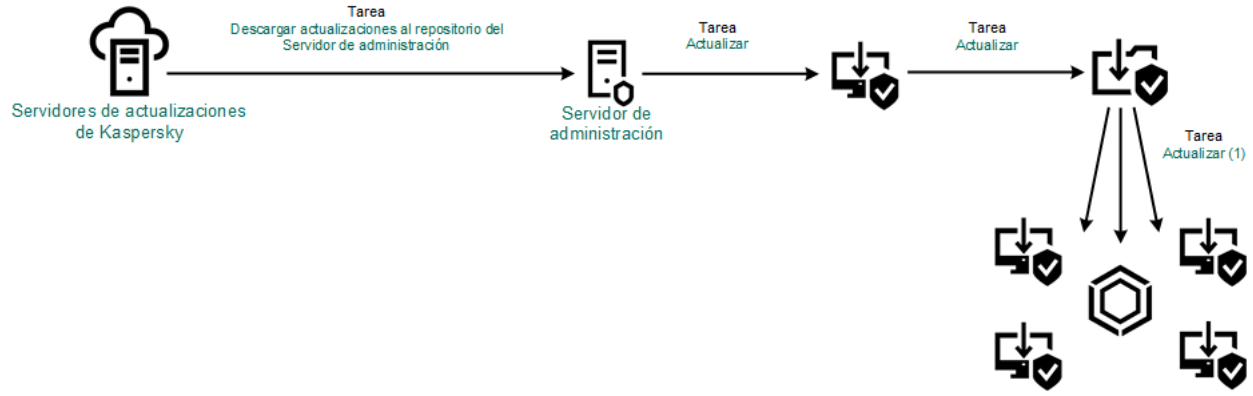
   La dirección del origen debe ser la misma que haya especificado al configurar la copia del paquete de actualización a la carpeta compartida (consulte las instrucciones de más arriba).

6. Haga clic en **Seleccionar**.

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

8. Guarde los cambios.



Actualización con una carpeta compartida

Actualización con Kaspersky Update Utility

Puede utilizar Kaspersky Update Utility para que, en la LAN de su organización, los equipos obtengan de una carpeta compartida las actualizaciones de las bases de datos y de los módulos de la aplicación. Esto ayuda a reducir el tráfico de Internet. En esta modalidad, uno de los equipos de la LAN se encarga de recibir los paquetes de actualización del Servidor de administración de Kaspersky Security Center o de los servidores de actualizaciones de Kaspersky. El equipo luego copia estos paquetes a la carpeta compartida usando la utilidad. Los demás equipos conectados a la LAN obtienen el paquete de actualización de esa carpeta.

La versión y localización de la aplicación Kaspersky Endpoint Security que copia el paquete de actualización a una carpeta compartida debe coincidir con la versión y localización de la aplicación que actualiza las bases de datos desde la carpeta compartida. Si las versiones o localizaciones de las aplicaciones no coinciden, la actualización de la base de datos puede terminar con un error.

Si desea utilizar una carpeta compartida para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. Utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación.

2. Instale Kaspersky Update Utility en uno de los equipos conectados a la LAN de su organización.

3. Configure Kaspersky Update Utility para que el paquete de actualización se copie a la carpeta compartida.

   Para descargar el paquete de distribución de Kaspersky Update Utility, visite el sitio web de soporte técnico de Kaspersky. Después de instalar la utilidad, seleccione el origen de las actualizaciones (por ejemplo, el repositorio del Servidor de administración) y la carpeta compartida a la que Kaspersky Update Utility copiará los paquetes de actualización. Para obtener información detallada sobre el uso de Kaspersky Update Utility, consulte la Base de conocimientos de Kaspersky.

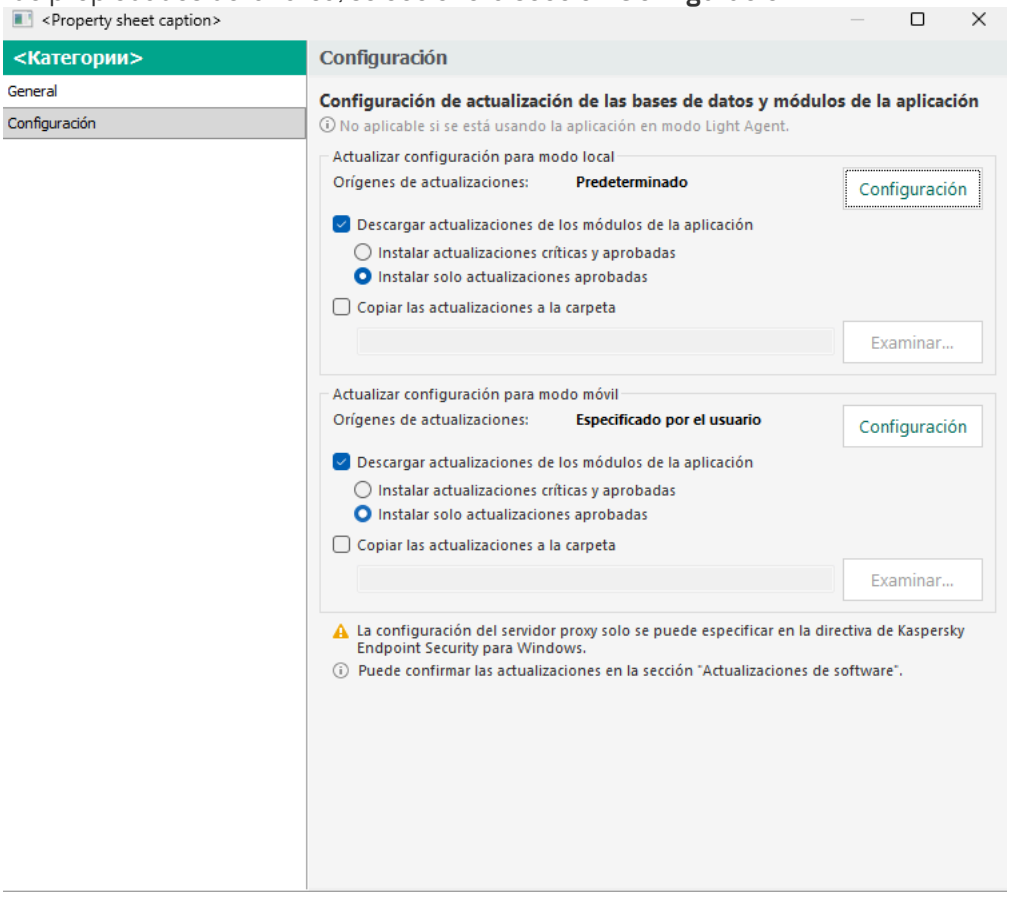
4. Configuración del proceso de actualización para que los demás equipos de la LAN de la organización obtengan las bases de datos y los módulos de la aplicación más recientes de la carpeta compartida.

Cómo configurar actualizaciones desde la carpeta compartida en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.
4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de las bases de datos y módulos de la aplicación

5. En el bloque **Actualizar configuración para modo local**, haga clic en el botón **Configuración**.
6. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.
7. En la ventana que se abre, introduzca la ruta UNC a la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

   La dirección del origen debe coincidir con la indicada en la configuración de Kaspersky Update Utility.
8. Haga clic en **Aceptar**.

9. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

10. Guarde los cambios.

Cómo configurar actualizaciones desde la carpeta compartida en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. Seleccione la pestaña **Configuración de la aplicación** → **Modo local**.

4. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.

5. En la ventana que se abre, introduzca la ruta UNC a la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

   La dirección del origen debe coincidir con la indicada en la configuración de Kaspersky Update Utility.

6. Haga clic en **Aceptar**.

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

8. Guarde los cambios.

Cómo configurar actualizaciones desde la carpeta compartida en la interfaz de la aplicación

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



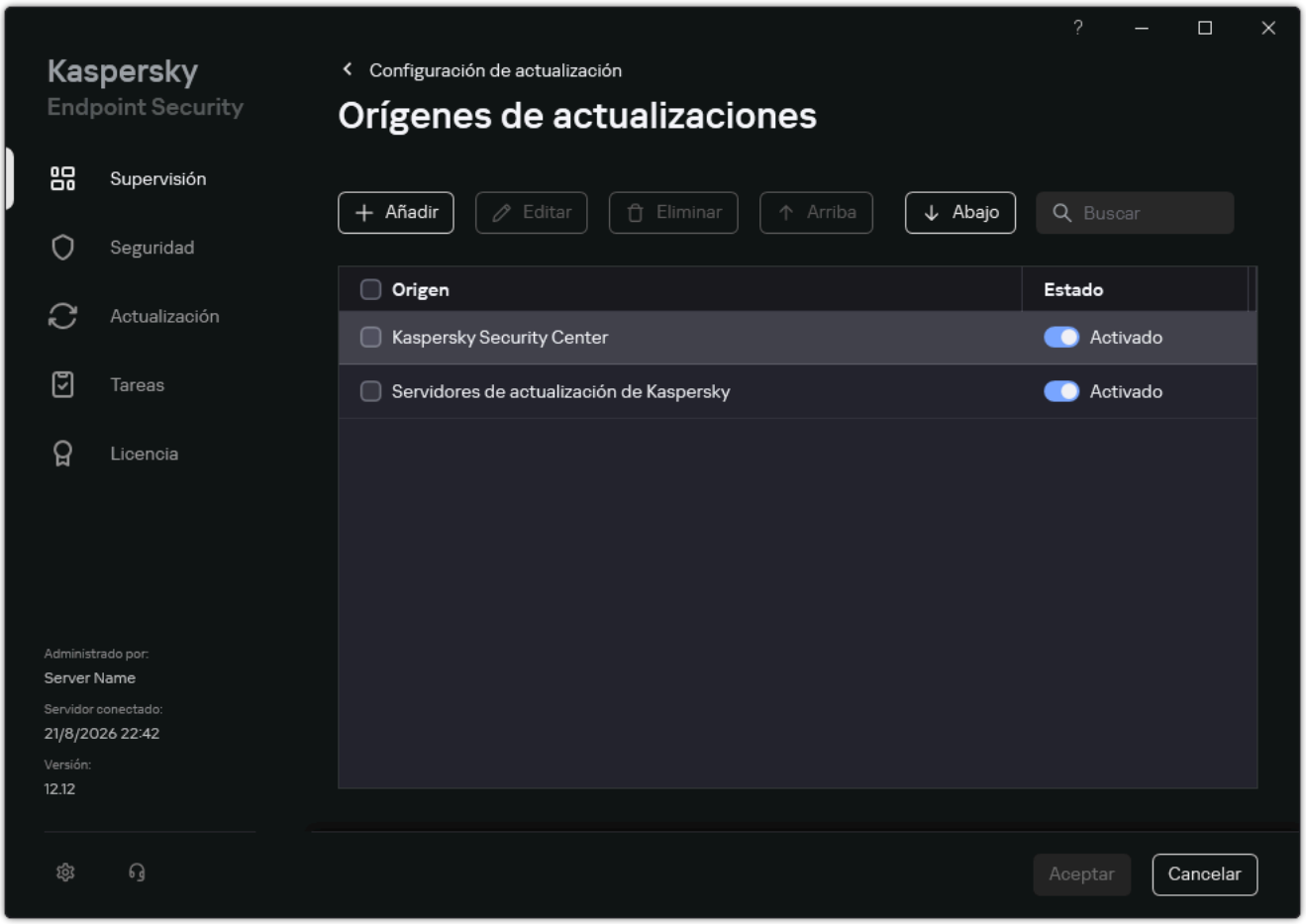
Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. En la ventana de propiedades de la tarea, haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.



Fuentes de actualización

5. Introduzca la ruta UNC a la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

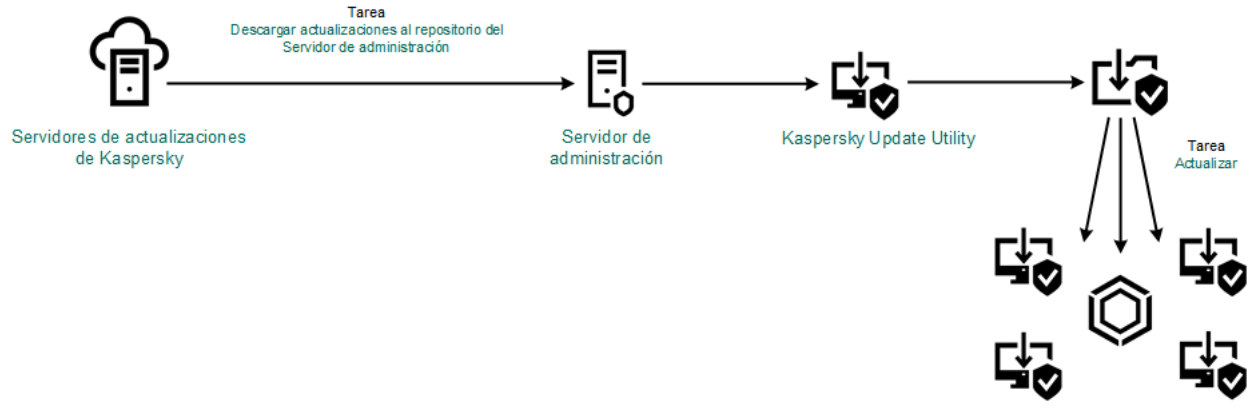
> La dirección del origen debe coincidir con la indicada en la configuración de Kaspersky Update Utility.

6. Haga clic en **Seleccionar**.

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

8. Guarde los cambios.



Actualización con Kaspersky Update Utility

Actualización en modo móvil

Se denomina *modo móvil* al modo en que Kaspersky Endpoint Security funciona cuando un equipo sale de la red de la organización (*equipo sin conexión*). Para más información sobre cómo trabajar con los equipos sin conexión y los usuarios que están fuera de la oficina, consulte la Ayuda de Kaspersky Security Center.

Los equipos sin conexión a la red de la organización no pueden acceder al Servidor de administración para actualizar las bases de datos y los módulos de la aplicación. De forma predeterminada en el modo móvil, solo los servidores de actualización de Kaspersky se utilizan como fuente de actualización para actualizar bases de datos y módulos de aplicaciones. El uso de un servidor proxy para acceder a Internet se rige por una directiva especial, llamada directiva fuera de la oficina. Esta directiva debe crearse por separado. Cuando Kaspersky Endpoint Security cambia al modo móvil, la tarea de actualización se ejecuta cada dos horas.

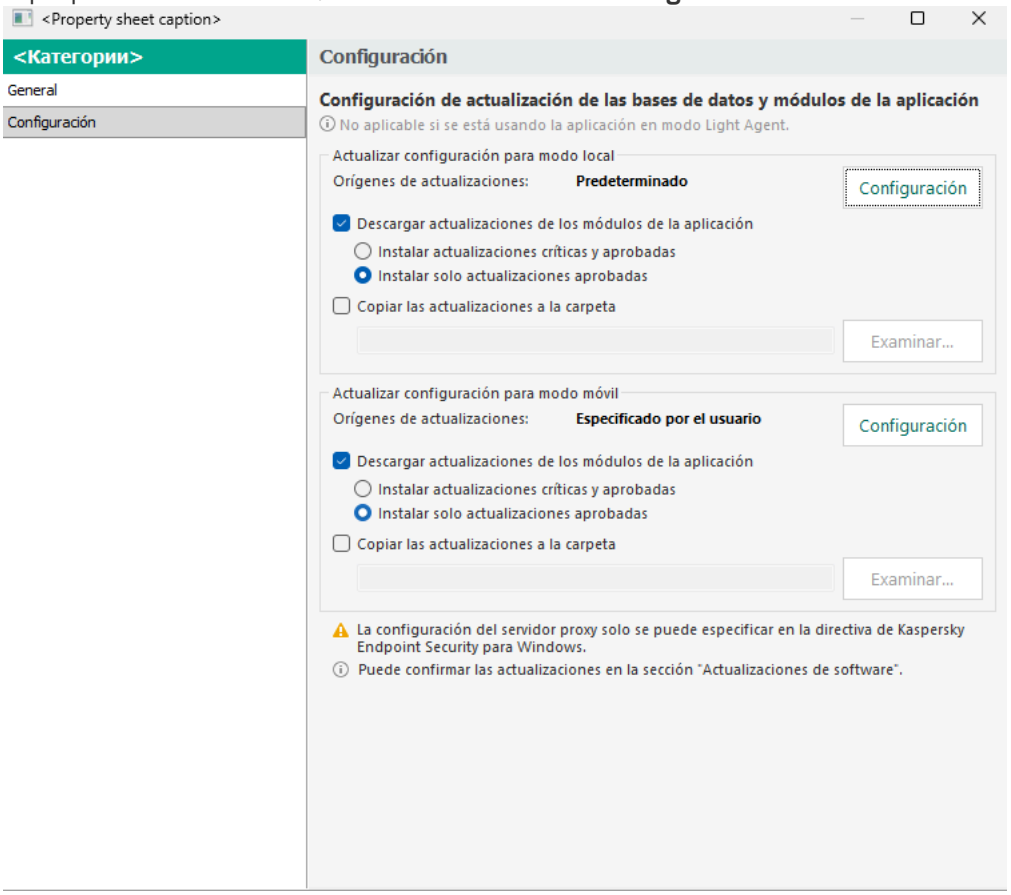
Cómo configurar los ajustes de actualización en modo móvil en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de las bases de datos y módulos de la aplicación

5. En el bloque **Actualizar configuración para modo móvil**, haga clic en el botón **Configuración**.

6. Configure los orígenes de las actualizaciones. Las actualizaciones pueden obtenerse de los servidores de actualizaciones de Kaspersky, de otros servidores FTP o HTTP, o de carpetas locales o de red.

7. Guarde los cambios.

Cómo configurar los ajustes de actualización en modo móvil en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. Seleccione la pestaña **Configuración de la aplicación → Modo móvil**.

4. Configure los orígenes de las actualizaciones. Las actualizaciones pueden obtenerse de los servidores de actualizaciones de Kaspersky, de otros servidores FTP o HTTP, o de carpetas locales o de red.

5. Guarde los cambios.

Como resultado, las bases de datos y los módulos de aplicación se actualizarán en los equipos de los usuarios cuando cambien al modo móvil.

Inicio y parada de una tarea de actualización

Independientemente del modo de ejecución de la tarea de actualización seleccionado, puede iniciar o parar una tarea de actualización de Kaspersky Endpoint Security en cualquier momento.

Para iniciar o parar una tarea de actualización:

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.
2. En el mosaico **Actualización de las bases de datos y módulos de la aplicación**, haga clic en el botón **Actualizar** si desea iniciar la tarea de actualización.

   Kaspersky Endpoint Security comenzará a actualizar los módulos y las bases de datos de la aplicación. La aplicación mostrará el progreso de la tarea, el tamaño de los archivos descargados y el origen de actualizaciones. Puede detener la tarea en cualquier momento haciendo clic en el botón **Detener actualización**.

Para iniciar o detener la tarea de actualización cuando se muestra la interfaz simplificada de la aplicación:

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En la lista desplegable **Tareas** del menú contextual, lleve a cabo una de las siguientes acciones:
   - seleccione una tarea de actualización que no esté en ejecución para iniciarla
   - seleccione una tarea de actualización en ejecución para detenerla
   - seleccione una tarea de actualización suspendida para reanudarla o reiniciarla

Inicio de una tarea de actualización con los permisos de una cuenta de usuario distinta

De forma predeterminada, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta se ha utilizado para iniciar la sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security se podría actualizar desde un origen de actualizaciones al que el usuario no pueda acceder debido a la falta de los permisos necesarios (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o un origen de actualizaciones para el que no se haya configurado la autenticación del servidor proxy. En la configuración de la aplicación, puede especificar un usuario que tenga esos permisos e iniciar la tarea de actualización de Kaspersky Endpoint Security con la cuenta de ese usuario.

Para iniciar una tarea de actualización con una cuenta de usuario distinta:

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. Haga clic en **Ejecutar actualizaciones de bases de datos con derechos de usuario**.

4. En la ventana que se abre, elija **Otro usuario**.

5. Introduzca las credenciales de la cuenta de un usuario con los permisos necesarios para acceder al origen de actualizaciones.

6. Guarde los cambios.

Selección del modo de ejecución de la tarea de actualización

Si no es posible iniciar la tarea de actualización por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se inicie automáticamente lo antes posible.

Puede retrasar la ejecución de la tarea de actualización después de que se inicie la aplicación si selecciona el modo de ejecución de la tarea de ejecución **Según programación** y si el momento del inicio de Kaspersky Endpoint Security coincide con la planificación del inicio de la tarea de actualización. La tarea de actualización solamente puede ejecutarse después de que transcurra la cantidad de tiempo especificada una vez que se inicia Kaspersky Endpoint Security.

Para seleccionar el modo de ejecución de la tarea de actualización:

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. Haga clic en **Modo de ejecución**.

4. En la ventana que se abre, seleccione el modo de ejecución de la tarea de actualización:

   - Si quiere que Kaspersky Endpoint Security ejecute la tarea de actualización en función de si hay o no disponible un paquete de actualización en el origen de actualizaciones, seleccione **Automáticamente**. La frecuencia de las comprobaciones que realiza Kaspersky Endpoint Security para ver si hay paquetes de actualización aumenta durante los brotes de virus y disminuye en otros momentos.

   - Si quiere iniciar una tarea de actualización manualmente, seleccione **Manualmente**.

   - Si quiere configurar una planificación para ejecutar la tarea de actualización, seleccione otras opciones. Establezca la configuración avanzada para iniciar la tarea de actualización:

     - En el campo **Posponer ejecución después del inicio de la aplicación durante N minutos**, introduzca el intervalo de tiempo durante el que desea posponer el inicio de la tarea de actualización después del inicio de Kaspersky Endpoint Security.

     - Seleccione la opción **Ejecutar análisis programado al día siguiente si el equipo está apagado** si desea que Kaspersky Endpoint Security ejecute las tareas de actualización no realizadas en la primera oportunidad. Cuando la aplicación tiene la oportunidad de ejecutar tareas omitidas, las ejecuta de manera aleatoria dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo.

5. Guarde los cambios.

Adición de un origen de actualizaciones

Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security.

Las fuentes de las actualizaciones incluyen el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky y carpetas locales y en red.

Si no hay servidores de actualización de Kaspersky disponibles, Kaspersky Endpoint Security puede usar dominios alternativos para actualizar sus bases de datos y módulos de software de la aplicación. Para obtener información detallada, consulte la Base de conocimientos de soporte técnico.

La lista predeterminada de orígenes de actualizaciones incluye los servidores de actualizaciones de Kaspersky Security Center y Kaspersky. Puede agregar a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones.

Kaspersky Endpoint Security no es compatible con las actualizaciones de los servidores HTTPS a menos que sean servidores de actualizaciones de Kaspersky.

Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno después de otro, empieza desde el inicio de la lista y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible.

De forma predeterminada, Kaspersky Endpoint Security utiliza el servidor de Kaspersky Security Center como la primera fuente de actualización. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una política al equipo, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de la tarea local *Actualización de las bases de datos y módulos de la aplicación*, porque es posible que la aplicación no tenga acceso al servidor de Kaspersky Security Center.

Si la aplicación se está ejecutando en modo Light Agent, se selecciona una carpeta en la SVM como origen de actualizaciones.

Cómo añadir un origen de actualizaciones en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

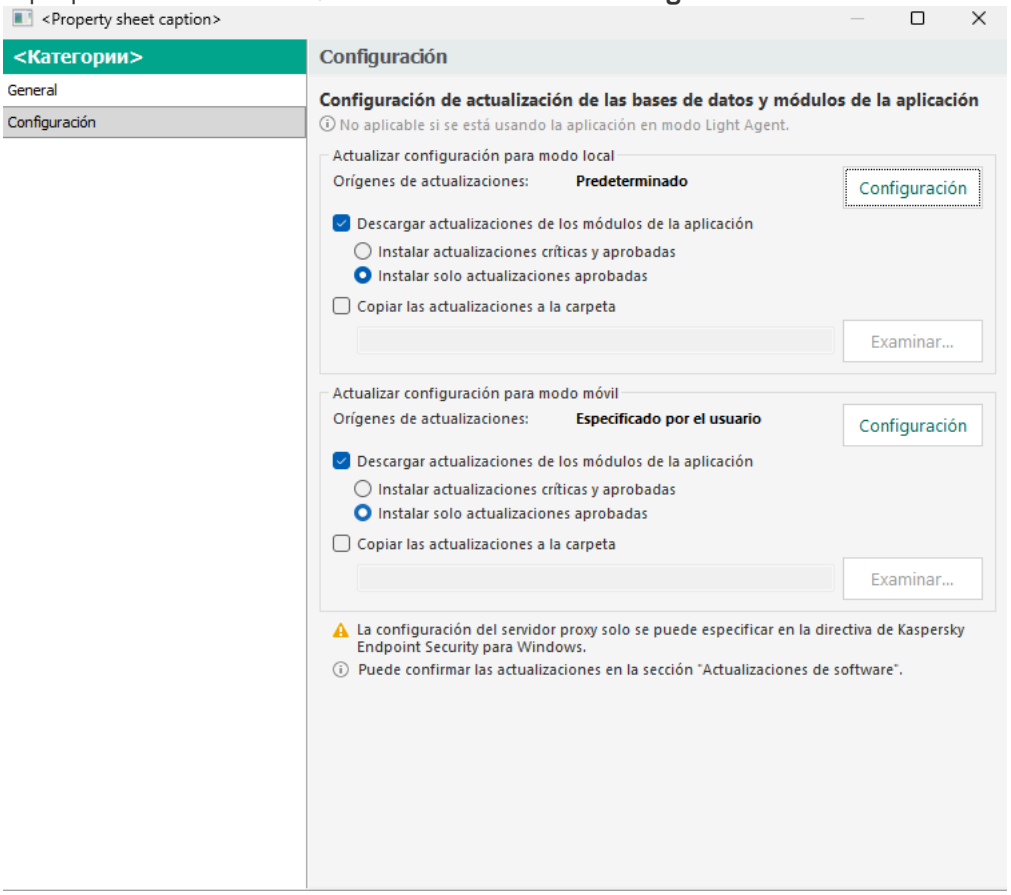
   En el árbol de la consola, seleccione **Tareas**.

2. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

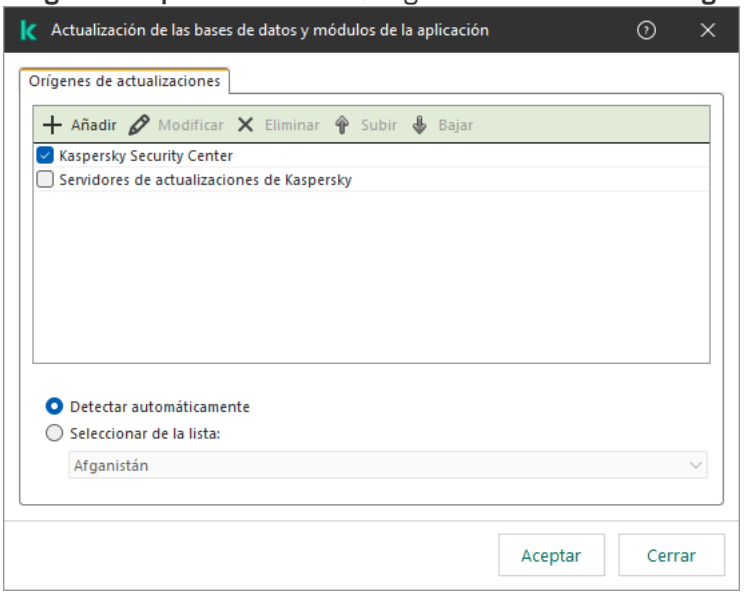
   La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de las bases de datos y módulos de la aplicación

4. En el bloque **Actualizar configuración para modo local**, haga clic en el botón **Configuración**.



Fuentes de actualización

5. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.

6. En el campo **Orígenes de actualizaciones**, especifique la dirección del servidor FTP o HTTP, la carpeta de red o la carpeta local que contiene el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Para un servidor FTP o HTTP, introduzca su dirección web o su dirección IP.

     Por ejemplo, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

     Si es necesario autenticarse para acceder al servidor FTP, especifique los datos en la dirección siguiendo este formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Para una carpeta de red, introduzca la ruta UNC.

     Por ejemplo, `\\Server\Share\Update distribution`.

   - En el caso de una carpeta local, introduzca la ruta completa de esa carpeta.

     Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Puede excluir la fuente de actualización sin eliminarla de la lista de fuentes de actualización. Para hacerlo, desactive la casilla de verificación junto al objeto.

7. Haga clic en **Aceptar**.

8. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

9. Si necesario, agregue un origen de actualizaciones para el modo móvil. Se denomina *modo móvil* al modo en que Kaspersky Endpoint Security funciona cuando un equipo sale de la red de la organización (*equipo sin conexión*).

10. Guarde los cambios.

Cómo añadir un origen de actualizaciones en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

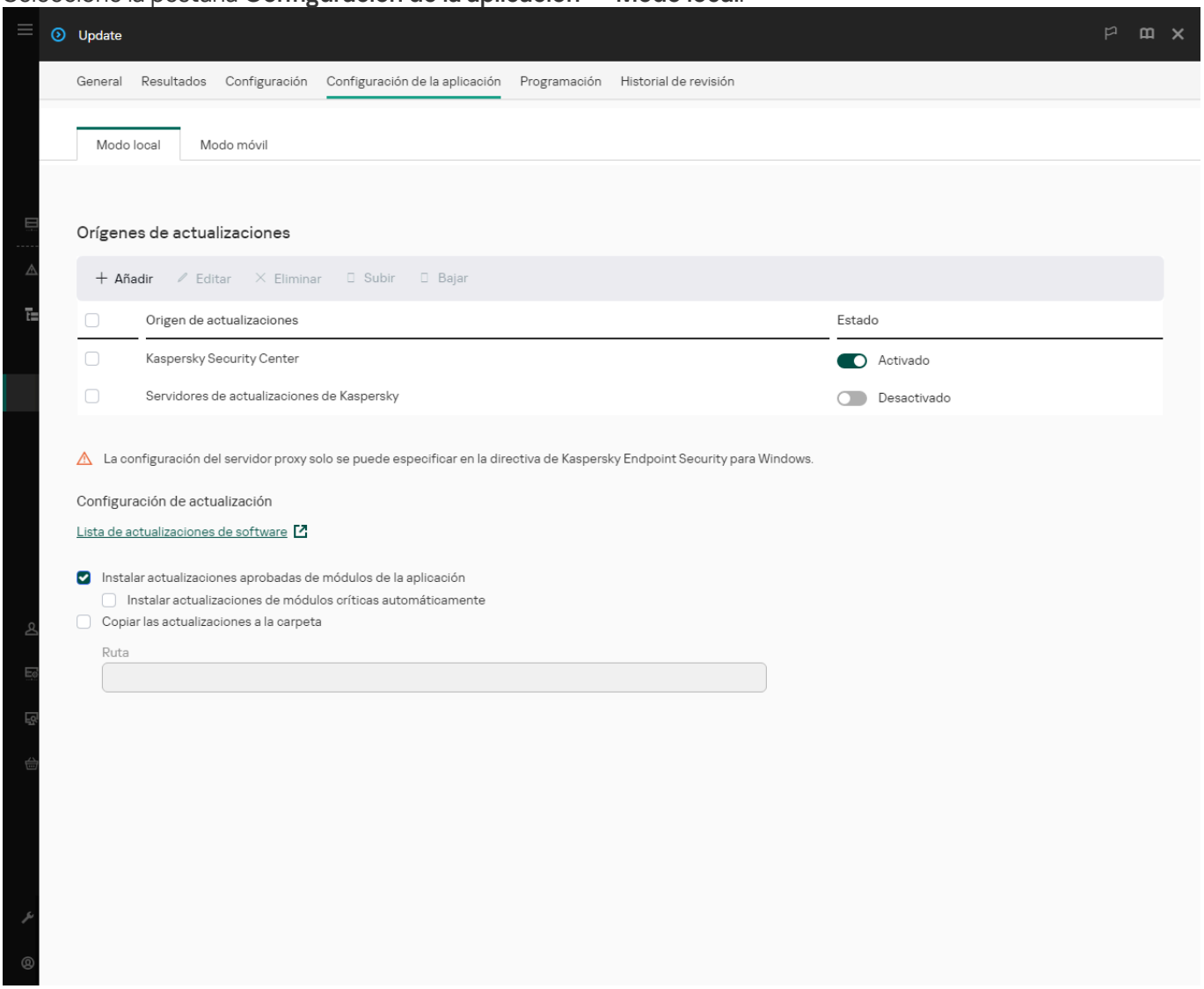
   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. Seleccione la pestaña **Configuración de la aplicación → Modo local**.



Fuentes de actualización

4. En la lista de orígenes de actualizaciones, haga clic en el botón **Añadir**.

5. En la ventana que se abre, especifique la dirección del servidor FTP o HTTP, la carpeta de red o la carpeta local que contiene el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Para un servidor FTP o HTTP, introduzca su dirección web o su dirección IP.

     Por ejemplo, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

Si es necesario autenticarse para acceder al servidor FTP, especifique los datos en la dirección siguiendo este formato: `ftp://<user name>:<password>@<node>:<port>`.

- Para una carpeta de red, introduzca la ruta UNC.

  Por ejemplo, `\\Server\Share\Update distribution`.

- En el caso de una carpeta local, introduzca la ruta completa de esa carpeta.

  Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Puede excluir la fuente de actualización sin eliminarla de la lista de fuentes de actualización. Para hacerlo, coloque el interruptor junto a él en la posición de apagado.

6. Haga clic en **Aceptar**.
7. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

   Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

8. Si necesario, agregue un origen de actualizaciones para el modo móvil. Se denomina *modo móvil* al modo en que Kaspersky Endpoint Security funciona cuando un equipo sale de la red de la organización (*equipo sin conexión*).
9. Guarde los cambios.

Cómo añadir un origen de actualizaciones en la interfaz de la aplicación

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



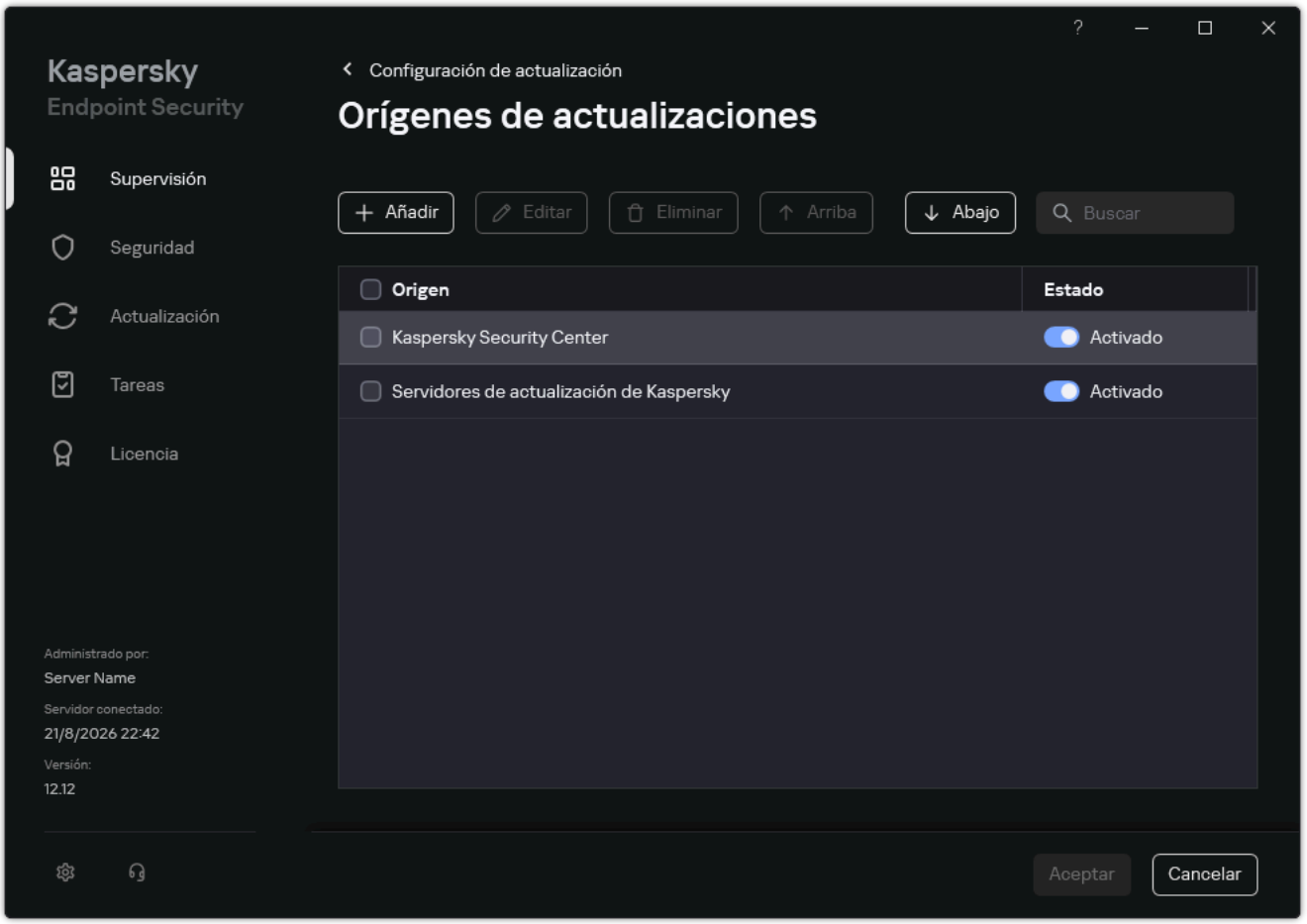
Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. Haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la ventana que se abre, haga clic en el botón **Añadir**.



Fuentes de actualización

5. En la ventana que se abre, especifique la dirección del servidor FTP o HTTP, la carpeta de red o la carpeta local que contiene el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Para un servidor FTP o HTTP, introduzca su dirección web o su dirección IP.

     Por ejemplo, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

     Si es necesario autenticarse para acceder al servidor FTP, especifique los datos en la dirección siguiendo este formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Para una carpeta de red, introduzca la ruta UNC.

     Por ejemplo, `\\Server\Share\Update distribution`.

   - En el caso de una carpeta local, introduzca la ruta completa de esa carpeta.

     Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Haga clic en **Seleccionar**.

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.

8. Guarde los cambios.

Actualización de los módulos de la aplicación

Las actualizaciones del módulo de la aplicación corrigen errores, mejoran el rendimiento y añaden nuevas funciones. Cuando esté disponible una nueva actualización del módulo de la aplicación, debe confirmar la instalación de la actualización. Puede confirmar la instalación de una actualización del módulo de la aplicación en la interfaz de la aplicación o en Kaspersky Security Center. Cuando hay una actualización disponible, la aplicación muestra una notificación en la ventana principal de Kaspersky Endpoint Security: . Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia de usuario final, la aplicación instala las actualizaciones después de que se hayan aceptado dichos términos.

Después de instalar una actualización de la aplicación, es posible que deba reiniciar su equipo.

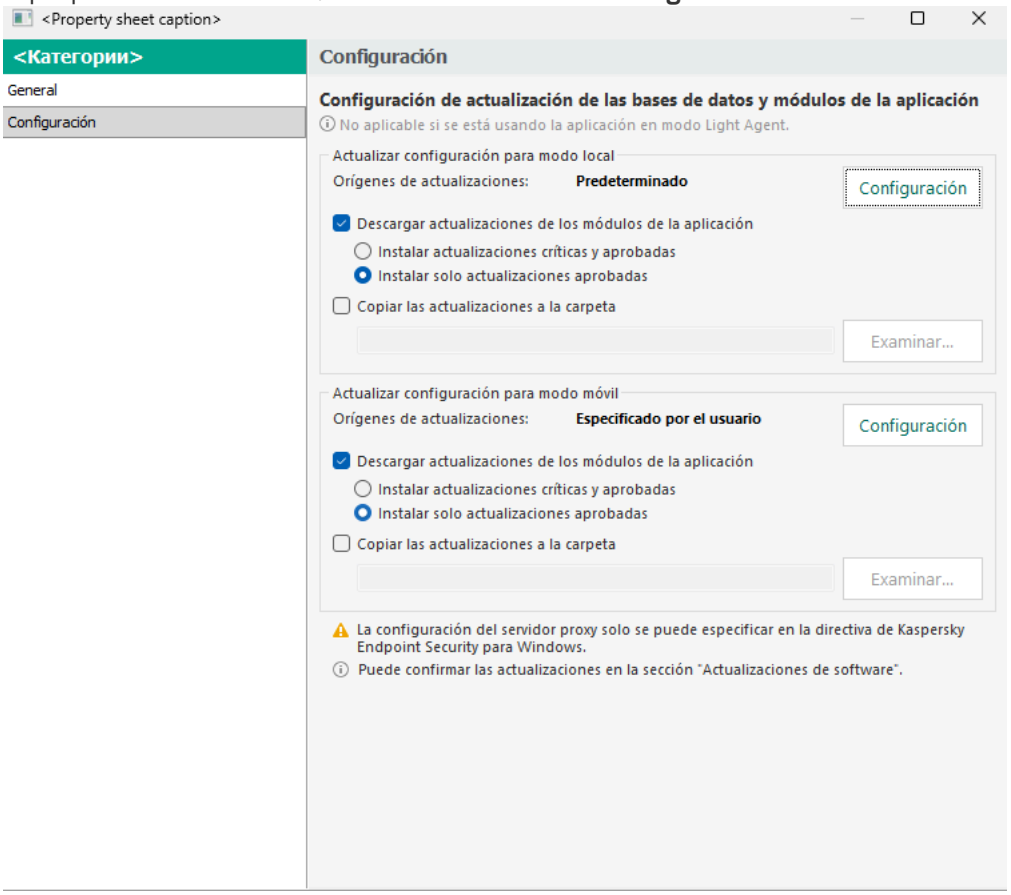
Cómo configurar las actualizaciones de módulos de la aplicación en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de las bases de datos y módulos de la aplicación

5. En el bloque **Actualizar configuración para modo local**, seleccione la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación**.

   Si desea evitar que se descarguen las actualizaciones de los módulos de la aplicación, desactive la casilla **Descargar actualizaciones de los módulos de la aplicación** y prohíba el uso de tareas locales por parte del usuario.

6. Seleccione las actualizaciones del módulo de la aplicación que desea instalar.

   - **Instalar actualizaciones críticas y aprobadas**. Si se selecciona esta opción, cuando las actualizaciones de los módulos de la aplicación están disponibles, Kaspersky Endpoint Security instala automáticamente las actualizaciones críticas y todas las demás únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center.

   - **Instalar solo actualizaciones aprobadas**. Si se selecciona esta opción, cuando están disponibles las actualizaciones de los módulos de la aplicación, Kaspersky Endpoint Security las instala únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.

7. Si es necesario, configure actualizaciones de los módulos de la aplicación para el modo móvil. Se denomina *modo móvil* al modo en que Kaspersky Endpoint Security funciona cuando un equipo sale de la red de la organización (*equipo sin conexión*).

8. Guarde los cambios.

Cómo configurar las actualizaciones de los módulos de la aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

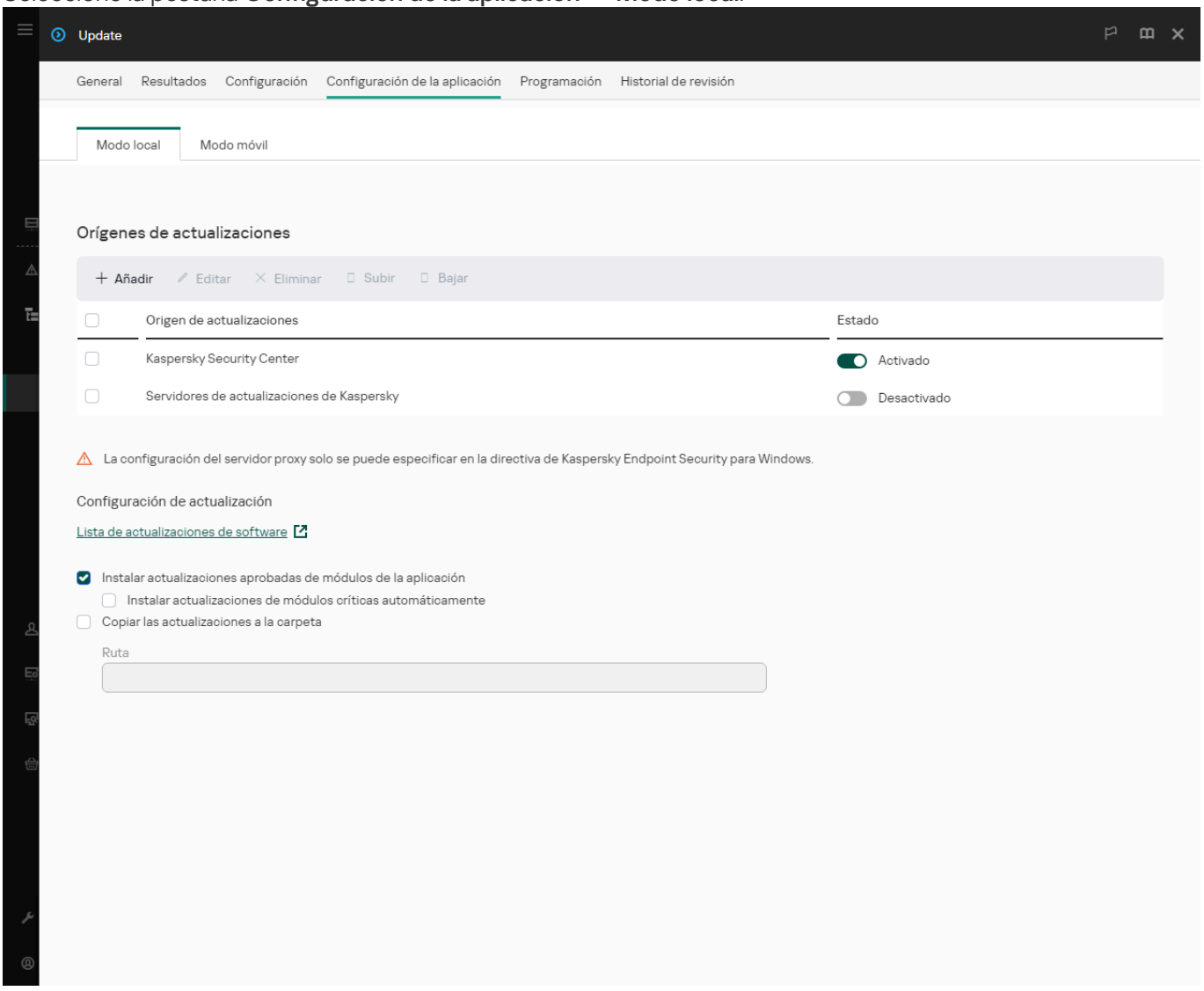
   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización de las bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   La tarea *Actualización de las bases de datos y módulos de la aplicación* se crea automáticamente mediante el asistente de inicio rápido del Servidor de administración. Para crear la tarea *Actualización de las bases de datos y módulos de la aplicación*, instale el Complemento de administración de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.

3. Seleccione la pestaña **Configuración de la aplicación → Modo local**.



Configuración de la tarea Actualización

4. En **Configuración de actualización**, seleccione las actualizaciones de los módulos de la aplicación que desea instalar.

   - **Instalar actualizaciones aprobadas de módulos de la aplicación**. Si se selecciona esta opción, cuando están disponibles las actualizaciones de los módulos de la aplicación, Kaspersky Endpoint Security las instala únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.

   - **Instalar actualizaciones de módulos críticas automáticamente**. Si se selecciona esta opción, cuando las actualizaciones de los módulos de la aplicación están disponibles, Kaspersky Endpoint Security instala automáticamente las actualizaciones críticas y todas las demás únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center.

Si desea evitar que se descarguen las actualizaciones de los módulos de la aplicación, desactive las casillas de verificación **Instalar actualizaciones aprobadas de módulos de la aplicación** y **Instalar actualizaciones de módulos críticas automáticamente** y prohíba el uso de tareas locales por parte del usuario.

5. Si es necesario, configure actualizaciones de los módulos de la aplicación para el modo móvil. Se denomina *modo móvil* al modo en que Kaspersky Endpoint Security funciona cuando un equipo sale de la red de la organización (*equipo sin conexión*).

6. Guarde los cambios.

Cómo configurar las actualizaciones de los módulos de la aplicación en la interfaz de la aplicación

No puede configurar la tarea del grupo *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de las bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de las bases de datos y módulos de la aplicación*, significa que el administrador ha prohibido el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de las bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana propiedades de la tarea.

3. En el bloque **Descargando e instalando las actualizaciones de los módulos de la aplicación**, seleccione la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación**.

4. Seleccione las actualizaciones del módulo de la aplicación que desea instalar.

   - **Instalar actualizaciones críticas y aprobadas**. Si se selecciona esta opción, cuando las actualizaciones de los módulos de la aplicación están disponibles, Kaspersky Endpoint Security instala automáticamente las actualizaciones críticas y todas las demás únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center.

   - **Instalar solo actualizaciones aprobadas**. Si se selecciona esta opción, cuando están disponibles las actualizaciones de los módulos de la aplicación, Kaspersky Endpoint Security las instala únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.

5. Guarde los cambios.

Actualización mediante un servidor proxy

Para que las bases de datos y los módulos de la aplicación más recientes puedan descargarse de un origen de actualizaciones, puede ser necesario especificar los parámetros de conexión de un servidor proxy. Estos parámetros se utilizan para todos los orígenes de actualizaciones. Si el servidor proxy no se necesita para un origen en particular, su uso puede deshabilitarse en las propiedades de la directiva. Kaspersky Endpoint Security también usará un servidor proxy para acceder a Kaspersky Security Network y a los servidores de activación.

Para conectarse a los orígenes de actualizaciones a través de un servidor proxy:

1. En la ventana principal de Web Console, haga clic en ⚙.

   Se abre la ventana de propiedades del Servidor de administración.

2. Vaya a la sección **Configuración del acceso a Internet**.

3. Seleccione la casilla **Usar servidor proxy**.

4. Defina los parámetros para conectarse con el servidor proxy: la dirección del servidor proxy, el número de puerto y los valores de autenticación (nombre de usuario y contraseña).

5. Guarde los cambios.

Para desactivar el uso de un servidor proxy para un grupo de administración específico:

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general → Configuración de red**.

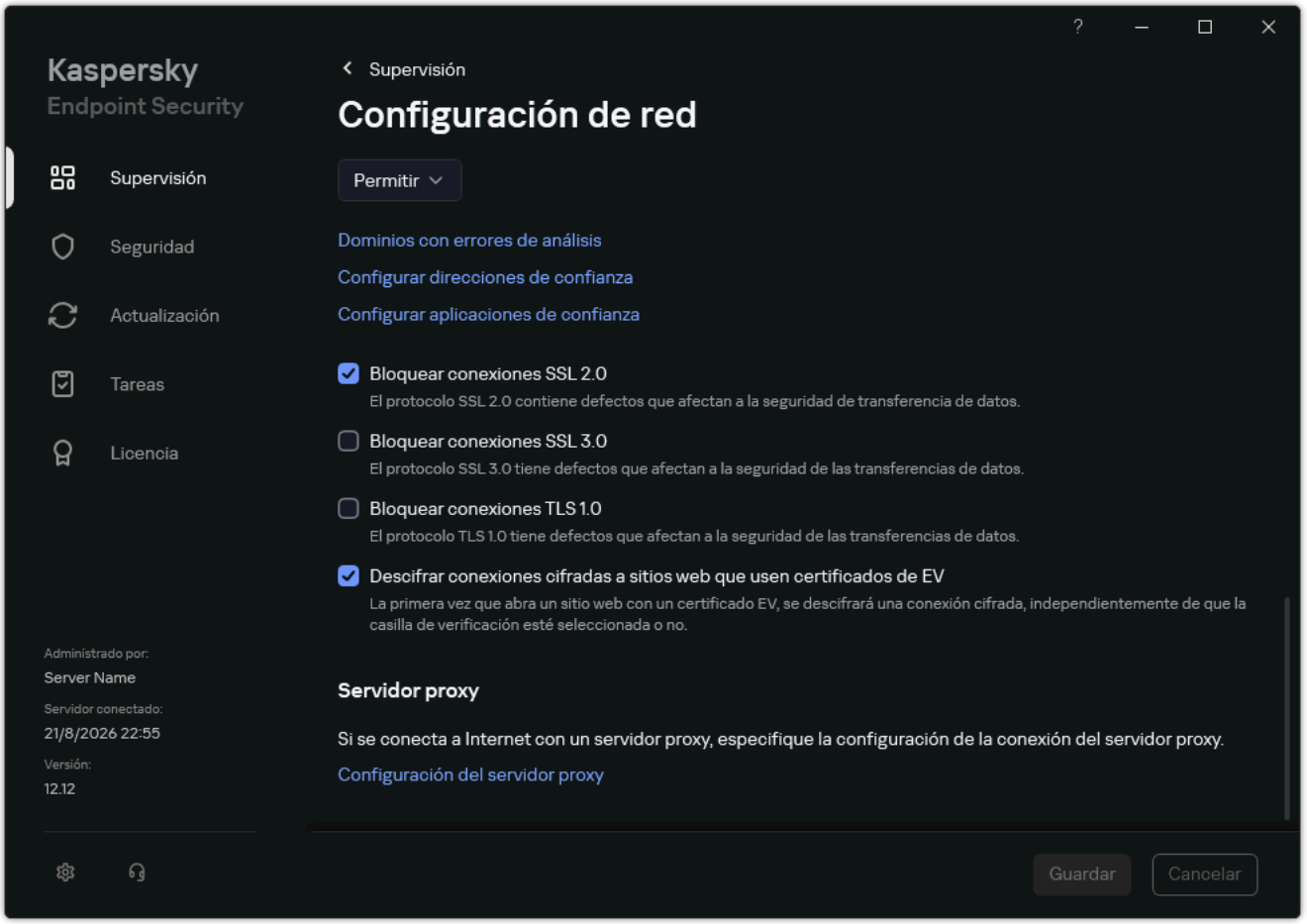
5. En el bloque **Servidor proxy**, haga clic en el botón **Configuración**.

6. En la ventana que se abre, active la casilla **No usar servidor proxy para direcciones locales**.

7. Guarde los cambios.

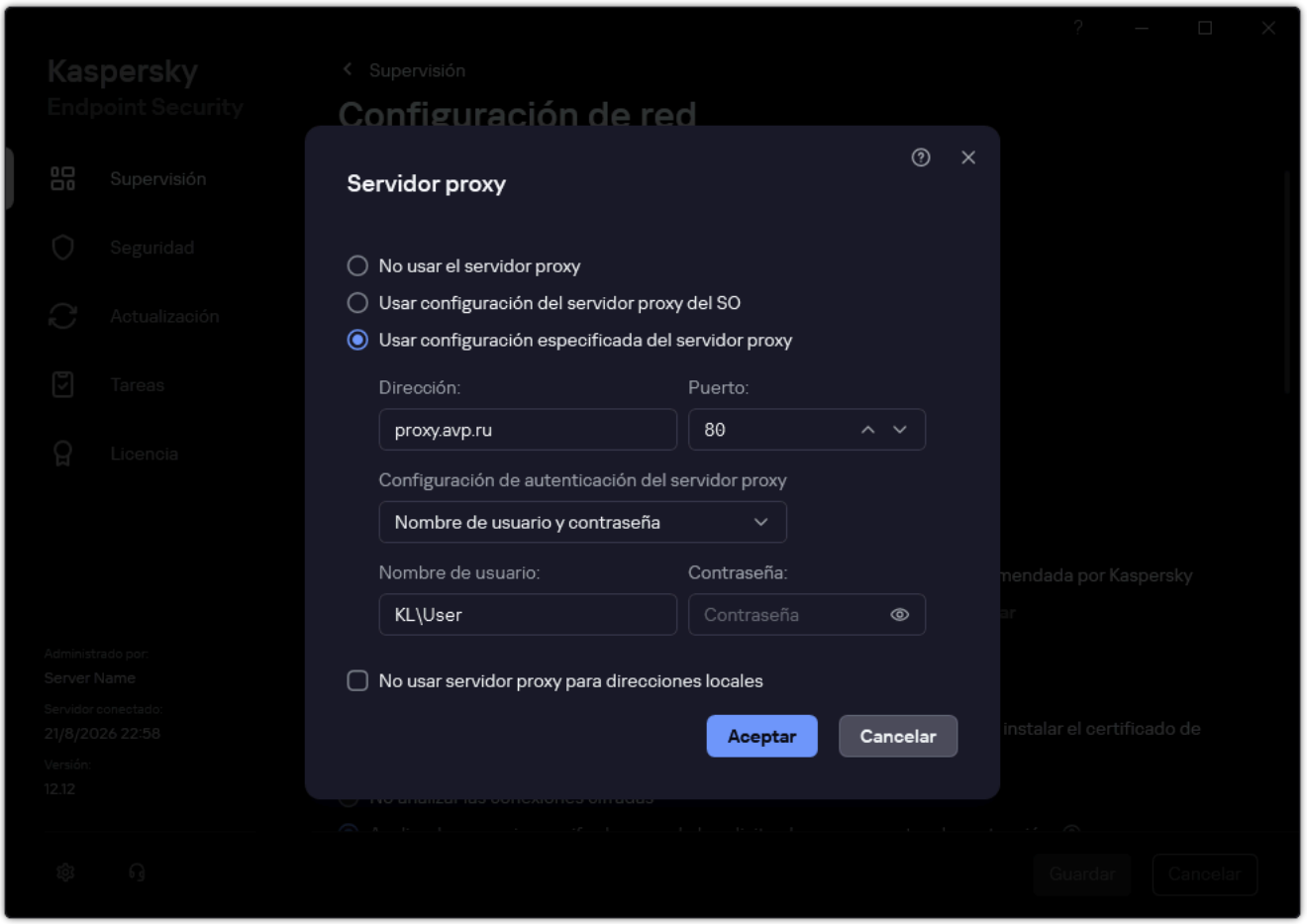
Para establecer la configuración del servidor proxy en la interfaz de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.



Configuración de red de aplicaciones

3. En el bloque **Servidor proxy**, haga clic en el enlace **Configuración del servidor proxy**.



Configuración de conexión al servidor proxy

4. En la ventana que se abre, seleccione una de las siguientes opciones para determinar la dirección del servidor proxy:

   - **Usar configuración del servidor proxy del SO**.

     Esta opción está seleccionada de forma predeterminada. Kaspersky Endpoint Security utiliza la configuración del servidor proxy que se define en la configuración del sistema operativo.

   - **Usar configuración especificada del servidor proxy**.

     Si seleccionó esta opción, establezca la configuración para conectarse al servidor proxy: dirección y puerto del servidor proxy.

5. Seleccione cómo desea que la aplicación se autentique en el servidor proxy. De forma predeterminada, la aplicación utiliza la autenticación NTLM de dominio del usuario actual.

6. Si desea desactivar el uso del servidor proxy al actualizar las bases de datos y los módulos de aplicaciones desde una carpeta compartida, seleccione la casilla **No usar servidor proxy para direcciones locales**.

7. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security utilizará el servidor proxy para descargar actualizaciones de los módulos de la aplicación y de la base de datos. Kaspersky Endpoint Security también usará un servidor proxy para acceder a servidores KSN y a los servidores de activación de Kaspersky. Si se requiere autenticación en el servidor proxy, pero las credenciales de la cuenta de usuario no se proporcionaron o son incorrectas, Kaspersky Endpoint Security le solicitará el nombre de usuario y la contraseña.

Reversión de la última actualización

Una vez actualizadas las bases de datos y los módulos de la aplicación por segunda vez, la función de deshacer la actualización de las bases de datos y los módulos de la aplicación a sus versiones anteriores pasa a estar disponible.

Cada vez que un usuario inicia el proceso de actualización, Kaspersky Endpoint Security crea una copia de seguridad de las bases de datos y de los módulos de la aplicación actuales. Esto permite deshacer la actualización de las bases de datos y de los módulos de la aplicación y restablecer sus versiones anteriores cuando sea necesario. Revertir la última actualización es útil, por ejemplo, si una nueva versión de la base de datos provoca un falso positivo que provoca que Kaspersky Endpoint Security bloquee una aplicación segura.

Kaspersky Endpoint Security en modo Light Agent no admite la tarea *Revertir actualización*.

Cómo revertir la última actualización en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

1. Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Revertir actualización**.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Configurar una planificación de inicio de tarea

Configure la planificación de la tarea; por ejemplo, manualmente.

Paso 4. Definir el nombre de la tarea

Introduzca un nombre para la tarea.

Paso 7. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo revertir la última actualización en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Revertir**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve; por ejemplo, *Revertir actualización*.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

7. La nueva tarea aparecerá en la lista de tareas.

8. Active la casilla ubicada junto a la tarea.

9. Haga clic en **Iniciar**.

Cómo revertir última actualización en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Actualización**.



Tareas de actualización locales

2. En el mosaico **Restauración de las bases de datos a su versión anterior**, haga clic en el botón **Deshacer**.

Kaspersky Endpoint Security comenzará a revertir la última actualización de la base de datos. La aplicación mostrará el progreso de la reversión, el tamaño de los archivos descargados y el origen de actualizaciones. Puede detener la tarea en cualquier momento haciendo clic en el botón **Detener actualización**.

Tecnología de desinfección avanzada

Para trabajar con amenazas activas, Kaspersky Endpoint Security utiliza la tecnología de Desinfección avanzada. La Desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Puede configurar la desinfección avanzada en la configuración de la tarea *Análisis antimalware* y en la configuración de la aplicación.

Si Kaspersky Endpoint Security no puede detener la ejecución de malware, puede usar la tecnología de desinfección avanzada. Para los equipos que se encuentran bajo la directiva, la opción Desinfección avanzada está desactivada de manera predeterminada porque esta tecnología usa una cantidad significativa de recursos informáticos. Para los equipos que no están bajo la directiva, la opción Desinfección avanzada está activada de forma predeterminada.

La Desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Para usar la tecnología en servidores, debe activar la Desinfección avanzada en las propiedades de la tarea *Análisis antimalware*. Este requisito previo no es necesario para usar la tecnología en estaciones de trabajo.

Cómo activar o desactivar la tecnología de desinfección avanzada en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de la aplicación**.
4. En el bloque **General**, seleccione o desactive la casilla **Activar tecnología de desinfección avanzada** para activar o desactivar la tecnología de desinfección avanzada.
5. Guarde los cambios.

Cómo activar o desactivar la tecnología de desinfección avanzada en Web Console y Cloud Console

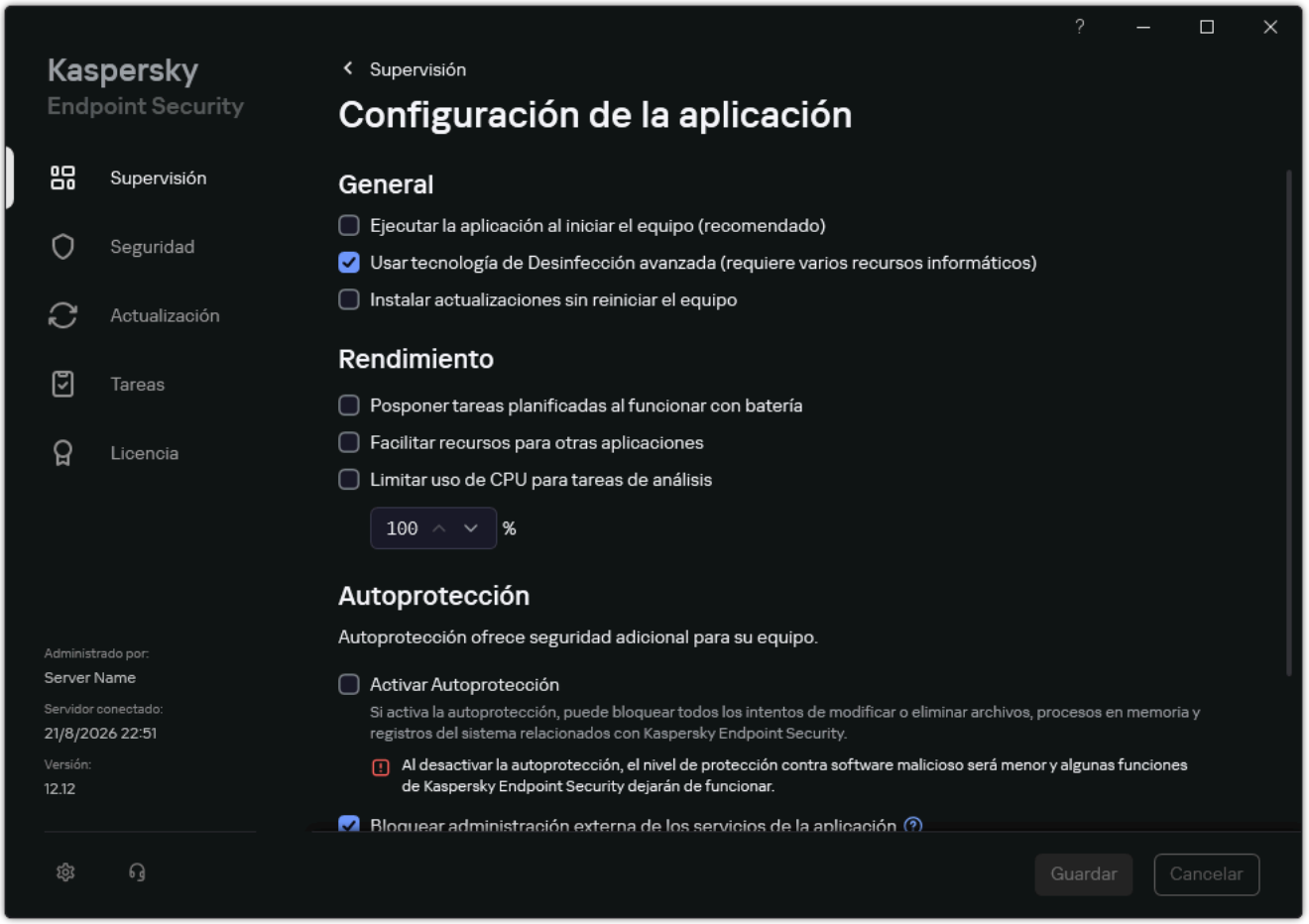
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Configuración general** → **Configuración de detección**.
5. En el bloque **Tecnología de desinfección avanzada**, active o desactive el interruptor **Tecnología de desinfección avanzada ACTIVADA** para activar o desactivar la tecnología Desinfección avanzada.
6. Guarde los cambios.

Cómo activar o desactivar la tecnología de desinfección avanzada en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. En el bloque **General**, seleccione o desactive la casilla **Usar tecnología de Desinfección avanzada (requiere varios recursos informáticos)** para activar o desactivar la tecnología de desinfección avanzada.

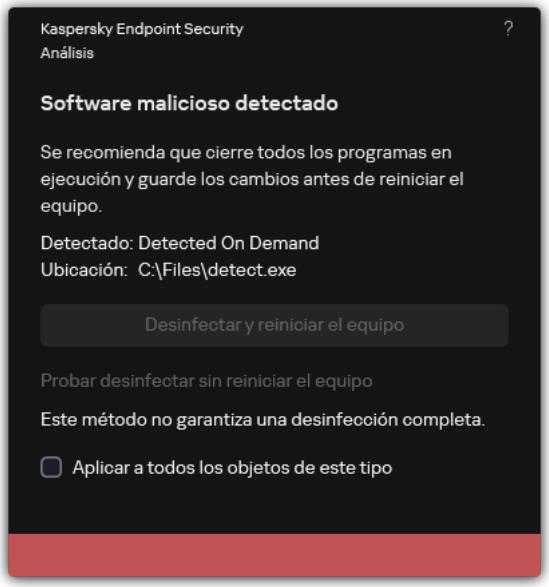
4. Guarde los cambios.

Como resultado, el usuario no puede usar la mayoría de las características del sistema operativo mientras la desinfección avanzada está en curso. Cuando la desinfección esté completa, se reiniciará el equipo.

Desinfección de amenazas activas en estaciones de trabajo

Para trabajar con amenazas activas en estaciones de trabajo, active la tecnología de Desinfección avanzada en la configuración de aplicaciones. A continuación, configure la experiencia del usuario en las propiedades de la tarea *Análisis antimalware*. Hay una casilla de verificación **Ejecutar la desinfección avanzada de inmediato** en las propiedades de la tarea. Si se establece una marca, Kaspersky Endpoint Security realizará una desinfección sin notificarle al usuario. Cuando la desinfección esté completa, se reiniciará el equipo. Si no se establece la marca, Kaspersky Endpoint Security mostrará una notificación sobre amenazas activas (consulte la figura a continuación). No puede cerrar esta notificación sin procesar el archivo.

Se realiza una desinfección avanzada durante una tarea de análisis antivirus en un equipo solo si la característica Desinfección avanzada está activada en las propiedades de la directiva aplicada a este equipo.



Notificación sobre amenazas activas

Desinfección de amenazas activas en servidores

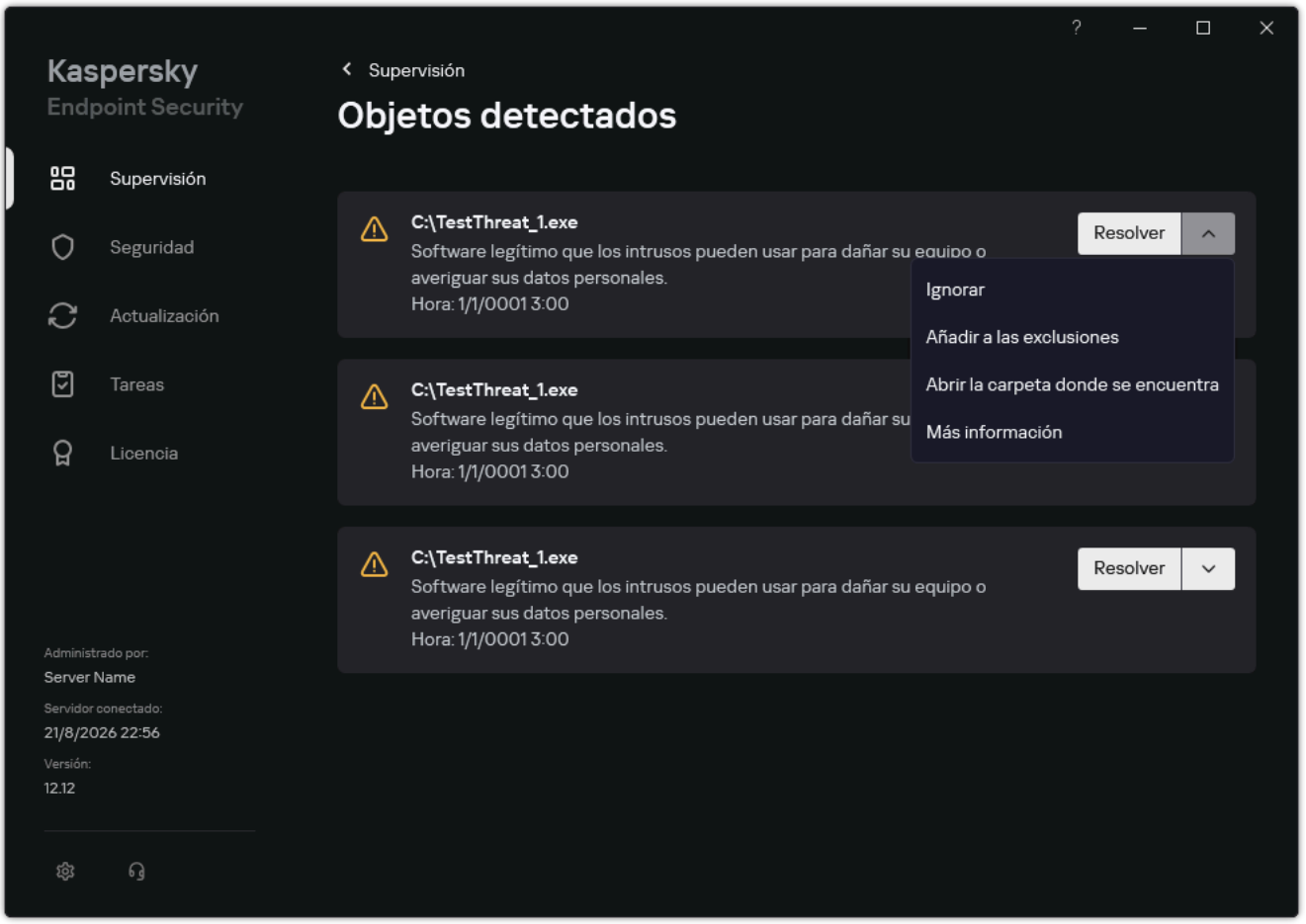
Para trabajar con amenazas activas en servidores, debe hacer lo siguiente:

- activar la tecnología de Desinfección avanzada en la configuración de aplicaciones;
- active Desinfección avanzada inmediata en las propiedades de la tarea *Análisis antimalware*.

Si Kaspersky Endpoint Security se instala en un equipo en el que se ejecuta Windows para servidores, Kaspersky Endpoint Security no muestra la notificación. Por lo tanto, no puede seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe activar la tecnología de Desinfección avanzada en la configuración de la aplicación y activar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis antimalware*. Luego, debe iniciar la tarea *Análisis antimalware*.

Eliminar amenazas no procesadas

Kaspersky Endpoint Security registra información sobre los archivos que no ha procesado por alguna razón. Esta información se recoge como eventos en la lista de amenazas activas (consulte la figura siguiente).



Una lista de amenazas activas

Se considera un archivo infectado como *procesado* si Kaspersky Endpoint Security desinfectó el archivo o eliminó la amenaza como parte del análisis del equipo en busca de virus y otro malware.

Kaspersky Endpoint Security mueve el archivo a la lista de amenazas activas si, por cualquier motivo, Kaspersky Endpoint Security no lleva a cabo una acción en este archivo de acuerdo con la configuración especificada de la aplicación al analizar el equipo en busca de virus y otras amenazas.

Esta situación puede darse en los siguientes casos:

- El archivo analizado no está disponible (por ejemplo, se encuentra en una unidad de red o en una unidad extraíble sin derechos de escritura).
- En la configuración de la tarea *Análisis antimalware*, la acción al detectar una amenaza se establece como **Informar**. Después, cuando la notificación de archivo infectado se mostró en la pantalla, el usuario seleccionó **Omitir**.

Si hay amenazas sin procesar, Kaspersky Endpoint Security cambia el icono a . En la ventana principal de la aplicación, aparece la notificación de amenaza (consulte la figura siguiente). En la consola de Kaspersky Security Center, el estado del equipo cambia a *Crítico* – .

Cómo procesar una directiva en la Consola de administración (MMC)

1. En la Consola de administración, vaya a la carpeta **Servidor de administración → Avanzado → Repositorios → Amenazas activas**.

   Se abre la lista de amenazas activas.

2. Seleccione el objeto que desea procesar.

3. Elija de qué manera quiere manejar la amenaza:

   - **Desinfectar**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

   - **Eliminar**. Si se selecciona esta opción, la aplicación elimina el archivo infectado que se detecta desde el repositorio de amenazas activas. En este caso, la aplicación mantiene el archivo detectado en la memoria del equipo. Para eliminar la amenaza del equipo, seleccione **Desinfectar**.

Cómo procesar una directiva en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Operaciones → Repositorios → Amenazas activas**.

   Se abre la lista de amenazas activas.

2. Seleccione el objeto que desea procesar.

3. Elija de qué manera quiere manejar la amenaza:

   - **Desinfectar**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

   - **Eliminar**. Si se selecciona esta opción, la aplicación elimina el archivo infectado que se detecta desde el repositorio de amenazas activas. En este caso, la aplicación mantiene el archivo detectado en la memoria del equipo. Para eliminar la amenaza del equipo, seleccione **Desinfectar**.

Cómo procesar una amenaza en la interfaz de la aplicación

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **La protección está en peligro**.

   Se abre la lista de amenazas activas.

2. Seleccione el objeto que desea procesar.

3. Elija de qué manera quiere manejar la amenaza:

   - **Resolver**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

   - **Añadir a las exclusiones**. Si se selecciona esta acción, Kaspersky Endpoint Security sugiere añadir el archivo a la lista de exclusiones del análisis. Los ajustes de la exclusión se configuran automáticamente. Si no está disponible la opción para añadir una exclusión, significa que el administrador ha desactivado la adición de exclusiones en la configuración de la directiva.

   - **Ignorar**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina la entrada de la lista de amenazas activas. Si no quedan amenazas activas en la lista, el estado del equipo se modificará a *Aceptar*. Si el objeto se vuelve a detectar, Kaspersky Endpoint Security añadirá una nueva entrada a la lista de amenazas activas.

- **Abrir la carpeta donde se encuentra**. Si se selecciona esta opción, Kaspersky Endpoint Security abre la carpeta que contiene el objeto en el administrador de archivos. A continuación, puede eliminar manualmente el objeto o mover el objeto a una carpeta que no está dentro de la cobertura de protección.

- **Más información**. Si se selecciona esta opción, Kaspersky Endpoint Security abre el sitio web de la base de datos de vulnerabilidades y amenazas de Kaspersky.

Para procesar amenazas activas en la consola de Kaspersky Security Center, debe activar la transferencia de información sobre archivos no procesados al Servidor de administración. La transferencia de datos está activada de forma predeterminada.

Cómo activar la transferencia de datos de archivos no procesados en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Informes y Almacenamiento**.
4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.
5. Seleccione la casilla **Archivos no procesados**.
6. Guarde los cambios.

Cómo activar la transferencia de datos de archivos no procesados en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Integración con KSC**.

5. En el bloque **Transferencia de datos al Servidor de administración**, seleccione la casilla de verificación **Acerca de los archivos no procesados**.

6. Guarde los cambios.



Ventana principal de la aplicación cuando se detecta una amenaza

Protección del equipo

Estado de la protección en tiempo real

Kaspersky Endpoint Security envía la configuración **Estado de protección en tiempo real** al Servidor de Administración de Kaspersky Security Center; el valor de esta configuración depende del estado actual de los componentes de protección de la aplicación en el equipo protegido (consulte la tabla siguiente).

Kaspersky Endpoint Security determina el estado de la protección en tiempo real según el estado de los siguientes componentes de la aplicación:

- Protección frente a amenazas en archivos.
- Protección frente a amenazas web.
- Protección frente a amenazas en el correo.
- Protección AMSI.
- Prevención de ataques de BadUSB.
- Protección frente a amenazas en la red.
- Firewall.
- Prevención de exploits.
- Detección de comportamiento.
- Motor de reparación.
- Prevención de intrusiones en el host.

Puede comprobar el estado de la protección en tiempo real de la aplicación en una consola de Kaspersky Security Center.

Cómo averiguar el estado de la protección en tiempo real en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos administrados**.

El estado actual de la protección en tiempo real se muestra en la lista de dispositivos, en la columna **Estado de protección en tiempo real**. Si falta la columna **Estado de protección en tiempo real**, administre la configuración de las columnas haciendo clic en el enlace **Añadir/Quitar columnas**.

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos administrados**.

El estado actual de la protección en tiempo real se muestra en la lista de dispositivos, en la columna **Estado de protección en tiempo real**. Si falta la columna **Estado de protección en tiempo real**, administre la configuración de las columnas haciendo clic en el enlace **Añadir/Quitar columnas**.

Cómo consultar la Protección del equipo en tiempo real en Web Console

En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.

El estado actual de la protección en tiempo real se muestra en la lista de dispositivos, en la columna **Estado de protección en tiempo real**. Si falta la columna **Estado de protección en tiempo real**, administre la configuración de las columnas (⚙).

Posibles valores de la configuración Estado de protección en tiempo real

Valor	Descripción
Desconocido	El Servidor de administración no dispone de información sobre el estado de la protección en tiempo real de este equipo.
No instalado	No hay ningún componente instalado.
No compatible con la licencia	La aplicación no está activada o la licencia no permite que funcionen los componentes instalados.
Fallo	Uno o varios componentes no funcionan correctamente.
Detenido	Uno o varios componentes están desactivados.
En pausa	Uno o varios componentes están en pausa.
Iniciando	Uno o varios componentes se están activando.
En ejecución	Los componentes de la aplicación están en funcionamiento.

Si el valor de la configuración **Estado de protección en tiempo real** en Kaspersky Security Center es distinto de *En ejecución*, compruebe que los componentes instalados de Kaspersky Endpoint Security incluidos en la lista estén activados y que la aplicación esté activada.

Protección frente a amenazas en archivos

El componente Protección frente a amenazas en archivos le permite evitar la infección del sistema de archivos del equipo. De forma predeterminada, el componente Protección frente a amenazas en archivos reside permanentemente en la RAM del equipo y analiza todos los archivos abiertos, guardados o ejecutados en tiempo real. Este componente analiza archivos en todas las unidades del equipo, incluidas las unidades conectadas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

El componente analiza los archivos a los que accede el usuario o la aplicación. Si se detecta un archivo malicioso, Kaspersky Endpoint Security bloquea la operación del archivo. A continuación, la aplicación desinfecta o elimina el archivo malicioso, en función de la configuración del componente Protección frente a amenazas en archivos.

Cuando se intenta acceder a un archivo cuyo contenido reside en el almacenamiento en la nube de OneDrive, Kaspersky Endpoint Security descarga el contenido y lo analiza.

Activación y desactivación de Protección frente a amenazas en archivos

De forma predeterminada, el componente Protección frente a amenazas en archivos está configurado en el modo recomendado por los expertos de Kaspersky. Para Protección frente a amenazas en archivos, Kaspersky Endpoint Security puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que la configuración del nivel de seguridad **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky (vea la tabla abajo). Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración recomendada del nivel de seguridad.

El componente Protección frente a amenazas en archivos utiliza datos recibidos de otros componentes de la aplicación. La activación de estos componentes es opcional. Los componentes que proporcionan datos adicionales incluyen los siguientes:

- Kaspersky Security Network.
- Prevención de intrusiones en el host.
- Detección de comportamiento.

Cómo activar o desactivar el componente Protección frente a amenazas en archivos en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.
4. Utilice la casilla de verificación **Protección frente a amenazas en archivos** para activar o desactivar el componente.

5. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:

   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:

     - **Máximo**. Si se selecciona este nivel de seguridad de archivos, el componente Protección frente a amenazas en archivos realiza el control más estricto de todos los archivos abiertos, guardados y ejecutados. El componente Protección frente a amenazas en archivos analiza todos los tipos de archivos en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. También analiza archivos comprimidos, paquetes de instalación y objetos OLE incrustados.

     - **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección frente a amenazas en archivos solo analiza los formatos de archivos especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo y en los objetos de OLE incrustados. El componente Protección frente a amenazas en archivos no analiza los archivos ni los paquetes de instalación.

     - **Mínimo**. La configuración de este nivel de seguridad garantiza la velocidad máxima de análisis. El componente Protección frente a amenazas en archivos solo analiza los archivos con extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. El componente Protección frente a amenazas en archivos no analiza los archivos compuestos.

   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** y defina su propia configuración del componente (consulte la tabla siguiente).

     Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Predeterminado**.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos:

   - **Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si la desinfección falla, la aplicación bloquea este archivo.

   - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea automáticamente el archivo infectado sin intentar desinfectarlo ni eliminarlo.

   - **Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.

   Antes de intentar desinfectar o eliminar un archivo infectado, la aplicación crea una copia de seguridad del archivo en caso de que necesite restaurarlo o que sea posible desinfectarlo en el futuro.

7. Guarde los cambios.

Cómo activar o desactivar el componente Protección frente a amenazas en archivos en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host** → **Protección frente a amenazas en archivos**.

5. Utilice interruptor **Protección frente a amenazas en archivos ACTIVADA** para activar o desactivar el componente.

6. Si desea añadir un nuevo objeto a la cobertura de protección:

   a. En **Configuración avanzada**, seleccione la pestaña **Cobertura de protección**.

   b. Haga clic en **Añadir**.

   c. Esta acción abrirá una ventana. En ella, seleccione los objetos que desea añadir a la cobertura de la protección.

   Usar máscaras:

   - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

   - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

   Puede utilizar máscaras en cualquier parte de la ruta de un archivo o carpeta. Por ejemplo, si desea que la cobertura del análisis incluya la carpeta descargas para todas las cuentas de usuario del equipo, ingrese la máscara `C:\Users\*\Downloads\`.

   Puede excluir un objeto de la protección sin eliminarlo de la lista de objetos en la cobertura de la protección. Para hacerlo, coloque el interruptor junto a él en la posición de apagado.

   d. Guarde los cambios.

7. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos:

   - **Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si la desinfección falla, la aplicación bloquea este archivo.

   - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea automáticamente el archivo infectado sin intentar desinfectarlo ni eliminarlo.

Antes de intentar desinfectar o eliminar un archivo infectado, la aplicación crea una copia de seguridad del archivo en caso de que necesite restaurarlo o que sea posible desinfectarlo en el futuro.

8. De ser necesario, edite la configuración avanzada de la Protección frente a amenazas en archivos.

9. Guarde los cambios.

Cómo activar o desactivar el componente Protección frente a amenazas en archivos en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.

3. Utilice interruptor **Protección frente a amenazas en archivos** para activar o desactivar el componente.

4. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:

   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:

     - **Alto**. Si se selecciona este nivel de seguridad de archivos, el componente Protección frente a amenazas en archivos realiza el control más estricto de todos los archivos abiertos, guardados y ejecutados. El componente Protección frente a amenazas en archivos analiza todos los tipos de archivos en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. También analiza archivos comprimidos, paquetes de instalación y objetos OLE incrustados.

     - **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección frente a amenazas en archivos solo analiza los formatos de archivos especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo y en los objetos de OLE incrustados. El componente Protección frente a amenazas en archivos no analiza los archivos ni los paquetes de instalación.

     - **Bajo**. La configuración de este nivel de seguridad garantiza la velocidad máxima de análisis. El componente Protección frente a amenazas en archivos solo analiza los archivos con extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. El componente Protección frente a amenazas en archivos no analiza los archivos compuestos.

   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina su propia configuración del componente (consulte la tabla siguiente).

     Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Restaurar nivel de seguridad recomendado**.

5. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos:

   - **Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si la desinfección falla, la aplicación bloquea este archivo.

- **Bloquear**. Si se selecciona esta opción, la aplicación bloquea automáticamente el archivo infectado sin intentar desinfectarlo ni eliminarlo.

- **Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.

Antes de intentar desinfectar o eliminar un archivo infectado, la aplicación crea una copia de seguridad del archivo en caso de que necesite restaurarlo o que sea posible desinfectarlo en el futuro.

6. Guarde los cambios.

Configuración de Protección frente a amenazas en archivos recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
Tipos de archivos	**Archivos analizados por formato**	Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.
Análisis heurístico	**Análisis superficial**	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
Analizar solamente archivos nuevos y modificados	**Activa**	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
Usar tecnología iSwift	**Activa**	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
Usar tecnología iChecker	**Activa**	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).
Analizar archivos en formatos de Microsoft Office	**Activa**	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
Analizar archivos de formatos de correo electrónico	**Activa**	Analiza archivos con formato de correo electrónico. La aplicación analiza archivos MSG y EML. Los archivos con formato de correo electrónico también incluyen objetos OLE y archivos MHT. Kaspersky Endpoint Security analiza los archivos con formato de correo electrónico que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
Modo de análisis	**Modo inteligente**	En este modo, Protección frente a amenazas en archivos analiza un objeto en función de un análisis de las acciones aplicadas al objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.
Acción al detectar una amenaza	**Desinfectar; eliminar si la desinfección falla**	Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.

Suspensión automática de Protección frente a amenazas en archivos

Puede configurar la Protección frente a amenazas en archivos para que se suspenda de forma automática a una hora concreta o cuando utilice determinados programas.

La Protección frente a amenazas en archivos se debería suspender solo como último recurso cuando entra en conflicto con algunas aplicaciones. Si surge algún conflicto mientras se ejecuta un componente, se recomienda que se comunique con el Soporte técnico de Kaspersky. Los expertos de soporte le ayudarán a configurar el componente de Protección frente a amenazas en archivos para que se ejecute simultáneamente con otras aplicaciones en su equipo.

Para configurar la suspensión automática de la Protección frente a amenazas en archivos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Pausar la Protección frente a amenazas en archivos**, haga clic en el enlace **Pausar la Protección frente a amenazas en archivos**.
5. En la ventana que se abre, establezca la configuración para pausar la Protección frente a amenazas en archivos:
   a. Configure una programación para pausar la Protección frente a amenazas en archivos automáticamente.
   b. Cree una lista de aplicaciones cuyo funcionamiento debería hacer que la Protección frente a amenazas en archivos detenga sus actividades.
6. Guarde los cambios.

Modificación de las acciones tomadas en archivos infectados por parte del componente Protección frente a amenazas en archivos

De forma predeterminada, el componente Protección frente a amenazas en archivos automáticamente intenta desinfectar todos los archivos infectados que se detecten. Si la desinfección falla, el componente Protección frente a amenazas en archivos elimina estos archivos.

Para cambiar la acción realizada a los archivos infectados por el componente de Protección frente a amenazas en archivos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.

3. En el bloque **Acción al detectar una amenaza**, seleccione la opción correspondiente:

   - **Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo.
   - **Desinfectar; bloquear si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si la desinfección falla, la aplicación bloquea este archivo.
   - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea automáticamente el archivo infectado sin intentar desinfectarlo ni eliminarlo.

   Antes de intentar desinfectar o eliminar un archivo infectado, la aplicación crea una copia de seguridad del archivo en caso de que necesite restaurarlo o que sea posible desinfectarlo en el futuro.

4. Guarde los cambios.

Formación la cobertura de protección del componente Protección frente a amenazas en archivos

La cobertura de protección hace referencia a los objetos que analiza el componente cuando está activado. Las coberturas de protección de los distintos componentes tienen distintas propiedades. La ubicación y el tipo de archivos que se van a analizar son propiedades de la cobertura de protección del componente Protección frente a amenazas en archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza solo los archivos potencialmente infectables ejecutados desde discos duros, unidades extraíbles y unidades de red.

Al seleccionar el tipo de archivos que vayan a analizarse, tenga en cuenta lo siguiente:

1. Hay una probabilidad baja de introducir código malicioso en archivos de determinados formatos y su posterior activación (por ejemplo, formato TXT). De igual modo, otros formatos de archivos contienen código ejecutable (por ejemplo, .exe o .dll). El código ejecutable también puede estar contenido en formatos de archivo que no están destinados para este fin (por ejemplo, el formato DOC). Es elevado el riesgo de penetración y activación de código malicioso en estos archivos.
2. Un intruso puede enviar un virus u otra aplicación maliciosa a su equipo en un archivo ejecutable al que se ha cambiado el nombre con la extensión .txt. Si selecciona el análisis de archivos por extensión, la aplicación omitirá el archivo durante el análisis. Si se selecciona el análisis de archivos por formato, Kaspersky Endpoint Security analiza el encabezado del archivo sin importar su extensión. Si se determina que el archivo es de un formato ejecutable (por ejemplo, EXE), se lo somete a análisis.

Para crear la Cobertura de protección:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.
3. Haga clic en **Configuración avanzada**.

4. En el bloque **Tipos de archivos**, especifique el tipo de archivo que desea que el componente Protección frente a amenazas en archivos analice:

   - **Todos los archivos**. Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones).

   - **Archivos analizados por formato**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.

   - **Archivos analizados por extensión**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. El formato de archivo se determina en función de su extensión.

5. Haga clic en el enlace **Editar cobertura de protección**.

6. En la ventana que se abre, seleccione los objetos que desea añadir a la cobertura de protección o excluir de ella.

   No puede eliminar ni editar objetos que se incluyan en la cobertura de protección predeterminada.

7. Si desea añadir un nuevo objeto a la cobertura de protección:

   a. Haga clic en **Añadir**.

      Se abre el árbol de carpetas.

   b. En el campo **Ruta**, introduzca la ruta a la carpeta o archivo.

      Usar máscaras:

      - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

      - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

      - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

      Puede utilizar máscaras en cualquier parte de la ruta de un archivo o carpeta. Por ejemplo, si desea que la cobertura del análisis incluya la carpeta descargas para todas las cuentas de usuario del equipo, ingrese la máscara `C:\Users\*\Downloads\`.

      El objeto **Este equipo** de la lista de recursos de archivos del equipo incluye los siguientes objetos: **Todos los discos duros**, **Todas las unidades de red** y **Todas las unidades extraíbles**.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura del análisis. Para hacerlo, desactive la casilla de verificación junto al objeto.

8. Guarde los cambios.

Uso de métodos de análisis

Kaspersky Endpoint Security usa una técnica de análisis llamada Aprendizaje automático y análisis de firmas. Durante el análisis de firmas, Kaspersky Endpoint Security equipara el objeto detectado con los registros en su base de datos. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.

Para aumentar la eficacia de la protección, puede usar el análisis heurístico. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.

Para configurar el uso del análisis heurístico en el funcionamiento del componente Protección frente a amenazas en archivos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en **Configuración avanzada**.
4. Si desea que la aplicación utilice un análisis heurístico para la protección frente a amenazas en archivos, seleccione la casilla **Análisis heurístico** en el bloque **Métodos de análisis**. A continuación, utilice el control deslizante para definir el análisis de nivel heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.
5. Guarde los cambios.

Utilización de las tecnologías de análisis en el funcionamiento del componente Protección frente a amenazas en archivos

Para configurar el uso de tecnologías de análisis en el funcionamiento del componente Protección frente a amenazas en archivos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en **Configuración avanzada**.

4. En el bloque **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar para la protección frente a amenazas en archivos:

   - **Usar tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

   - **Usar tecnología iChecker**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

5. Guarde los cambios.

Optimización del análisis de archivos

Puede optimizar el análisis de archivos realizado por el componente Protección frente a amenazas en archivos, lo que reduce el tiempo de análisis y aumenta la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede conseguir si analiza solamente los archivos nuevos y los que se hayan modificado desde el último análisis. Este modo se aplica tanto a archivos simples como a compuestos.

También puede activar el uso de las tecnologías iChecker e iSwift, que optimizan la velocidad del análisis de archivos mediante la exclusión de archivos que no se han modificado desde el análisis más reciente.

Para optimizar el análisis de archivos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Optimización**, seleccione la casilla de verificación **Analizar solamente archivos nuevos y modificados**.

5. Guarde los cambios.

Análisis de archivos compuestos

Una técnica común para ocultar virus y otro tipo de software malicioso (malware) consiste en implantarlos en archivos compuestos, como archivos comprimidos o bases de datos. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

El método empleado para procesar un archivo compuesto infectado (desinfección o eliminación) depende del tipo de este.

El componente Protección frente a amenazas en archivos desinfecta archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR y ICE, y elimina archivos con otros formatos (excepto bases de datos de correo).

Para configurar el análisis de archivos compuestos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiera analizar: archivos, paquetes de distribución, correo o archivos en formatos de Office.
5. Si el análisis de solo archivos nuevos y modificados está desactivado, establezca la configuración para analizar cada tipo de archivo compuesto: analice todos los archivos de este tipo o solo los archivos nuevos.

   Si está activado el análisis de solo archivos nuevos y modificados, Kaspersky Endpoint Security analiza solo archivos nuevos y modificados de todos los tipos de archivos compuestos.
6. Establezca la configuración avanzada para el análisis de archivos compuestos.

   - **No descomprimir archivos compuestos grandes**.

     Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security no escanea archivos compuestos cuyo tamaño exceda el valor especificado.

     Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.

     Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos grandes**.

   - **Descomprimir archivos compuestos en segundo plano**.

     Si la casilla de verificación está seleccionada, Kaspersky Endpoint Security proporciona acceso a archivos compuestos cuyo tamaño sea superior al valor especificado antes de analizar estos archivos. En este caso, Kaspersky Endpoint Security extrae y analiza los archivos compuestos en segundo plano.

Kaspersky Endpoint Security proporciona acceso a archivos compuestos cuyo tamaño sea inferior a este valor solo después de extraer y analizar estos archivos.

Si la casilla de verificación no está seleccionada, Kaspersky Endpoint Security proporciona acceso a archivos compuestos solo después de extraer y analizar archivos de cualquier tamaño.

7. Guarde los cambios.

Modificación del modo de análisis

Modo de análisis remite a la condición que activa el análisis de archivos por parte del componente Protección frente a amenazas en archivos. De forma predeterminada, Kaspersky Endpoint Security analiza archivos en modo inteligente. En este modo de análisis, el componente Protección frente a amenazas en archivos analiza las operaciones que el usuario o una aplicación en nombre del usuario (con la cuenta actual activa o una cuenta de usuario diferente) o el sistema operativo han realizado con un archivo. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office Word la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.

Para modificar el modo de análisis de archivos:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Modo de análisis**, seleccione el modo requerido:
   - **Modo inteligente**. En este modo, Protección frente a amenazas en archivos analiza un objeto en función de un análisis de las acciones aplicadas al objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.
   - **Al acceder y modificar**. En este modo, Protección frente a amenazas en archivos analiza objetos cuando se intenta abrirlos o modificarlos.
   - **Al acceder**. En este modo, Protección frente a amenazas en archivos analiza objetos solo tras intentar abrirlos.
   - **Al ejecutar**. En este modo, Protección frente a amenazas en archivos solo analiza objetos tras intentar ejecutarlos.
5. Guarde los cambios.

Análisis de contenedores

Un *contenedor* es un entorno aislado en el que se puede ejecutar una aplicación sin interactuar directamente con el sistema operativo. El uso de contenedores implica los siguientes riesgos:

- Los piratas informáticos pueden aprovechar las vulnerabilidades de la organización en contenedores para poner en peligro las aplicaciones dentro del contenedor.
- Los piratas informáticos pueden explotar una configuración insegura del entorno del contenedor para obtener acceso no autorizado a los datos del equipo o para poner en peligro la integridad del sistema.
- Un ataque exitoso a un contenedor puede permitir a un pirata informático obtener acceso a los datos del equipo.
- Los piratas informáticos pueden aprovechar las vulnerabilidades de la red para interceptar el tráfico de red.

Kaspersky Endpoint Security analiza archivos no solo en discos, sino también dentro de contenedores. Es decir, Kaspersky Endpoint Security es una herramienta externa para detectar actividad maliciosa dentro de los contenedores. Esto permite mantener el rendimiento de los contenedores y evita conflictos con otras aplicaciones dentro del contenedor. No se admite la instalación de Kaspersky Endpoint Security dentro del contenedor.

Además de proporcionar seguridad a los contenedores, Kaspersky Endpoint Security permite administrar aplicaciones dentro de contenedores mediante Control de aplicaciones. El Control de aplicaciones se configura para contenedores de la misma manera que para aplicaciones instaladas en el equipo. Control de integridad del sistema también admite contenedores.

Requisitos del contenedor

- El contenedor debe ser un contenedor Docker. No se admiten otras herramientas de organización de contenedores.
- El contenedor debe ejecutarse en modo de aislamiento de proceso. El modo de aislamiento Hyper-V no se admite.
- El contenedor debe colocarse en un servidor Windows Server 2016, 2019 o 2022 (Docker Host).
- El contenedor debe incluir una imagen de Windows (Docker Image). Windows 10 y 11 no se admiten. Las imágenes de Linux no se admiten.

Acción al detectar una amenaza

Si se detecta una amenaza dentro de un contenedor, la aplicación aplica la acción seleccionada para el componente Protección frente a amenazas en archivos. Análisis de contenedores tiene configuraciones adicionales (consulte las instrucciones a continuación). Si se detecta una amenaza, la aplicación bloquea la actividad maliciosa y realiza la acción seleccionada (por ejemplo, intenta desinfectar el objeto). Kaspersky Endpoint Security puede detener el contenedor si el objeto detectado no se puede desinfectar. De forma predeterminada, la función de detención de contenedores está desactivada.

Cómo configurar el análisis de contenedores en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.
4. Haga clic en **Configuración**.
5. Se abre una ventana; en ella, seleccione la pestaña **Adicional**.
6. En el bloque **Análisis de operaciones de archivos ejecutadas en contenedores de Windows**, establezca la configuración del análisis:
   - **Detener el contenedor si la desinfección falla**. Es posible que la aplicación no tenga suficientes derechos de lectura y escritura para el objeto detectado. En ese caso, es imposible desinfectar o eliminar el objeto detectado. Si esta casilla de verificación está seleccionada, la aplicación bloquea el objeto detectado y detiene el contenedor. Si esta casilla está desactivada, la aplicación solo bloquea el objeto detectado.
   - **No analizar operaciones de archivos ejecutadas en contenedores de Windows**. Si la casilla de verificación está seleccionada, la aplicación analiza el contenedor solo cuando se inicia. Si la casilla de verificación está desactivada, la aplicación analiza el contenedor continuamente en tiempo real.
7. Guarde los cambios.

Cómo configurar el análisis de contenedores en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Protección frente a amenazas en archivos**.
5. En **Configuración avanzada**, seleccione la pestaña **Rendimiento**.
6. En el bloque **Optimización de análisis**, establezca la configuración del análisis:
   - **Detener contenedor si la desinfección falla**. Es posible que la aplicación no tenga suficientes derechos de lectura y escritura para el objeto detectado. En ese caso, es imposible desinfectar o eliminar el objeto detectado. Si esta casilla de verificación está seleccionada, la aplicación bloquea el objeto detectado y detiene el contenedor. Si esta casilla está desactivada, la aplicación solo bloquea el objeto detectado.
   - **No analizar operaciones de archivos ejecutadas en contenedores de Windows**. Si la casilla de verificación está seleccionada, la aplicación analiza el contenedor solo cuando se inicia. Si la casilla de verificación está desactivada, la aplicación analiza el contenedor continuamente en tiempo real.
7. Guarde los cambios.

Cómo configurar el análisis de contenedores en la interfaz de la aplicación.

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en archivos**.
3. En el bloque **Análisis de operaciones de archivos ejecutadas en contenedores de Windows**, establezca la configuración del análisis:
   - **Detener el contenedor si la desinfección falla**. Es posible que la aplicación no tenga suficientes derechos de lectura y escritura para el objeto detectado. En ese caso, es imposible desinfectar o eliminar el objeto detectado. Si esta casilla de verificación está seleccionada, la aplicación bloquea el objeto detectado y detiene el contenedor. Si esta casilla está desactivada, la aplicación solo bloquea el objeto detectado.
   - **No analizar operaciones de archivos ejecutadas en contenedores de Windows**. Si la casilla de verificación está seleccionada, la aplicación analiza el contenedor solo cuando se inicia. Si la casilla de verificación está desactivada, la aplicación analiza el contenedor continuamente en tiempo real.
4. Guarde los cambios.

Prevención de intrusiones en el host

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El componente Prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus y el servicio en la nube Kaspersky Security Network.

El componente controla el funcionamiento de las aplicaciones mediante el uso de *derechos de las aplicaciones*. Los derechos de las aplicaciones incluyen los siguientes parámetros de acceso:

- Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro)
- Acceso a datos personales (por exemplo, archivos y aplicaciones)

La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

Durante el primer inicio de la aplicación, el componente Prevención de intrusiones en el host realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

   Se le recomienda participar en Kaspersky Security Network para ayudar al componente Prevención de intrusiones en el host a trabajar con más eficacia.

3. Coloca la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima*, *No fiable*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

   Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

   Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la configuración del componente Prevención de intrusiones en el host. Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea las acciones de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza *Restricción máxima* se les niega el acceso a los módulos del sistema operativo.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

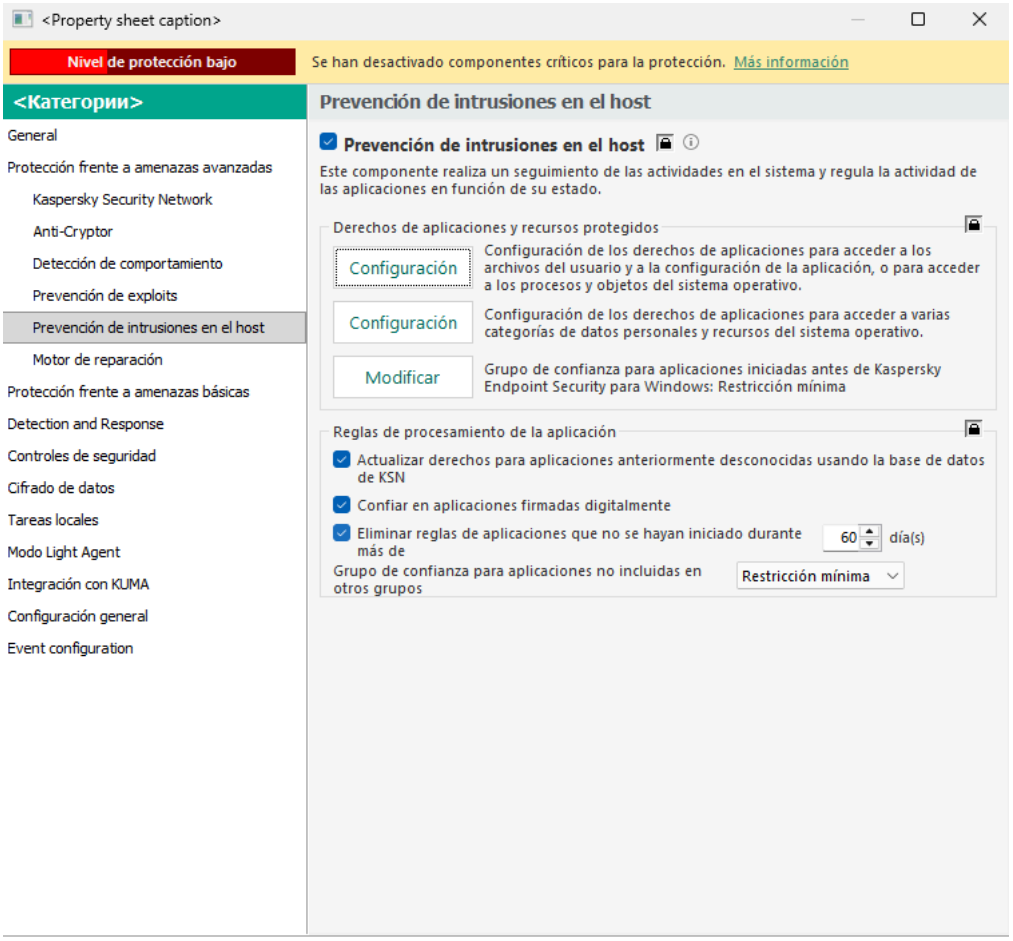
Activación y desactivación de Prevención de intrusiones en el host

De forma predeterminada, el componente Prevención de intrusiones en el host está configurado y se ejecuta en el modo recomendado por los expertos de Kaspersky.

Cómo activar o desactivar el componente Prevención de intrusiones en el host en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. Utilice la casilla de verificación **Prevención de intrusiones en el host** para activar o desactivar el componente.

5. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el componente Prevención de intrusiones en el host en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host → Prevención de intrusiones en el host**.

5. Utilice interruptor **Prevención de intrusiones en el host ACTIVADA** para activar o desactivar el componente.

6. Guarde los cambios.

Cómo activar o desactivar el componente Prevención de intrusiones en el host en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.

3. Utilice interruptor **Prevención de intrusiones en el host** para activar o desactivar el componente.

4. Guarde los cambios.

Si el componente Prevención de intrusiones en el host está activado, Kaspersky Endpoint Security incluye una aplicación en un grupo de confianza en función del nivel de peligro que represente dicha aplicación para el equipo. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza.

Gestionar grupos de confianza de aplicaciones

Cuando la aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host comprueba la seguridad de la aplicación y la coloca en uno de los grupos de confianza.

En la primera etapa del análisis de aplicaciones, Kaspersky Endpoint Security busca en la base de datos interna de aplicaciones conocidas una entrada coincidente y, simultáneamente, envía una solicitud a la base de datos de Kaspersky Security Network (si hay alguna conexión a Internet disponible). Según los resultados de la búsqueda en la base de datos interna y la base de datos de Kaspersky Security Network, la aplicación se sitúa en un grupo de confianza. Cada vez que la aplicación se inicia posteriormente, Kaspersky Endpoint Security envía una nueva consulta a la base de datos de KSN y sitúa la aplicación en un grupo de confianza diferente si la reputación de la aplicación en la base de datos de KSN ha cambiado.

Puede seleccionar un grupo de confianza en el que desea que Kaspersky Endpoint Security coloque automáticamente todas las aplicaciones desconocidas. Las aplicaciones que se han estado ejecutando antes de que se iniciara Kaspersky Endpoint Security se colocan automáticamente en el grupo de confianza establecido en la configuración de Prevención de intrusiones del host.

> En las aplicaciones que se iniciaron antes que Kaspersky Endpoint Security, solo se controla la actividad de la red. El control se realiza según las reglas de red especificadas en la configuración del Firewall.

Cambiar el grupo de confianza de una aplicación

Cuando la aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host comprueba la seguridad de la aplicación y la coloca en uno de los grupos de confianza.

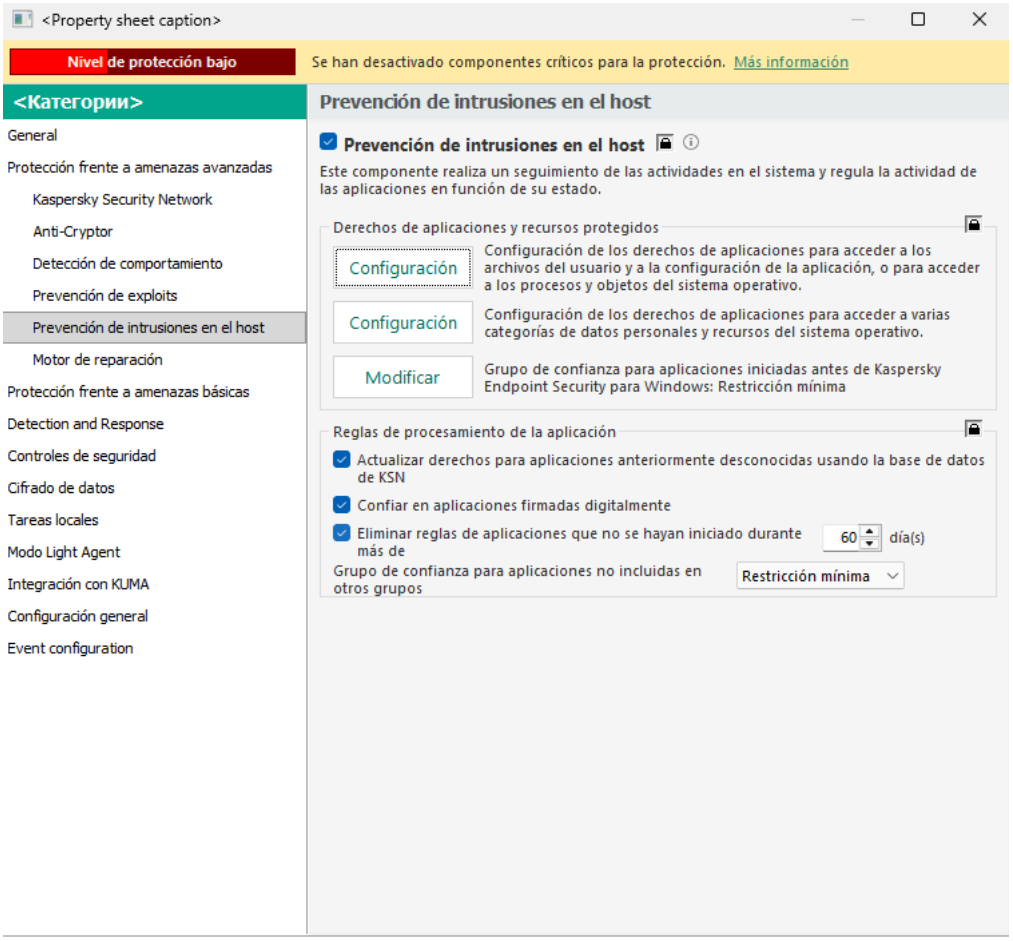
> Los especialistas de Kaspersky no recomiendan mover aplicaciones del grupo de confianza asignado automáticamente a otro grupo diferente. Considere, en cambio, modificar los derechos de una aplicación en particular cuando resulte necesario.

Cómo cambiar el grupo de confianza de una aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

5. Seleccione la pestaña **Derechos de la aplicación**.

6. Haga clic en **Añadir**.

7. En la ventana que se abre, introduzca los criterios para buscar la aplicación cuyo grupo de confianza desea cambiar.

   Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

8. Haga clic en **Actualizar**.

   Kaspersky Endpoint Security buscará la aplicación en la lista consolidada de aplicaciones instaladas en equipos administrados. Kaspersky Endpoint Security mostrará una lista de aplicaciones que coincidan con sus criterios de búsqueda.

9. Seleccione la aplicación pertinente.

10. En la lista desplegable **Añadir aplicación seleccionada al grupo de confianza**, seleccione el grupo de confianza necesario para la aplicación.

11. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo cambiar el grupo de confianza de una aplicación en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
6. Seleccione la pestaña **Derechos de la aplicación**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.
7. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir una aplicación a un grupo de confianza.
8. Seleccione el grupo de confianza correspondiente para la aplicación.
9. Seleccione el tipo **Aplicación**. Ir al paso siguiente.

   Si desea cambiar el grupo de confianza para varias aplicaciones, seleccione el tipo **Grupo** y defina un nombre para el grupo de aplicaciones.
10. En la lista de aplicaciones abiertas, seleccione las aplicaciones cuyo grupo de confianza desea cambiar.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.
11. Finalice el asistente.

    La aplicación se añadirá al grupo de confianza.
12. Guarde los cambios.

Cómo cambiar el grupo de confianza de una aplicación en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Haga clic en **Administrar aplicaciones**.

   Esto abre la lista de aplicaciones instaladas.
4. Seleccione la aplicación pertinente.
5. En el menú contextual de la aplicación, haga clic en **Restricciones** → **<grupo de confianza>**.
6. Guarde los cambios.

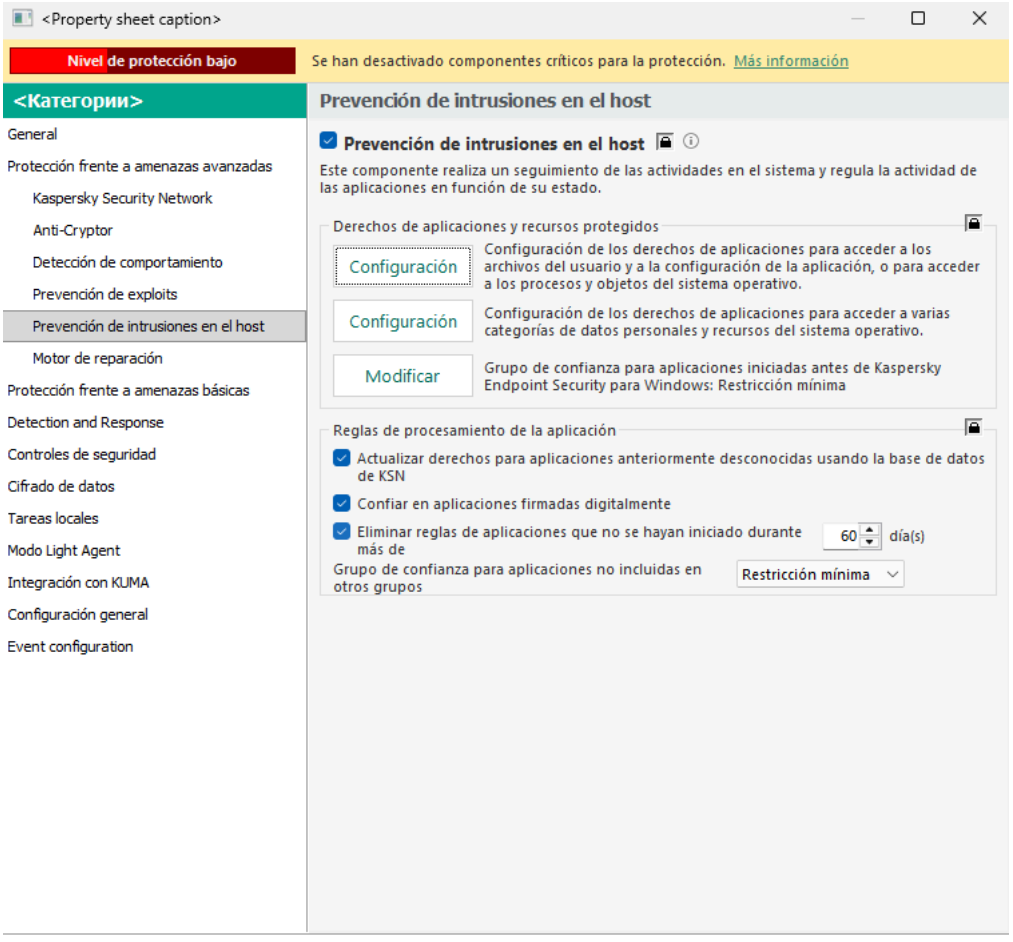
En consecuencia, la aplicación se colocará en el otro grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza. Se asignará a la aplicación el estado *(definido por el usuario)*. Si se cambia la reputación de la aplicación en Kaspersky Security Network, el componente de prevención de intrusiones en el host dejará el grupo de confianza de esta aplicación sin cambios.

Configuración de derechos del grupo de confianza

Los derechos de aplicación óptimos se crean para diferentes grupos de confianza de forma predeterminada. Los grupos de aplicaciones que forman parte de un grupo de confianza heredan de este la configuración de sus derechos.

Cómo cambiar los derechos del grupo de confianza en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
5. Vaya a la pestaña **Derechos de la aplicación**.
6. Seleccione el grupo de confianza pertinente.

7. En el menú contextual del grupo de confianza, seleccione **Derechos del grupo**.

   Se abren las propiedades del grupo de confianza.

8. Realice una de las siguientes acciones:

   - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
   - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Permisos**.

   La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

9. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y elegir la opción necesaria: **Heredar**, **Permitir** (✓) o **Bloquear** (⊘).

10. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (✓/⊘).

    Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

11. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo cambiar los derechos de un grupo de confianza en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

6. Vaya a la pestaña **Derechos de la aplicación**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.

7. En la parte izquierda de la ventana, seleccione el grupo de confianza relevante.

8. En la parte derecha de la ventana, en la lista desplegable, lleve a cabo una de las siguientes acciones:

   - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
   - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Permisos**.

   La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

9. Para el recurso relevante, en la columna de la acción correspondiente, seleccione la opción necesaria: **Heredar**, **Permitir** (), **Bloquear** ().
10. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (/).

    Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

11. Guarde los cambios.

Cómo cambiar los derechos del grupo de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.
3. Haga clic en **Administrar aplicaciones**.

   Esto abre la lista de aplicaciones instaladas.

4. Seleccione el grupo de confianza pertinente.
5. En el menú contextual del grupo de confianza, seleccione **Detalles y reglas**.

   Se abren las propiedades del grupo de confianza.

6. Realice una de las siguientes acciones:

   - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
   - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Permisos**.

   La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

7. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y elegir la opción necesaria: **Heredar**, **Permitir** () o **Rechazar** ().

8. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** ( ).

   Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

9. Guarde los cambios.

Se cambiarán los derechos del grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza. El estado ■ (*Configuración personalizada*) se asignará al grupo de confianza.

Seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security

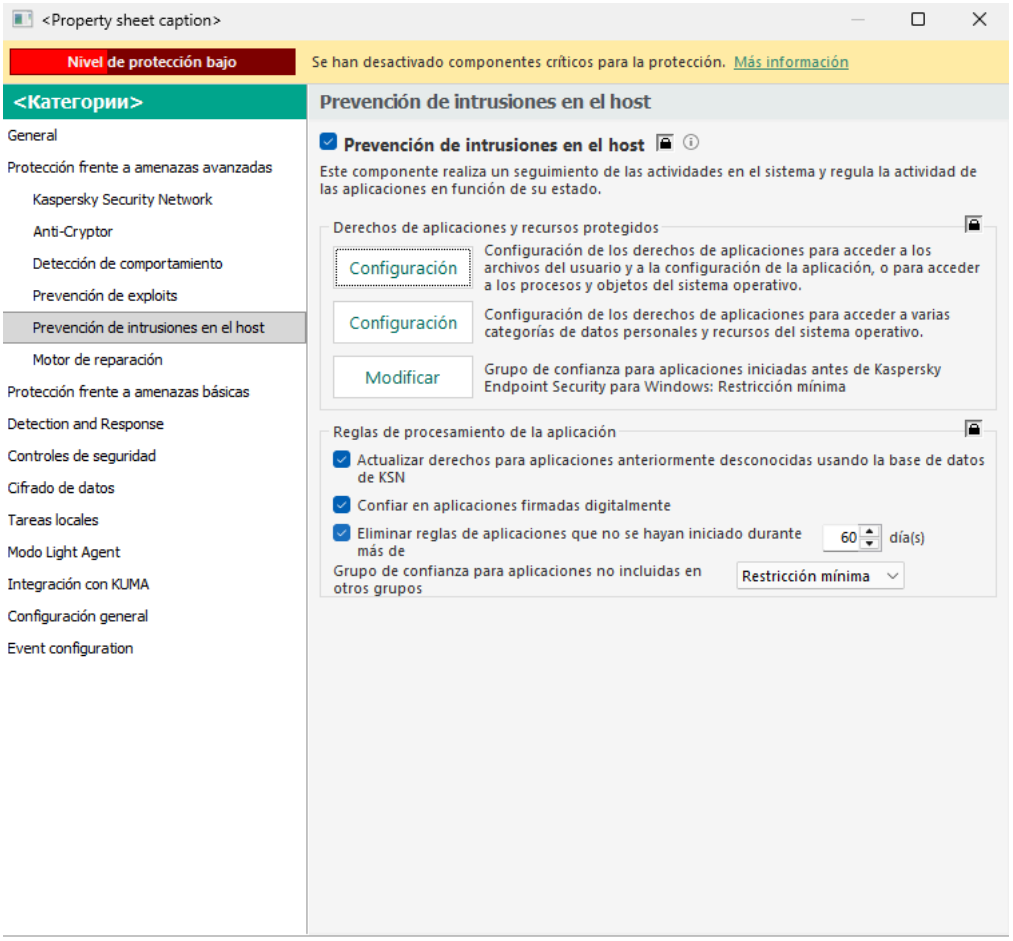
En las aplicaciones que se iniciaron antes que Kaspersky Endpoint Security, solo se controla la actividad de la red. El control se realiza según las reglas de red especificadas en la configuración del Firewall. Para especificar qué reglas de red se deben aplicar a la supervisión de la actividad de la red de tales aplicaciones, debe seleccionar un grupo de confianza.

Cómo seleccionar un grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Modificar**.

5. Para el parámetro **Grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security**, seleccione el grupo de confianza apropiado.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar un grupo de confianza para las aplicaciones iniciadas antes de Kaspersky Endpoint Security en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host → Prevención de intrusiones en el host**.

5. Para el parámetro **Grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security**, seleccione el grupo de confianza apropiado.

6. Guarde los cambios.

Cómo seleccionar un grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.
3. En el bloque **Grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security**, seleccione el grupo de confianza adecuado.
4. Guarde los cambios.

Como resultado, una aplicación que se inicia antes que Kaspersky Endpoint Security se incluirá en el otro grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza.

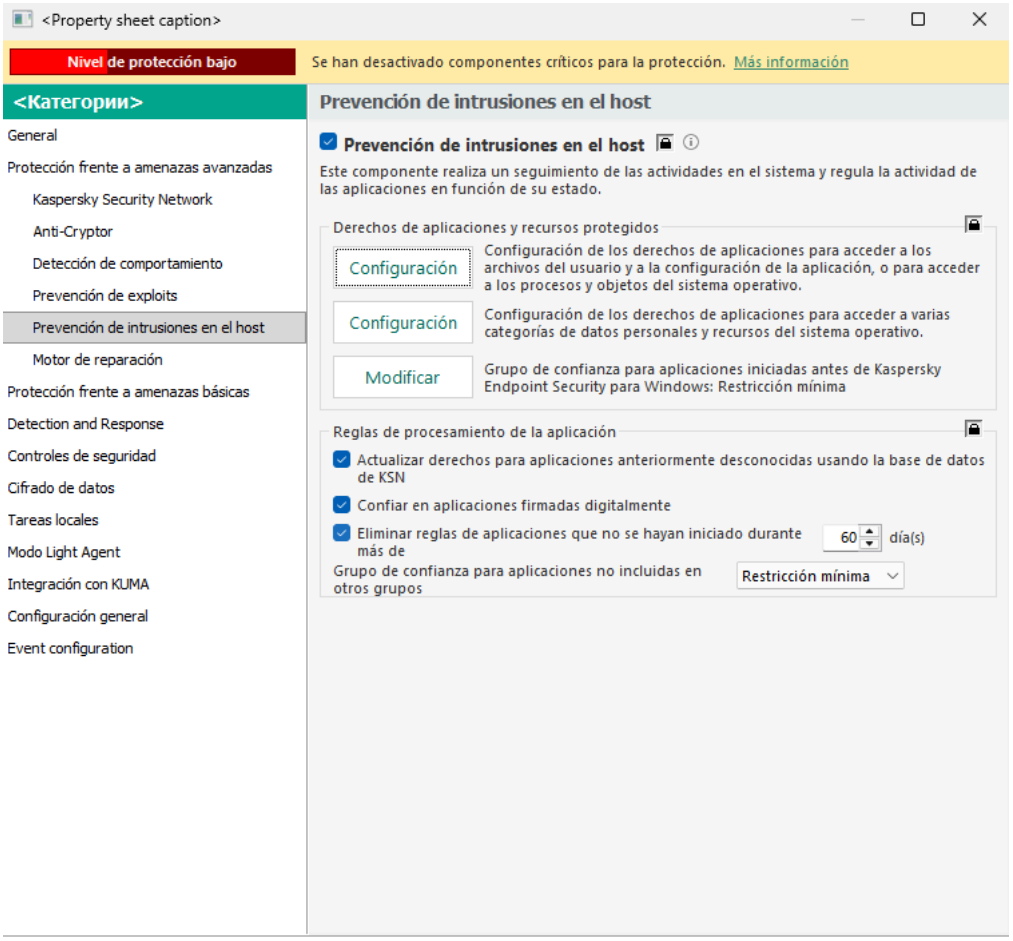
Selección de un grupo de confianza para aplicaciones desconocidas

Durante el primer inicio de una aplicación, el componente Prevención de intrusiones en el host determina el grupo de confianza para la aplicación. Si no tiene acceso a Internet o si Kaspersky Security Network no tiene información sobre esta aplicación, Kaspersky Endpoint Security colocará la aplicación en el grupo *Restricción mínima* de manera predeterminada. Cuando se detecta información sobre una aplicación previamente desconocida en KSN, Kaspersky Endpoint Security actualizará los derechos de esta aplicación. Luego, los derechos de la aplicación pueden modificarse manualmente.

Cómo seleccionar un grupo de confianza para aplicaciones desconocidas en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Reglas de procesamiento de la aplicación**, use la lista desplegable **Grupo de confianza para aplicaciones no incluidas en otros grupos** para seleccionar el grupo de confianza necesario.

   Si se activa la participación en Kaspersky Security Network, Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta recibida, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración del componente Prevención de intrusiones en el host.

5. Utilice la casilla de verificación **Actualizar derechos para aplicaciones anteriormente desconocidas usando la base de datos de KSN** para configurar la actualización automática de los derechos de aplicaciones desconocidas.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar un grupo de confianza para aplicaciones desconocidas en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host → Prevención de intrusiones en el host**.

5. En el bloque **Reglas de procesamiento de la aplicación**, use la lista desplegable **Grupo de confianza para aplicaciones no incluidas en otros grupos** para seleccionar el grupo de confianza necesario.

   Si se activa la participación en Kaspersky Security Network, Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta recibida, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración del componente Prevención de intrusiones en el host.

6. Utilice la casilla de verificación **Actualizar derechos para aplicaciones anteriormente desconocidas usando la base de datos de KSN** para configurar la actualización automática de los derechos de aplicaciones desconocidas.

7. Guarde los cambios.

Cómo seleccionar un grupo de confianza para aplicaciones desconocidas en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.

3. En el bloque **Reglas de procesamiento de la aplicación**, seleccione el grupo de confianza necesario.

   Si se activa la participación en Kaspersky Security Network, Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta recibida, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración del componente Prevención de intrusiones en el host.

4. Utilice la casilla de verificación **Actualizar reglas de aplicaciones anteriormente desconocidas desde KSN** para configurar la actualización automática de los derechos de aplicaciones desconocidas.

5. Guarde los cambios.

Seleccionar un grupo de confianza para aplicaciones firmadas digitalmente

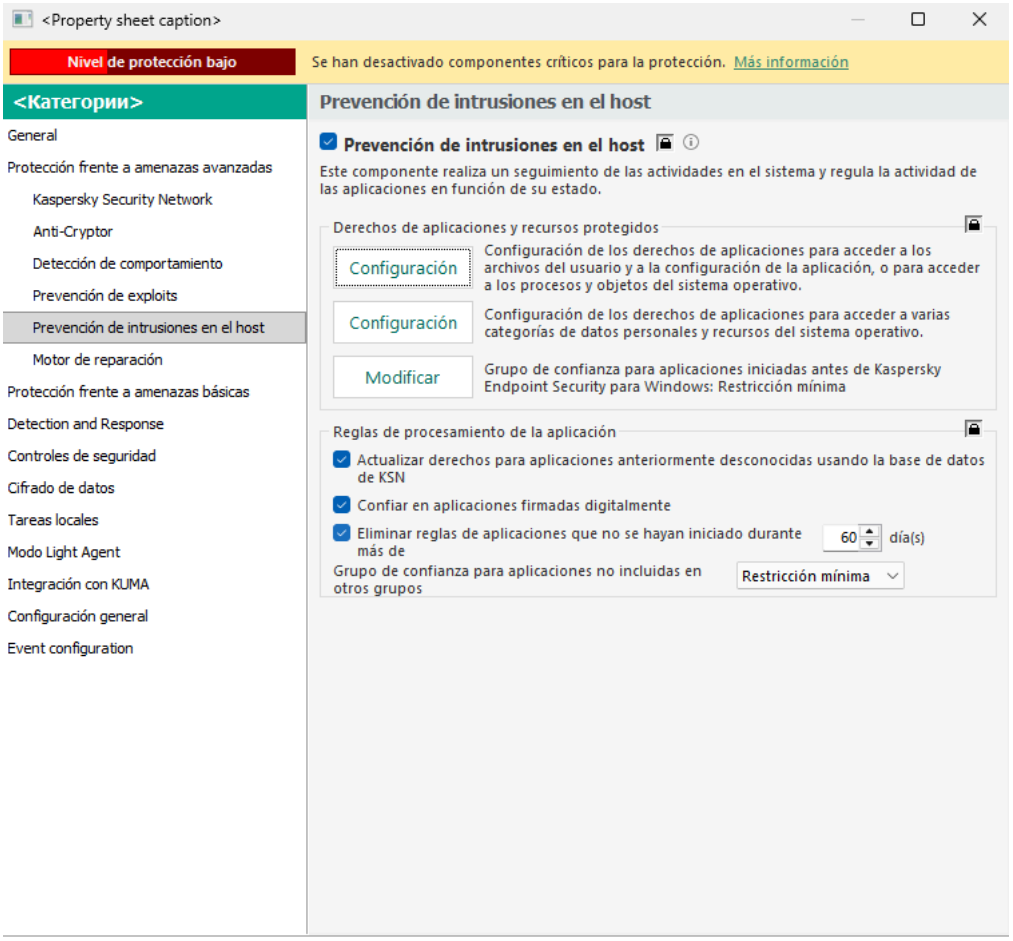
Kaspersky Endpoint Security siempre coloca las aplicaciones firmadas por certificados de Microsoft o certificados de Kaspersky en el grupo *De confianza*.

Cómo seleccionar un grupo de confianza para aplicaciones firmadas digitalmente en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Reglas de procesamiento de la aplicación**, use la casilla de verificación **Confiar en aplicaciones firmadas digitalmente** para activar o desactivar la asignación automática al grupo de confianza De confianza para las aplicaciones que contienen la firma digital de los proveedores de confianza.

   Los proveedores de confianza son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual.

   Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera de confianza las aplicaciones con firma digital y utiliza otros parámetros para determinar su grupo de confianza.

5. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar un grupo de confianza para aplicaciones firmadas digitalmente en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host → Prevención de intrusiones en el host**.

5. En el bloque **Reglas de procesamiento de la aplicación**, use la casilla de verificación **Confiar en aplicaciones firmadas digitalmente** para activar o desactivar la asignación automática al grupo de confianza De confianza para las aplicaciones que contienen la firma digital de los proveedores de confianza.

Los proveedores de confianza son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual.

Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera de confianza las aplicaciones con firma digital y utiliza otros parámetros para determinar su grupo de confianza.

6. Guarde los cambios.

Cómo seleccionar un grupo de confianza para aplicaciones firmadas digitalmente en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.

3. En el bloque **Reglas de procesamiento de la aplicación**, use la casilla de verificación **Confiar en aplicaciones firmadas digitalmente** para activar o desactivar la asignación automática al grupo de confianza De confianza para las aplicaciones que contienen la firma digital de los proveedores de confianza.

   Los proveedores de confianza son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual.

   Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera de confianza las aplicaciones con firma digital y utiliza otros parámetros para determinar su grupo de confianza.

4. Guarde los cambios.

Administración de los derechos de las aplicaciones

De manera predeterminada, la actividad de la aplicación se controla en función de los derechos de la aplicación que se definen para el grupo de confianza específico que Kaspersky Endpoint Security asignó a la aplicación cuando se inició por primera vez. Si es necesario, puede modificar los derechos de la aplicación para un grupo de confianza completo, para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza.

Los derechos de la aplicación definidos manualmente tienen una prioridad más alta que los derechos de la aplicación definidos para un grupo de confianza. En otras palabras, si los derechos de aplicaciones definidos manualmente difieren de los derechos de aplicaciones definidos para un grupo de confianza, el componente Prevención de intrusiones en el host controla la actividad de la aplicación de acuerdo con los derechos de aplicaciones definidos en forma manual.

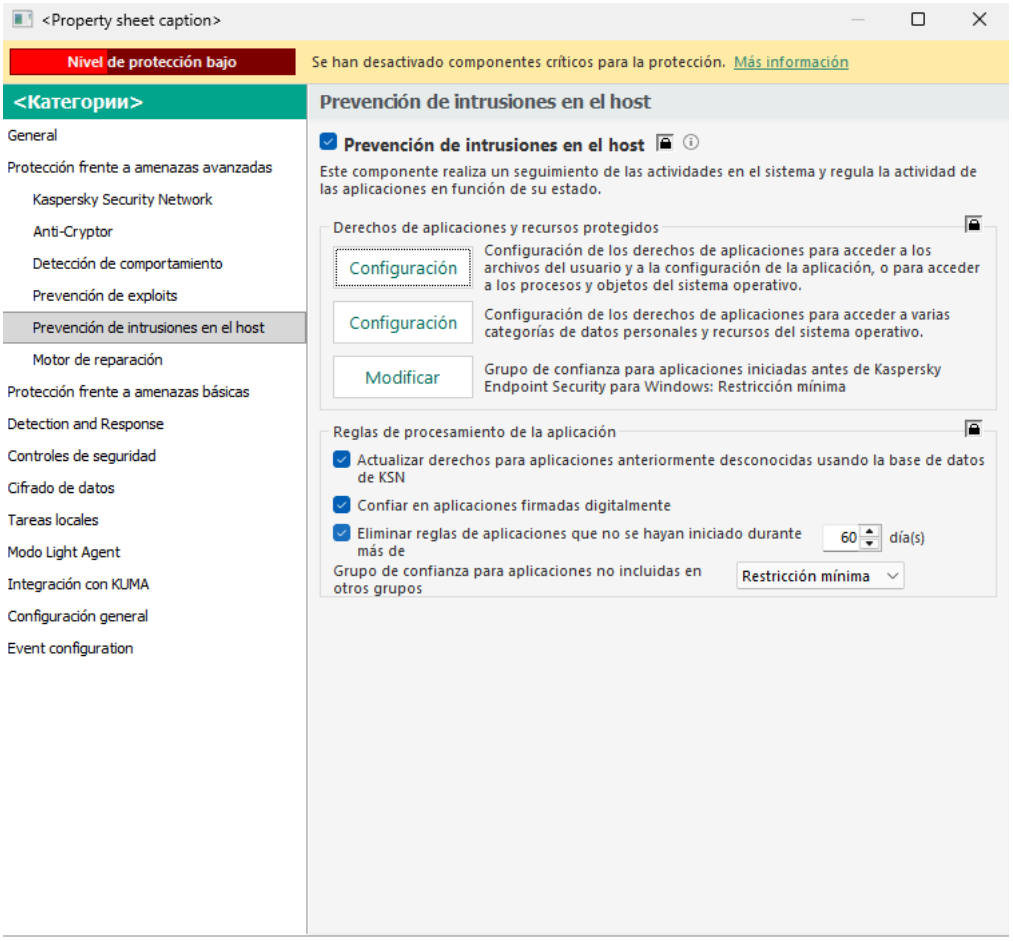
Las aplicaciones secundarias heredan las reglas que usted crea para las aplicaciones. Por ejemplo, si impide toda la actividad de red de cmd.exe, también se impedirá toda la actividad de red para notepad.exe si se inicia mediante cmd.exe. Cuando una aplicación no es secundaria de la aplicación de la que se ejecuta, las reglas no se heredan.

Cómo cambiar los derechos de la aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

5. Vaya a la pestaña **Derechos de la aplicación**.

6. Haga clic en **Añadir**.

7. En la ventana abierta, introduzca los criterios para buscar la aplicación cuyos derechos de la aplicación desea cambiar.

   Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

8. Haga clic en **Actualizar**.

   Kaspersky Endpoint Security buscará la aplicación en la lista consolidada de aplicaciones instaladas en equipos administrados. Kaspersky Endpoint Security mostrará una lista de aplicaciones que coincidan con sus criterios de búsqueda.

9. Seleccione la aplicación pertinente.

10. En la lista desplegable **Añadir aplicación seleccionada al grupo de confianza**, seleccione **Grupos predeterminados** y haga clic en **Aceptar**.

    La aplicación se añadirá al grupo predeterminado.

11. Seleccione la aplicación correspondiente y luego seleccione **Derechos de la aplicación** en el menú contextual de la aplicación.

    Se abren las propiedades de la aplicación.

12. Realice una de las siguientes acciones:

    - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
    - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Permisos**.

    La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

13. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y elegir la opción necesaria: **Heredar**, **Permitir** (✓) o **Bloquear** (⊘).

14. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (✓/⊘).

    Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

15. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo cambiar los derechos de la aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

6. Vaya a la pestaña **Derechos de la aplicación**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.

7. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir una aplicación a un grupo de confianza.

8. Seleccione el grupo de confianza correspondiente para la aplicación.

9. Seleccione el tipo **Aplicación**. Ir al paso siguiente.

   Si desea cambiar el grupo de confianza para varias aplicaciones, seleccione el tipo **Grupo** y defina un nombre para el grupo de aplicaciones.

10. En la lista de aplicaciones abiertas, seleccione las aplicaciones cuyos derechos desea cambiar.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

11. Finalice el asistente.

    La aplicación se añadirá al grupo de confianza.

12. En la parte izquierda de la ventana, seleccione la aplicación relevante.

13. En la parte derecha de la ventana, en la lista desplegable, lleve a cabo una de las siguientes acciones:

    - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
    - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Permisos**.

    La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

14. Para el recurso relevante, en la columna de la acción correspondiente, seleccione la opción necesaria: **Heredar**, **Permitir** (), **Bloquear** ().

15. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (/).

    Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

16. Guarde los cambios.

Cómo cambiar los derechos de la aplicación en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.

3. Haga clic en **Administrar aplicaciones**.

   Esto abre la lista de aplicaciones instaladas.

4. Seleccione la aplicación pertinente.

5. En el menú contextual de la aplicación, seleccione **Detalles y reglas**.

   Se abren las propiedades de la aplicación.

6. Realice una de las siguientes acciones:

   - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.

   - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Permisos**.

7. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y elegir la opción necesaria: **Heredar**, **Permitir** () o **Rechazar** ().

8. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** ().

   Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

9. Seleccione la pestaña **Exclusiones** y establezca la configuración avanzada de la aplicación (consulte la tabla a continuación).

10. Guarde los cambios.

Configuración avanzada de la aplicación

Parámetro	Descripción
No analizar archivos abiertos por la aplicación	Todos los archivos abiertos por la aplicación quedan excluidos de los análisis de Kaspersky Endpoint Security. Por ejemplo, si utiliza aplicaciones para realizar copias de seguridad de archivos, esta función ayuda a reducir el consumo de recursos de Kaspersky Endpoint Security.
No supervisar la actividad de la aplicación	Kaspersky Endpoint Security no supervisará la actividad de red y archivos de la aplicación en el sistema operativo. Puede configurar la supervisión de la actividad de la aplicación en diferentes componentes de Kaspersky Endpoint Security: • **No supervisar para los componentes de protección y control**. La actividad de la aplicación se supervisa a través de los siguientes componentes: Detección de comportamiento, Prevención de exploits, Prevención de intrusiones en el host, Motor de reparación y Firewall. • **No supervisar para Managed Detection and Response ni Endpoint Detection and Response**. La actividad de la aplicación es supervisada por el agente MDR integrado y el agente EDR integrado (KATA). • **No interceptar la entrada interactiva en la consola para Endpoint Detection and Response**. Kaspersky Endpoint Security no envía datos de telemetría sobre la administración de la aplicación en la consola. Kaspersky Anti Targeted Attack Platform (EDR) utiliza los datos de telemetría.
No heredar restricciones del proceso principal (aplicación)	Kaspersky Endpoint Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal se inicia a través de una aplicación para la que se configuran los derechos de aplicación (Prevención de intrusiones en el host) y las reglas de red de la aplicación (Firewall).
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Endpoint Security no supervisará la actividad de archivos ni redes de las aplicaciones iniciadas por esta aplicación. Puede aplicar la exclusión de forma recursiva. De este modo, la aplicación no supervisa la actividad de toda la cadena de aplicaciones secundarias.
Permitir interacción con la interfaz de Kaspersky Endpoint Security	Autoprotección de Kaspersky Endpoint Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona la casilla de verificación, la aplicación de acceso remoto tiene autorización para administrar la configuración de Kaspersky Endpoint Security mediante la interfaz de Kaspersky Endpoint Security.
No analizar el tráfico cifrado/No analizar todo el tráfico	El tráfico de red iniciado por la aplicación se excluirá de los análisis de Kaspersky Endpoint Security. Puede excluir todo el tráfico o solo el tráfico cifrado de los análisis. También puede excluir direcciones IP individuales y números de puerto de los análisis. Kaspersky Endpoint Security versión 14.0 o anterior no admite la exclusión del tráfico de red si se especifica un hash para una aplicación de confianza en lugar de una ruta.

Protección de recursos del sistema operativo y de datos personales

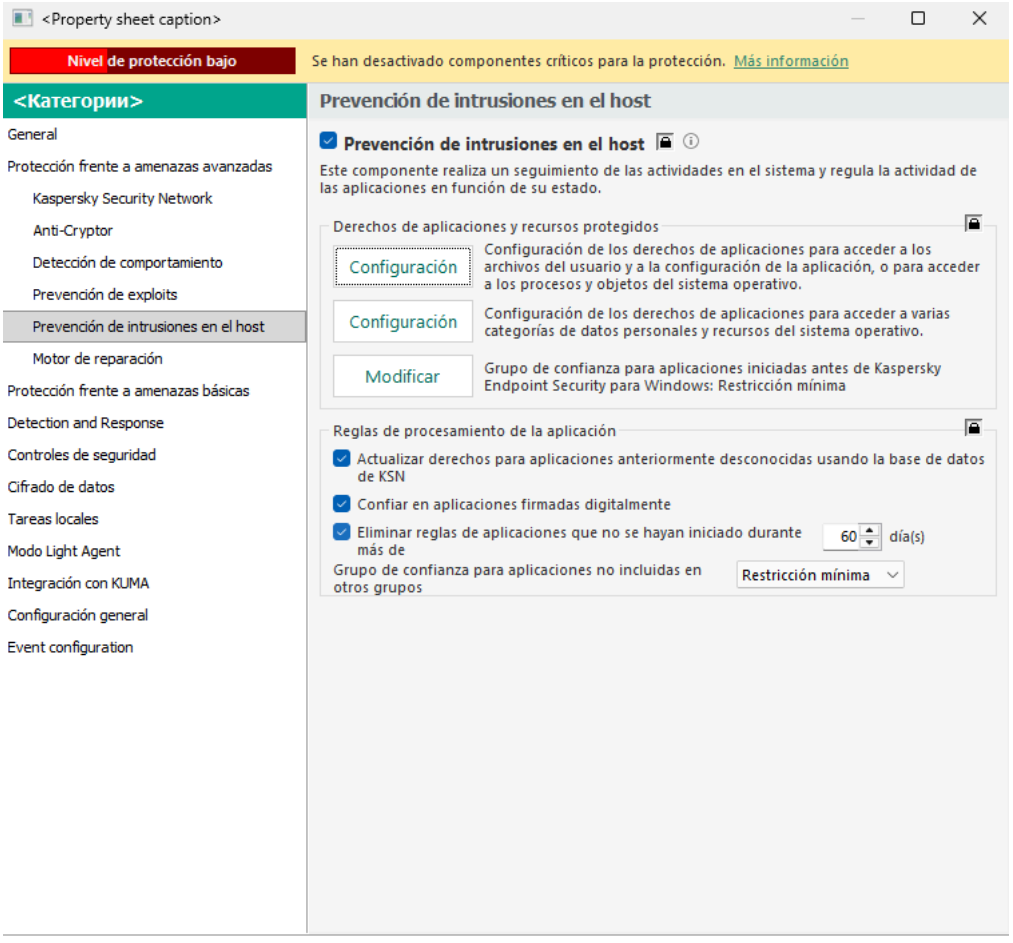
El componente Prevención de intrusiones en el host administra los derechos de las aplicaciones de realizar acciones en varias categorías de los recursos del sistema operativo y datos personales. Los especialistas de Kaspersky han creado categorías predefinidas de recursos protegidos. Por ejemplo, la categoría *Sistema operativo* tiene una subcategoría *Configuración del inicio* que enumera todas las claves de registro asociadas con la ejecución automática de aplicaciones. No puede editar ni eliminar las categorías predefinidas de recursos protegidos, ni los recursos protegidos que hay dentro de esas categorías.

Cómo añadir o un recurso protegido en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

5. Vaya a la pestaña **Recursos protegidos**.

   Verá una lista de recursos protegidos en la parte izquierda de la ventana y los derechos correspondientes para acceder a esos recursos según el grupo de confianza específico.

6. Seleccione la categoría de recursos protegidos a los que desea añadir un nuevo recurso protegido.

   Si desea añadir una subcategoría, haga clic en **Añadir** → **Categoría**.

7. Haga clic en el botón **Añadir**. En la lista desplegable, seleccione el tipo de recurso que desee añadir: **Archivo o carpeta** o **Clave de registro**.

8. En la ventana que se abre, seleccione un archivo, carpeta o clave de registro.

   Puede ver los derechos de las aplicaciones para acceder a los recursos añadidos. Para hacerlo, seleccione un recurso añadido en la parte izquierda de la ventana y Kaspersky Endpoint Security mostrará los derechos de acceso para cada grupo de confianza. También puede desactivar el control de la actividad de la aplicación con recursos utilizando la casilla de verificación junto a un nuevo recurso.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir un recurso protegido en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host** → **Prevención de intrusiones en el host**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

6. Vaya a la pestaña **Recursos protegidos**.

   Verá una lista de recursos protegidos en la parte izquierda de la ventana y los derechos correspondientes para acceder a esos recursos según el grupo de confianza específico.

7. Haga clic en **Añadir**.

   Se abre el Asistente de recurso nuevo.

8. En el bloque **Nombre del grupo**, seleccione la categoría de recursos protegidos a la que desea añadir un recurso protegido nuevo.

   Si desea añadir una subcategoría, seleccione la opción **Categoría de recursos protegidos**.

9. Seleccione el tipo de recurso que desea añadir: **Archivo o carpeta** o **Clave de registro**.

10. Seleccione un archivo, carpeta o clave de registro.

11. Finalice el asistente.

    Puede ver los derechos de las aplicaciones para acceder a los recursos añadidos. Para hacerlo, seleccione un recurso añadido en la parte izquierda de la ventana y Kaspersky Endpoint Security mostrará los derechos de acceso para cada grupo de confianza. También puede usar la casilla de verificación en la columna **Estado** para desactivar el control de la actividad de la aplicación con recursos.

12. Guarde los cambios.

Cómo añadir un recurso protegido en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Haga clic en **Administrar recursos**.

   Se abre la lista de Recursos protegidos.
4. Seleccione la categoría de recursos protegidos a los que desea añadir un nuevo recurso protegido.

   Si desea añadir una subcategoría, haga clic en **Añadir** → **Categoría**.
5. Haga clic en el botón **Añadir**. En la lista desplegable, seleccione el tipo de recurso que desee añadir: **Archivo o carpeta** o **Clave de registro**.
6. En la ventana que se abre, seleccione un archivo, carpeta o clave de registro.

   Puede ver los derechos de las aplicaciones para acceder a los recursos añadidos. Para hacerlo, seleccione un recurso añadido en la parte izquierda de la ventana y Kaspersky Endpoint Security mostrará una lista de aplicaciones y los derechos de acceso para cada aplicación. También puede desactivar el control de la actividad de la aplicación con recursos con el botón **Habilitar control** en la columna **Estado**.
7. Guarde los cambios.

Kaspersky Endpoint Security controlará el acceso a los recursos añadidos del sistema operativo y a los datos personales. Kaspersky Endpoint Security controla el acceso de una aplicación a los recursos según el grupo de confianza asignado a la aplicación. Además, puede cambiar el grupo de confianza de una aplicación.

Eliminación de información sobre aplicaciones sin uso

Kaspersky Endpoint Security emplea los derechos de las aplicaciones para controlar las actividades de las aplicaciones. Los derechos de las aplicaciones se determinan según su grupo de confianza. Kaspersky Endpoint Security incluye una aplicación en un grupo de confianza cuando la aplicación se inicia por primera vez. Puede cambiar manualmente el grupo de confianza de una aplicación. También puede configurar manualmente los derechos de una aplicación en particular. Kaspersky Endpoint Security almacena la siguiente información sobre una aplicación: grupo de confianza de la aplicación y derechos de la aplicación.

Kaspersky Endpoint Security elimina automáticamente la información sobre las aplicaciones sin uso para ahorrar recursos informáticos. Kaspersky Endpoint Security elimina la información de las aplicaciones siguiendo las reglas siguientes:

- Si el grupo de confianza y los derechos de una aplicación se han determinado automáticamente, Kaspersky Endpoint Security elimina la información sobre esta aplicación después de 30 días. No es posible cambiar el período de almacenamiento para la información de las aplicaciones ni desactivar la eliminación automática.
- Si coloca manualmente una aplicación en un grupo de confianza o configura sus derechos de acceso, Kaspersky Endpoint Security elimina la información sobre esta aplicación después de 60 días (período de almacenamiento predeterminado). Puede cambiar el período de almacenamiento para la información de las aplicaciones y desactivar la eliminación automática (consulte las instrucciones más abajo).

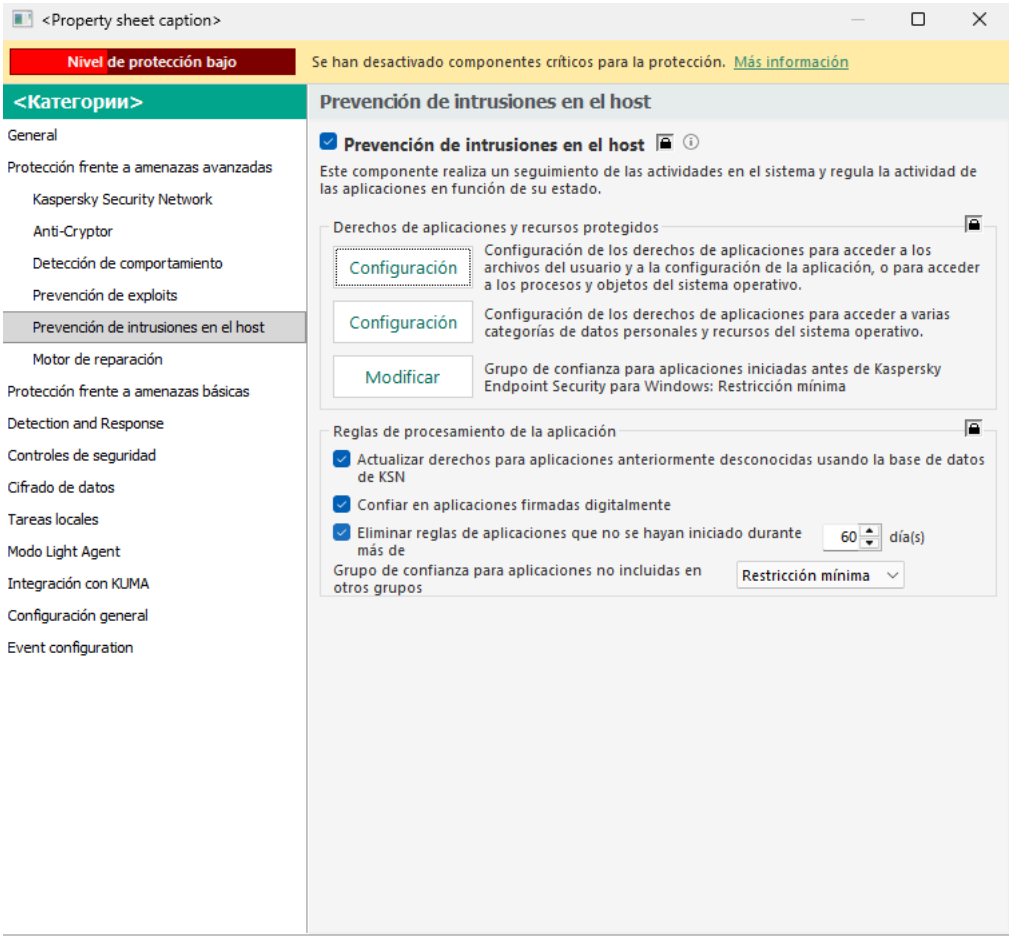
Cuando inicia una aplicación cuya información se ha eliminado, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

Cómo configurar la eliminación automática de información sobre aplicaciones no utilizadas en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Reglas de procesamiento de la aplicación**, lleve a cabo una de estas acciones:

   - Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N día(s)** e introduzca el número de días.

     Kaspersky Endpoint Security eliminará información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, después del número definido de días. Kaspersky Endpoint Security también eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.

   - Si desea desactivar la eliminación automática, desactive la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N día(s)**.

     Kaspersky Endpoint Security almacenará de forma indefinida información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, sin límites en el período de almacenamiento. Kaspersky Endpoint Security solo eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.

5. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar la eliminación automática de información sobre aplicaciones no utilizadas en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de la aplicación**, lleve a cabo una de estas acciones:

   - Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas para aplicaciones que no se inician por más de (días, 1 a 90)** e introduzca el número de días.

     Kaspersky Endpoint Security eliminará información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, después del número definido de días. Kaspersky Endpoint Security también eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.

   - Si desea desactivar la eliminación automática, desactive la casilla de verificación **Eliminar reglas para aplicaciones que no se inician por más de (días, 1 a 90)**.

     Kaspersky Endpoint Security almacenará de forma indefinida información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, sin límites en el período de almacenamiento. Kaspersky Endpoint Security solo eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.
6. Guarde los cambios.

Cómo configurar la eliminación automática de información sobre aplicaciones no utilizadas en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. En el bloque **Reglas de procesamiento de la aplicación**, lleve a cabo una de estas acciones:

   - Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días (de 1 a 90)** e introduzca el número de días.

     Kaspersky Endpoint Security eliminará información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, después del número definido de días. Kaspersky Endpoint Security también eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.

- Si desea desactivar la eliminación automática, desactive la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días (de 1 a 90)**.

  Kaspersky Endpoint Security almacenará de forma indefinida información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, sin límites en el período de almacenamiento. Kaspersky Endpoint Security solo eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.

4. Guarde los cambios.

Control de prevención de intrusiones en el host

Puede recibir informes sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

Para supervisar las operaciones de prevención de intrusiones en el host, debe activar la redacción de informes. Por ejemplo, puede activar el reenvío de informes para aplicaciones individuales en la configuración del componente Prevención de intrusiones en el host.

Al configurar la supervisión de prevención de intrusiones en el host, tenga en cuenta la carga potencial de la red al reenviar eventos a Kaspersky Security Center. También puede activar el guardado de informes solo en el registro local de Kaspersky Endpoint Security.

Protección del acceso a audio y vídeo

La función de protección de la señal de audio y la de protección del acceso a la cámara web no son compatibles con equipos basados en Arm.

Los ciberdelincuentes pueden usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web). Kaspersky Endpoint Security controla cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada.

De forma predeterminada, Kaspersky Endpoint Security permite recibir transmisiones de audio y vídeo solo para aplicaciones desde el grupo *De confianza*. Las aplicaciones de los grupos *Restricción mínima*, *Restricción máxima* y *No fiable* no pueden recibir la transmisión de audio y la transmisión de vídeo de los dispositivos. De forma manual, puede permitir que las aplicaciones reciban transmisión de audio y vídeo.

Características especiales de la protección de transmisión de audio

La protección del flujo de audio tiene las siguientes características especiales:

- El componente Prevención de intrusiones en el host se debe activar para que esta funcionalidad esté activa.
- Si la aplicación empezó a recibir el flujo de audio antes de que se iniciara el componente Prevención de intrusiones en el host, Kaspersky Endpoint Security permite que la aplicación reciba el flujo de audio y no muestre ninguna notificación.
- Si movió la aplicación al grupo *No fiable* o al grupo *Restricción máxima* después de que la aplicación comenzase a recibir el flujo de audio, Kaspersky Endpoint Security permite que la aplicación reciba el flujo de audio y no muestra ninguna notificación.
- Después de modificar la configuración del acceso a la aplicación a dispositivos de grabación de sonido (por ejemplo, si se ha bloqueado la recepción del flujo de audio por parte de la aplicación), esta aplicación se debe reiniciar para que deje de recibir el flujo de audio.
- El control del acceso a las secuencias de audio de los dispositivos de registro de sonidos no depende de la configuración de acceso a la cámara web de una aplicación.
- Kaspersky Endpoint Security protege el acceso únicamente los micrófonos integrados y micrófonos externos. El resto de los dispositivos de flujo de audio no son compatibles.
- Kaspersky Endpoint Security no puede garantizar la protección de un flujo de audio desde dispositivos como cámaras DSLR, videocámaras portátiles y cámaras de acción.
- Cuando ejecuta la grabación de vídeo y audio o aplicaciones de reproducción por primera vez desde la instalación de Kaspersky Endpoint Security, puede que se interrumpa la reproducción o grabación de vídeo y audio. Esto es necesario a fin de activar la funcionalidad que controla el acceso a los dispositivos de grabación de sonido por aplicaciones. El servicio del sistema que controla el hardware de audio se reiniciará cuando Kaspersky Endpoint Security se ejecute por primera vez.

Características especiales de la protección de acceso a la cámara web de la aplicación

La funcionalidad de protección del acceso a la cámara web tiene las siguientes consideraciones especiales y limitaciones:

- La aplicación controla el vídeo y las imágenes estáticas derivados del procesamiento de los datos de la cámara web.
- La aplicación controla el flujo de audio si este forma parte del flujo de vídeo recibido a través de la cámara web.
- La aplicación controla solo las cámaras web conectadas mediante USB o IEEE1394 que se muestran como Dispositivos de imagen en el Administrador del dispositivos de Windows.
- Kaspersky Endpoint Security admite las siguientes cámaras web:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310

- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky no puede garantizar la compatibilidad con las cámaras web que no se especifican en esta lista.

Prevención de ataques de BadUSB

Algunos virus modifican el firmware de los dispositivos USB para engañar al sistema operativo y que detecte el dispositivo USB y lo identifique como teclado. Como resultado, el virus puede ejecutar comandos en su cuenta de usuario para descargar software malicioso, por ejemplo.

El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.

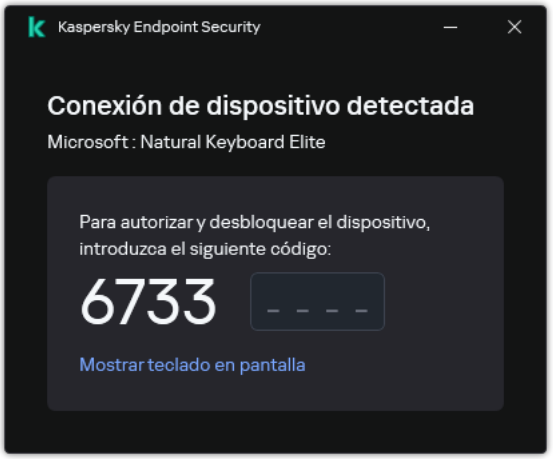
Cuando un dispositivo USB se conecta al equipo y el sistema operativo lo identifica como un teclado, la aplicación solicita al usuario que introduzca desde este teclado un código numérico generado por la aplicación, o bien que utilice el teclado en pantalla si está disponible (vea la figura a continuación). Este procedimiento se conoce como autorización del teclado.

Si el código se ha introducido correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al que se ha conectado) en la lista de teclados autorizados. No será necesario volver a realizar la autorización del teclado cuando se vuelva a conectar el teclado o después de que se reinicie el sistema operativo.

Cuando el teclado autorizado está conectado a un puerto USB diferente del equipo, la aplicación muestra un mensaje para la autorización de este teclado.

Si se introduce el código numérico de forma incorrecta, la aplicación generará un nuevo código. Puede configurar el número de intentos para introducir el código numérico. Si el código numérico se introduce de forma incorrecta muchas veces o si se cierra la ventana de autorización del teclado (ver la figura a continuación), la aplicación bloquea las acciones de ese teclado. Cuando se cumple el período de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación solicita al usuario que realice de nuevo el procedimiento de autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea los teclados que no se hayan autorizado.



Autorización del teclado

Activación y desactivación de Prevención de ataques de BadUSB

Los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente Prevención de ataques de BadUSB se considerarán autorizados después de la instalación del componente.

Cómo activar o desactivar el componente Prevención de ataques de BadUSB en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Prevención de ataques de BadUSB**.
4. Utilice la casilla de verificación **Prevención de ataques de BadUSB** para activar o desactivar el componente.
5. En el bloque **Autorización del dispositivo USB al conectar**, ajuste la configuración de seguridad para introducir el código de autorización:
   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para introducir el código de autorización, la aplicación bloquea el dispositivo USB tras el quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este período, volverá a disponer de cinco intentos para introducir el código de autorización.
   - **Tiempo de espera al alcanzar el número máximo de intentos (minutos)**. Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos de introducir el código de autorización. Los valores válidos son de 1 a 180 (minutos).
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el componente Prevención de ataques de BadUSB en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Prevención de ataques de BadUSB**.
5. Utilice interruptor **Prevención de ataques de BadUSB ACTIVADA** para activar o desactivar el componente.
6. En el bloque **Autorización de dispositivos USB**, ajuste la configuración de seguridad para introducir el código de autorización:

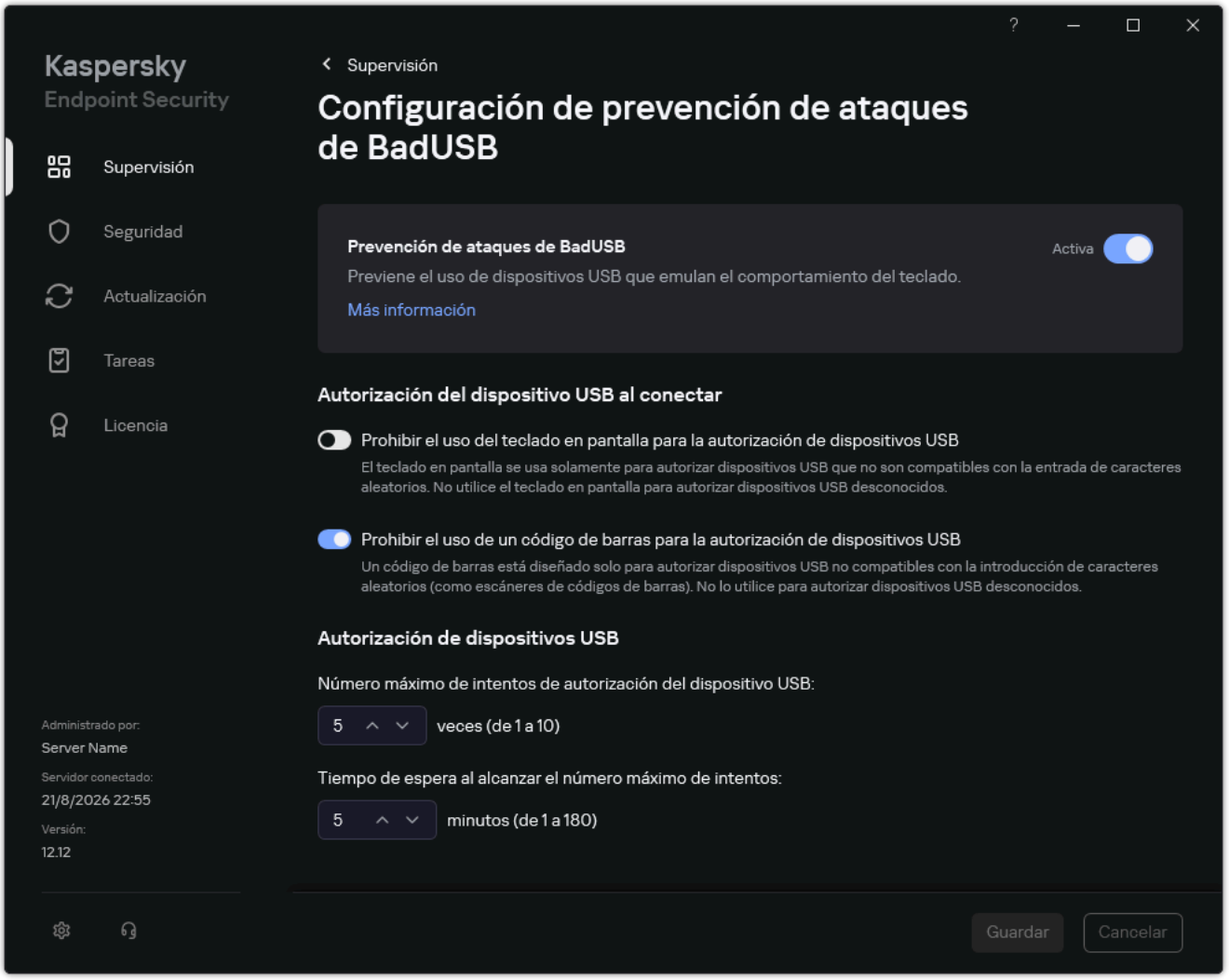
   - **Número máximo de intentos de autorización de dispositivos USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para introducir el código de autorización, la aplicación bloquea el dispositivo USB tras el quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este período, volverá a disponer de cinco intentos para introducir el código de autorización.

   - **Tiempo de espera cuando se alcanza la cantidad máxima de intentos (min)**. Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos de introducir el código de autorización. Los valores válidos son de 1 a 180 (minutos).
7. Guarde los cambios.

Cómo activar o desactivar el componente Prevención de ataques de BadUSB en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Prevención de ataques de BadUSB**.



Configuración del componente Prevención de ataques de BadUSB

3. Utilice interruptor **Prevención de ataques de BadUSB** para activar o desactivar el componente.

4. En el bloque **Autorización del dispositivo USB al conectar**, ajuste la configuración de seguridad para introducir el código de autorización:

   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para introducir el código de autorización, la aplicación bloquea el dispositivo USB tras el quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este período, volverá a disponer de cinco intentos para introducir el código de autorización.

   - **Tiempo de espera al alcanzar el número máximo de intentos**. Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos de introducir el código de autorización. Los valores válidos son de 1 a 180 (minutos).

5. Guarde los cambios.

Como resultado, si Prevención de ataques de BadUSB está activado, Kaspersky Endpoint Security requiere la autorización de un dispositivo USB conectado identificado como un teclado por el sistema operativo. El usuario no podrá usar un teclado no autorizado hasta que se autorice.

Usar el teclado en pantalla para la autorización de dispositivos USB

El teclado en pantalla solo se debe utilizar para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (como escáneres de códigos de barras). No se recomienda usar el teclado en pantalla para la autorización de dispositivos USB desconocidos.

Cómo permitir o prohibir el uso del teclado en pantalla para la autorización en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Prevención de ataques de BadUSB**.
4. Utilice la casilla de verificación **Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB** a fin de permitir o bloquear el uso del teclado en pantalla para la autorización.
5. Guarde los cambios.

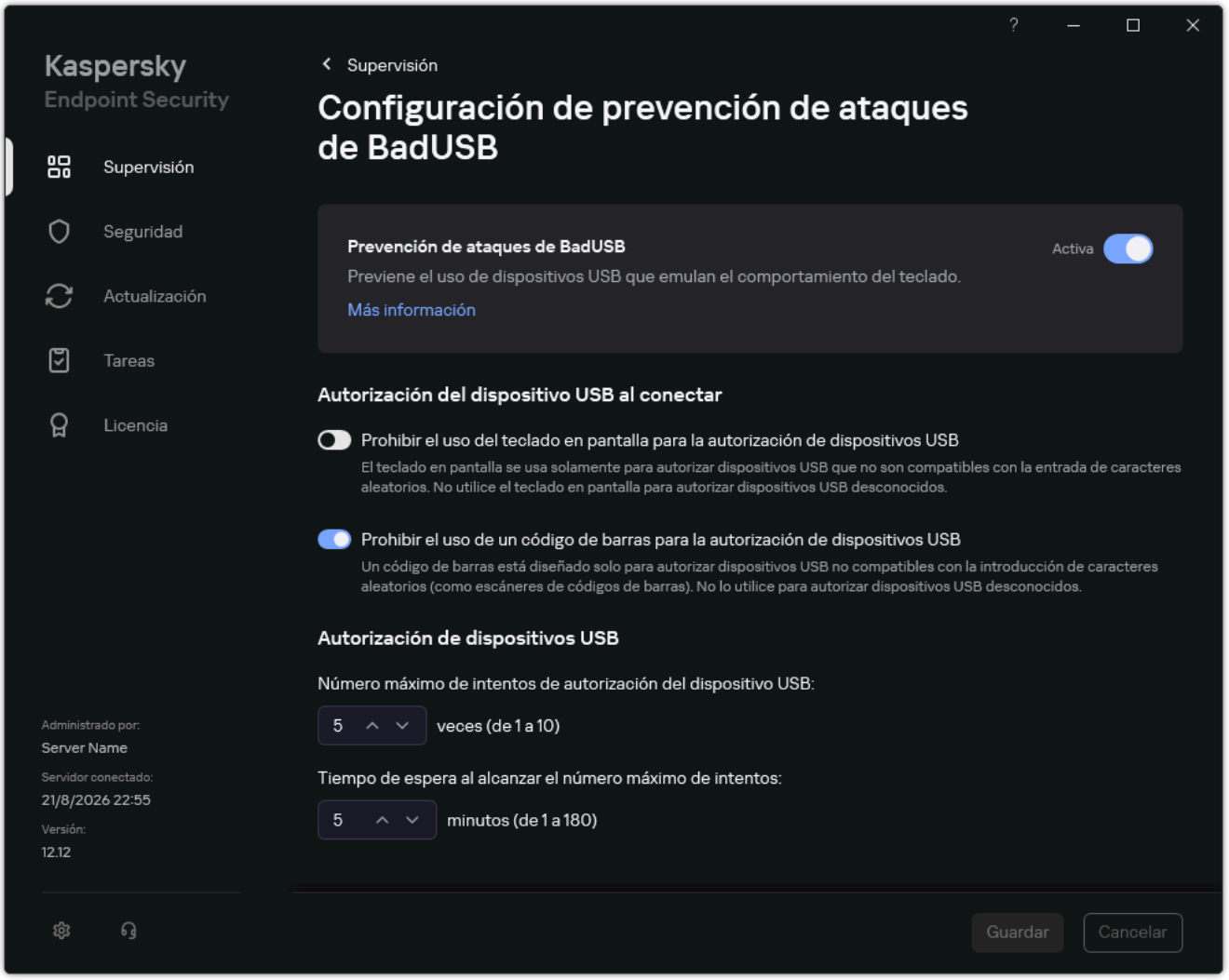
Cómo permitir o prohibir el uso del teclado en pantalla para la autorización en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Prevención de ataques de BadUSB**.
5. Utilice la casilla de verificación **Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB** para alternar o bloquear el uso del teclado en pantalla para la autorización.
6. Guarde los cambios.

Cómo permitir o prohibir el uso del teclado en pantalla para la autorización en la interfaz de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Prevención de ataques de BadUSB**.



Configuración del componente Prevención de ataques de BadUSB

3. Utilice la casilla de verificación **Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB** para alternar o bloquear el uso del teclado en pantalla para la autorización.

4. Guarde los cambios.



Autorización de dispositivos USB

Autorización de escáneres de códigos de barras

Al conectar un escáner de código de barras al equipo, el componente de prevención de ataques BadUSB identifica este dispositivo como un dispositivo de entrada y le solicita que realice la autorización. Para autorizar el escáner de códigos de barras, debe escanear un código de barras que aparece en la pantalla. La aplicación genera un código de barras en el formato Code39 compatible con la mayoría de los escáneres de códigos de barras y QR.

Kaspersky Endpoint Security también admite otro método de autorización de escáneres de códigos de barras. Si está utilizando dispositivos con pantalla táctil, puede utilizar un teclado en pantalla para escribir un código. Para hacerlo, necesita permitir el teclado en pantalla. Este método es cómodo, por ejemplo, en el caso de escáneres de códigos de barras estáticos integrados en cajas registradoras. Se prohíben otros métodos de autorización de escáneres de códigos de barras.

De forma predeterminada, la aplicación no utiliza un código de barras para la autorización de dispositivos USB.

Cómo activar la autorización de dispositivos USB por código de barras en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione **Directivas**.

3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Prevención de ataques de BadUSB**.

5. Utilice la casilla de verificación **Prohibir el uso de un código de barras para la autorización de dispositivos USB** a fin de permitir o bloquear el uso de los códigos de barras para la autorización.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar la autorización de dispositivos USB en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección frente a amenazas del host** → **Prevención de ataques de BadUSB**.

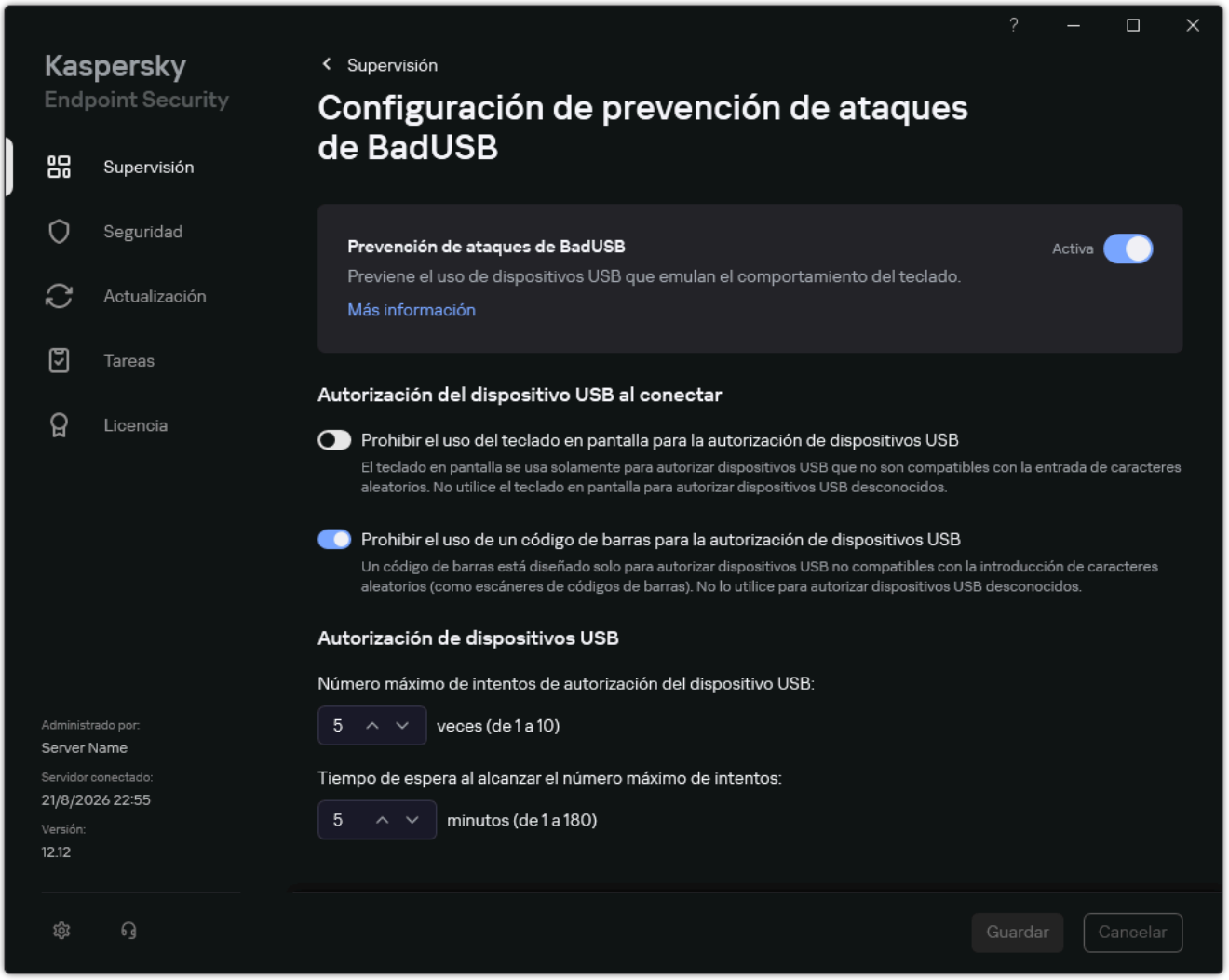
5. Utilice la casilla de verificación **Prohibir el uso de un código de barras para la autorización de dispositivos USB** para alternar, bloquear o permitir el uso de códigos de barras para la autorización.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo habilitar la autorización de dispositivos USB por código de barras en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Prevención de ataques de BadUSB**.



Configuración del componente Prevención de ataques de BadUSB

3. Utilice la casilla de verificación **Prohibir el uso de un código de barras para la autorización de dispositivos USB** para alternar, bloquear o permitir el uso de códigos de barras para la autorización.

4. Guarde los cambios.

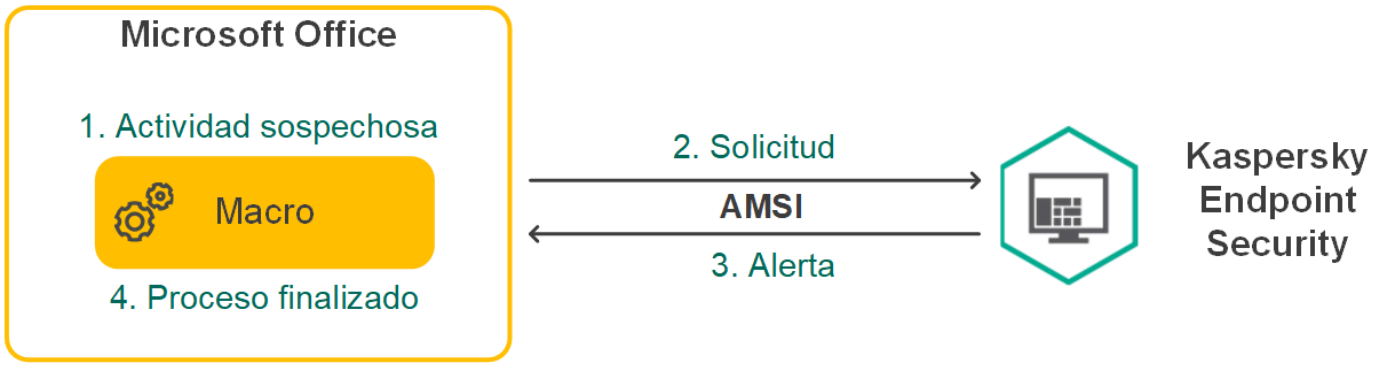


Autorización de escáneres de códigos de barras

Protección AMSI

El componente Protección AMSI está diseñado para admitir la Interfaz de análisis antimalware de Microsoft. La *interfaz de análisis antimalware (AMSI)* permite que las aplicaciones de terceros con soporte de la AMSI envíen a Kaspersky Endpoint Security aquellos objetos para los cuales precisan un análisis adicional (por ejemplo, scripts de PowerShell). Una vez que el análisis se completa, el resultado se devuelve a la aplicación que originó la solicitud. El concepto de "aplicaciones de terceros" incluye, por ejemplo, las aplicaciones de Microsoft Office (vea la imagen de más abajo). Para más detalles sobre AMSI, consulte la documentación de Microsoft.

La protección AMSI únicamente puede detectar una amenaza y notificar a una aplicación de terceros sobre dicha amenaza detectada. Una aplicación de terceros, después de recibir una notificación de una amenaza, no permite acciones maliciosas (por ejemplo, finaliza la acción).



Ejemplo del funcionamiento de AMSI

El componente de protección AMSI puede rechazar una solicitud de una aplicación de terceros si, por ejemplo, esta aplicación sobrepasa el número máximo de solicitudes dentro de un intervalo específico. Cuando esto ocurre, Kaspersky Endpoint Security envía información al respecto al Servidor de administración. El componente Protección AMSI no rechaza las solicitudes de aquellas aplicaciones de terceros para las cuales la integración continua con el componente de protección AMSI está activada.

La protección AMSI está disponible para los siguientes sistemas operativos para estaciones de trabajo y servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión
- Windows Server 2016 Essentials / Standard / Datacenter (modo Server Core incluido)
- Windows Server 2019 Essentials / Standard / Datacenter (modo Server Core incluido)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (modo Server Core incluido)
- Windows Server 2025 Standard / Datacenter

Activación y desactivación de la protección AMSI

De forma predeterminada, la Protección AMSI está activada y funciona en el modo recomendado por Kaspersky (consulte la tabla que aparece más adelante).

Cómo activar o desactivar la Protección AMSI en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Escáner de AMSI**.
4. Utilice la casilla de verificación **Escáner de AMSI** para activar o desactivar el componente.
5. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar la Protección AMSI en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Protección AMSI**.
5. Utilice interruptor **Protección para AMSI ACTIVADA** para activar o desactivar el componente.
6. Guarde los cambios. Para aplicar la directiva en equipos, cierre los candados .

Cómo activar o desactivar la Protección AMSI en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección AMSI**.



Configuración de Protección AMSI

3. Utilice interruptor **Protección AMSI** para activar o desactivar el componente.
4. Guarde los cambios.

Configuración de la Protección AMSI recomendada por los expertos de Kaspersky

Parámetro	Valor	Descripción
Analizar archivos	**Inactiva**	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar paquetes de distribución	**Inactiva**	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos en formatos de Microsoft Office	**Activa**	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
No descomprimir archivos compuestos grandes	**Tamaño máximo de archivo 8 MB**	Si esta casilla de verificación está marcada, la aplicación no analiza archivos compuestos cuyo tamaño exceda el valor especificado. Si esta casilla de verificación no está marcada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.

Optimización del análisis de archivos mediante la protección AMSI

Puede optimizar el análisis de archivos: reduzca el tiempo de análisis y aumente la velocidad de funcionamiento de Kaspersky Endpoint Security. Puede seleccionar los archivos compuestos que deben analizarse: archivos, paquetes de distribución o archivos en formatos de Office. También puede limitar el tamaño de los archivos compuestos que se analizarán. El componente de protección AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

Una técnica común para ocultar virus u otro malware es incorporarlo en archivos compuestos, como archivos de almacenamiento. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

Cómo optimizar el análisis de archivos por protección AMSI en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Escáner de AMSI**.
4. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiera analizar: archivos de almacenamiento, paquete de distribución o archivos en formatos de Office.
5. En el bloque **Límite de tamaño**, lleve a cabo una de estas acciones:
   - Para que el componente de protección AMSI no descomprima archivos compuestos de gran tamaño, active la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**, y especifique el valor que considere apropiado. El componente de protección AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.
   - Para permitir que el componente de protección AMSI descomprima archivos compuestos de gran tamaño, desactive la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

   El componente de protección AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No descomprimir archivos compuestos de gran tamaño** está activada.
6. Guarde los cambios. Para aplicar la directiva en equipos, cierre los candados .

Cómo optimizar el análisis de archivos por protección AMSI en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Protección AMSI**.

5. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiera analizar: archivos de almacenamiento, paquete de distribución o archivos en formatos de Office.

6. En el bloque **Optimización de análisis**, lleve a cabo una de estas acciones:

   - Para que el componente de protección AMSI no descomprima archivos compuestos de gran tamaño, active la casilla de verificación **Límites de tamaño activados**, y especifique el valor que considere apropiado. El componente de protección AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

   - Para permitir que el componente de protección AMSI descomprima archivos compuestos de gran tamaño, desactive la casilla de verificación **Límites de tamaño activados**.

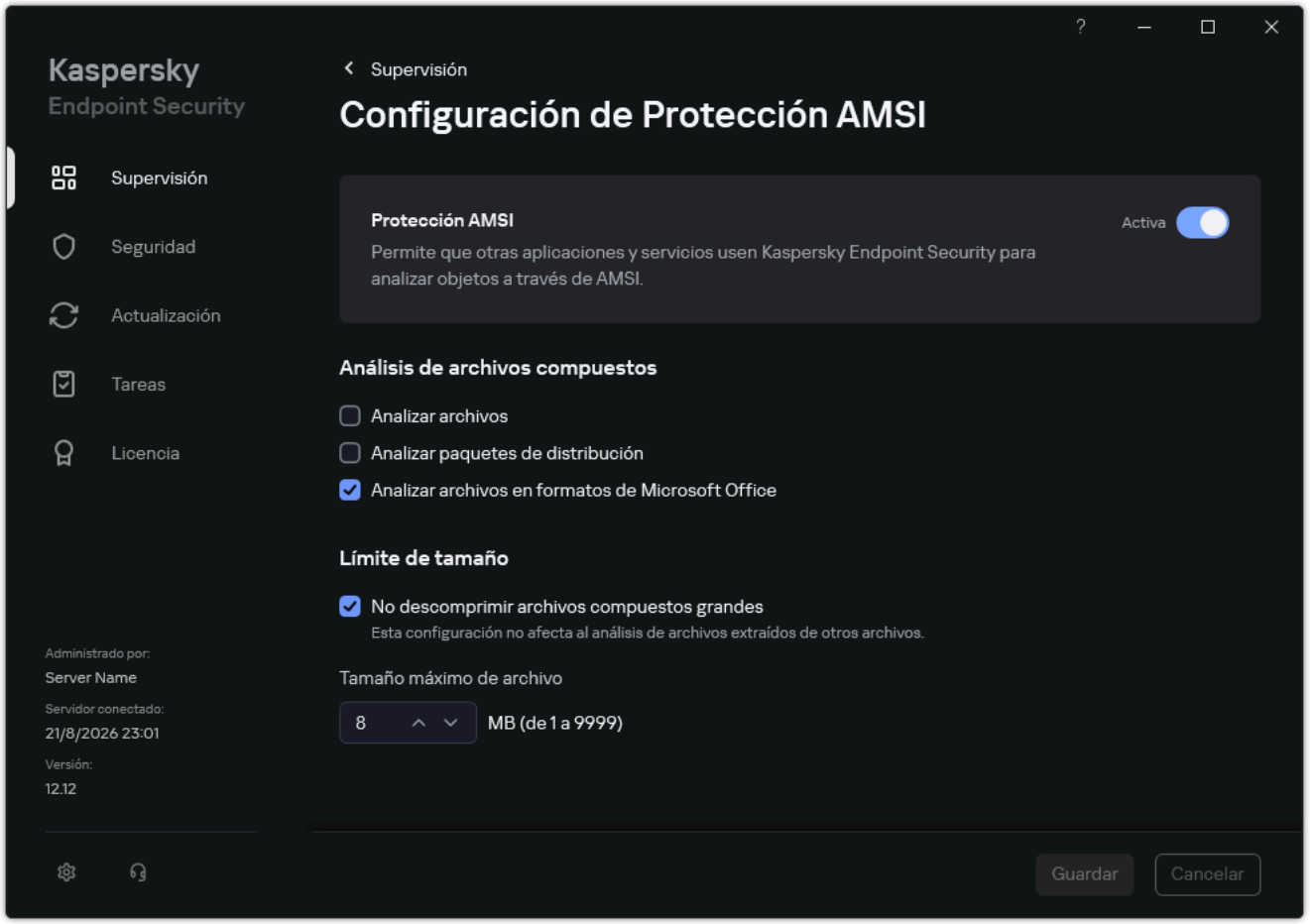
   El componente de protección AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **Límites de tamaño activados** está activada.

7. Guarde los cambios. Para aplicar la directiva en equipos, cierre los candados.

Cómo optimizar el análisis de archivos por protección AMSI en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección AMSI**.



Configuración de Protección AMSI

3. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiera analizar: archivos de almacenamiento, paquete de distribución o archivos en formatos de Office.

4. En el bloque **Límite de tamaño**, lleve a cabo una de estas acciones:

   - Para que el componente de protección AMSI no descomprima archivos compuestos de gran tamaño, active la casilla de verificación **No descomprimir archivos compuestos grandes**, y especifique el valor que considere apropiado. El componente de protección AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

   - Para permitir que el componente de protección AMSI descomprima archivos compuestos de gran tamaño, desactive la casilla de verificación **No descomprimir archivos compuestos grandes**.

   El componente de protección AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No descomprimir archivos compuestos grandes** está activada.

5. Guarde los cambios.

Protección frente a amenazas web

El componente Protección frente a amenazas web evita la descarga de archivos maliciosos de internet y también bloquea la conexión a sitios web maliciosos y de phishing. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

Kaspersky Endpoint Security analiza tráfico HTTP, HTTPS y FTP. Kaspersky Endpoint Security analiza direcciones IP y URLs.

Para utilizar Protección frente a amenazas web, debe completar la configuración inicial de la aplicación:

- Para la supervisión del tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitado de forma predeterminada).

- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación supervisa todos los puertos).

- Seleccione las aplicaciones cuyo tráfico desea que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya están presentes en la lista de aplicaciones recomendadas por Kaspersky. Si su navegador no aparece en la lista, agréguelo manualmente.

- Recomendamos inyectar un script de interacción de página web en el tráfico web (de forma predeterminada, la inyección de script está desactivada). Este script permite el registro de eventos de Protección frente a amenazas web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Cuando un usuario intenta abrir un sitio web malicioso o de phishing, Kaspersky Endpoint Security bloqueará el acceso y le mostrará una advertencia.

Activación y desactivación de Protección frente a amenazas web

De forma predeterminada, el componente Protección frente a amenazas web está activado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para la Protección frente a amenazas web, la aplicación puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que la configuración del nivel de seguridad para el tráfico web **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky (vea la tabla más abajo). Puede seleccionar uno de los niveles de seguridad preinstalados para el tráfico web que se recibe o se transmite a través de los protocolos HTTP y FTP, o configurar un nivel de seguridad del tráfico web personalizado. Si cambia la configuración del nivel de seguridad del tráfico web, siempre podrá volver a la configuración del nivel de seguridad recomendada del tráfico web.

Puede seleccionar o configurar el nivel de seguridad solo en la Consola de administración (MMC) o la interfaz local de la aplicación. No puede seleccionar ni configurar el nivel de seguridad en Web Console o Cloud Console.

Cómo activar o desactivar el componente Protección frente a amenazas web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
4. Utilice la casilla de verificación **Protección frente a amenazas web** para activar o desactivar el componente.
5. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:
   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
     - **Máximo**. El nivel de seguridad en el que componente Protección frente a amenazas web realiza el máximo análisis del tráfico web que el equipo recibe a través de HTTP y FTP. Protección frente a amenazas web analiza en detalle todos los objetos del tráfico web mediante todo el conjunto de bases de datos de la aplicación, y realiza el análisis heurístico más exhaustivo posible.
     - **Recomendado**. El nivel de seguridad que ofrece el equilibrio perfecto entre el rendimiento de la aplicación y la seguridad del tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.
     - **Mínimo**. La configuración de este nivel de seguridad de tráfico web garantiza el análisis más rápido de tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis superficial.
   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** y defina su propia configuración del componente (consulte la tabla siguiente).

     Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Predeterminado**.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos del tráfico web:

   - **Bloquear**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.

   - **Informar**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, Kaspersky Endpoint Security permite que este objeto se descargue en el equipo, pero añade información sobre el objeto a la lista de amenazas activas.

7. Guarde los cambios.

Cómo activar o desactivar el componente Protección frente a amenazas web en Web Console

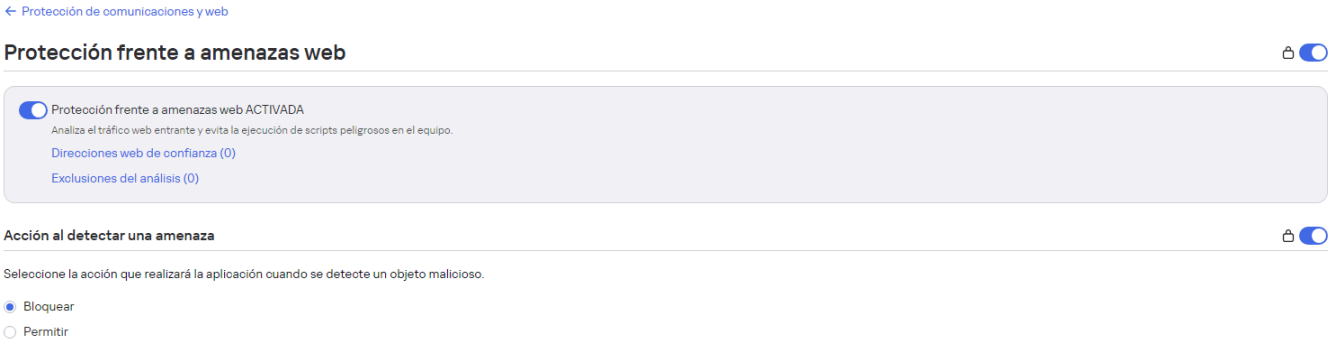
1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección de comunicaciones y web** → **Protección frente a amenazas web**.



Configuración de Protección frente a amenazas web

5. Utilice interruptor **Protección frente a amenazas web ACTIVADA** para activar o desactivar el componente.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos del tráfico web:

   - **Bloquear**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.

   - **Permitir, informar o solicitar una acción (depende del SO)**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, Kaspersky Endpoint Security permite que este objeto se descargue en el equipo, pero añade información sobre el objeto a la lista de amenazas activas.

7. De ser necesario, haga una lista de direcciones web de confianza.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el componente Protección frente a amenazas web

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
3. Utilice interruptor **Protección frente a amenazas web** para activar o desactivar el componente.
4. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:
   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
     - **Alto**. El nivel de seguridad en el que componente Protección frente a amenazas web realiza el máximo análisis del tráfico web que el equipo recibe a través de HTTP y FTP. Protección frente a amenazas web analiza en detalle todos los objetos del tráfico web mediante todo el conjunto de bases de datos de la aplicación, y realiza el análisis heurístico más exhaustivo posible.
     - **Recomendado**. El nivel de seguridad que ofrece el equilibrio perfecto entre el rendimiento de la aplicación y la seguridad del tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.
     - **Bajo**. La configuración de este nivel de seguridad de tráfico web garantiza el análisis más rápido de tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis superficial.
   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina su propia configuración del componente (consulte la tabla siguiente).

     Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Restaurar nivel de seguridad recomendado**.
5. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos del tráfico web:
   - **Bloquear**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.
   - **Informar**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, Kaspersky Endpoint Security permite que este objeto se descargue en el equipo, pero añade información sobre el objeto a la lista de amenazas activas.
6. Guarde los cambios.

Configuración de Protección frente a amenazas web recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
Contrastar la dirección web en la base de datos de direcciones web maliciosas	**Activa**	Al analizar los enlaces para determinar si están incluidos en la base de datos de direcciones web maliciosas, se le permite rastrear sitios web que hayan sido incluidos en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web maliciosas, que se incluye en el paquete de instalación de la aplicación y que se actualiza con las actualizaciones de la base de datos de Kaspersky Endpoint Security.
Contrastar la dirección web en la base de datos de direcciones web de phishing	**Activa**	La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.
Usar análisis heurístico (Protección frente a amenazas web)	**Análisis medio**	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
Usar análisis heurístico (Anti-Phishing)	**Activa**	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.
Acción al detectar una amenaza	**Bloquear**	Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.

Configuración de métodos de detección de direcciones web maliciosas

Protección frente a amenazas web detecta direcciones web maliciosas utilizando bases de datos antivirus, el Servicio en la nube de Kaspersky Security Network y análisis heurístico.

Puede seleccionar métodos de detección de direcciones web maliciosas solo en la Consola de administración (MMC) o en la interfaz local de la aplicación. No puede seleccionar métodos de detección de direcciones web maliciosas en Web Console o Cloud Console. La opción predeterminada es comparar las direcciones web con la base de datos de direcciones maliciosas con análisis heurístico (análisis medio).

Análisis usando la base de datos de direcciones maliciosas

Al analizar los enlaces para determinar si están incluidos en la base de datos de direcciones web maliciosas, se le permite rastrear sitios web que hayan sido incluidos en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web maliciosas, que se incluye en el paquete de instalación de la aplicación y que se actualiza con las actualizaciones de la base de datos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security analiza todos los enlaces para determinar si están incluidos en bases de datos de direcciones web maliciosas. La configuración del análisis de conexión segura de la aplicación no afecta la funcionalidad de análisis de enlaces. En otras palabras, si el análisis de conexiones cifradas está desactivado, Kaspersky Endpoint Security verifica los enlaces con bases de datos de direcciones web maliciosas, aunque el tráfico de red se transmita a través de una conexión cifrada.

Cómo habilitar o deshabilitar la verificación de direcciones web con la base de datos de direcciones web maliciosas a través de la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, en el bloque **Métodos de análisis**, seleccione o desactive la casilla de verificación **Contrastar la dirección web en la base de datos de direcciones web maliciosas** para activar o desactivar el contraste de direcciones con la base de datos de direcciones web maliciosas.
6. Guarde los cambios.

Cómo habilitar o deshabilitar la verificación de direcciones con la base de datos de direcciones maliciosas en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Métodos de análisis**, seleccione o desactive la casilla de verificación **Contrastar la dirección web en la base de datos de direcciones web maliciosas** para activar o desactivar el contraste de direcciones con la base de datos de direcciones web maliciosas.
5. Guarde los cambios.

Análisis heurístico

Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones en el sistema operativo. El análisis heurístico puede detectar amenazas para las que no existen registros actualmente en las bases de datos de Kaspersky Endpoint Security.

Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.

Cómo activar o desactivar el uso del análisis heurístico en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, en el bloque **Métodos de análisis**, seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar el tráfico web en busca de virus y otros tipos de software malicioso.
6. Utilice el control deslizante para definir el análisis de nivel heurístico: **análisis superficial**, **análisis medio** o **análisis profundo**.

   Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
7. Guarde los cambios.

Cómo activar o desactivar el uso del análisis heurístico en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Métodos de análisis**, seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar el tráfico web en busca de virus y otros tipos de software malicioso.

   Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
5. Guarde los cambios.

Anti-Phishing

Protección frente a amenazas web comprueba los enlaces para ver si pertenecen a direcciones web de phishing. Esto ayuda a prevenir *ataques de phishing*. Un intento de phishing se puede disfrazar, por ejemplo, como un mensaje de correo electrónico de su banco con un enlace al sitio web oficial del banco. Al hacer clic en el enlace, se abre una copia exacta del sitio web del banco e incluso puede ver la dirección real en el navegador, a pesar de que se trata de una imitación. A partir de este momento, todas sus acciones dentro del sitio son rastreadas y pueden servir para robarle su dinero.

Puesto que los enlaces a los sitios web phishing pueden recibirse no solo por correo electrónico, sino también por otros medios, como servicios de mensajería, el componente Protección frente a amenazas web supervisa los intentos de acceder a un sitio web phishing en el nivel de análisis del tráfico web y bloquea el acceso a esos sitios web. Las listas de direcciones fraudulentas se incluyen en el kit de distribución de Kaspersky Endpoint Security.

Puede configurar Anti-Phishing solo en la Consola de administración (MMC) o en la interfaz local de la aplicación. No puede configurar Anti-Phishing en Web Console o Cloud Console. De forma predeterminada, Anti-Phishing con análisis heurístico está habilitado.

Cómo activar o desactivar Anti-Phishing en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.

5. Dentro de la ventana que se abre, en el bloque **Configuración de Anti-Phishing**, seleccione o desactive la casilla de verificación **Contrastar la dirección web en la base de datos de direcciones web de phishing** para activar o desactivar Anti-Phishing.

   La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.

6. Seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar páginas web en busca de enlaces de phishing.

   Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones en el sistema operativo. El análisis heurístico puede detectar amenazas para las que no existen registros actualmente en las bases de datos de Kaspersky Endpoint Security.

   Para analizar enlaces, además de la base de datos antivirus y el análisis heurístico, puede utilizar bases de datos de reputación de Kaspersky Security Network.

7. Guarde los cambios.

Cómo activar o desactivar Anti-Phishing en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.

3. Haga clic en **Configuración avanzada**.

4. Si desea que el componente Protección frente a amenazas web compruebe los enlaces con las bases de datos de direcciones web de phishing, seleccione la casilla de verificación **Contrastar la dirección web en la base de datos de direcciones web de phishing** en el bloque **Anti-Phishing**. La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.

5. Seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar páginas web en busca de enlaces de phishing.

   Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones en el sistema operativo. El análisis heurístico puede detectar amenazas para las que no existen registros actualmente en las bases de datos de Kaspersky Endpoint Security.

   Para analizar enlaces, además de la base de datos antivirus y el análisis heurístico, puede utilizar bases de datos de reputación de Kaspersky Security Network.

6. Guarde los cambios.

Creación de la lista de direcciones web de confianza

Además de sitios web maliciosos y de phishing, Protección frente a amenazas web puede bloquear otros sitios web. Por ejemplo, Protección frente a amenazas web bloquea el tráfico HTTP que no cumple con los estándares RFC. Puede crear una lista de direcciones URL en cuyo contenido confía. El componente Protección frente a amenazas web no analiza la información desde direcciones web de confianza en busca de virus u otras amenazas. Esta opción es útil, por ejemplo, cuando el componente Protección frente a amenazas web interfiere en la descarga de un archivo de un sitio web conocido.

Una dirección URL puede ser la dirección de una página web concreta o de la dirección de un sitio web.

Cómo añadir una dirección web de confianza mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
5. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
6. En la ventana que se abre, seleccione la ficha **Direcciones web de confianza**.
7. Seleccione la casilla **No analizar tráfico web de direcciones web de confianza**.

   Si se selecciona esta opción, el componente Protección frente a amenazas web no analiza el contenido de páginas o sitios web cuyas direcciones estén incluidas en la lista de direcciones web de confianza. Puede añadir a esta lista de direcciones web de confianza tanto direcciones específicas como máscaras de páginas o sitios web.
8. Cree una lista de direcciones URL/páginas web en cuyo contenido confíe.

   Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

   También puede importar una lista de direcciones web de confianza desde un archivo XML.
9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir una dirección web de confianza en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Zona de confianza**.

5. En la ventana que se abre, haga clic en el vínculo **Direcciones web**.

   Esto abre una ventana que contiene una lista de direcciones web de confianza.

6. Cree una lista de direcciones URL/páginas web en cuyo contenido confíe.

   Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

   También puede importar una lista de direcciones web de confianza desde un archivo JSON.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir una dirección web de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.

3. Haga clic en **Configuración avanzada**.

4. Seleccione la casilla **No analizar el tráfico web de direcciones URL de confianza**.

   Si se selecciona esta opción, el componente Protección frente a amenazas web no analiza el contenido de páginas o sitios web cuyas direcciones estén incluidas en la lista de direcciones web de confianza. Puede añadir a esta lista de direcciones web de confianza tanto direcciones específicas como máscaras de páginas o sitios web.

5. Cree una lista de direcciones URL/páginas web en cuyo contenido confíe.

   Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

   También puede importar una lista de direcciones web de confianza desde un archivo XML.

6. Guarde los cambios.

Como resultado, Protección frente a amenazas web no analiza el tráfico de direcciones web de confianza. El usuario siempre puede abrir un sitio web de confianza y descargar un archivo de ese sitio web. Si no puede acceder al sitio web, verifique la configuración de los componentes Análisis de conexiones cifradas, Control Web y Supervisión de puertos de red. Si Kaspersky Endpoint Security detecta que un archivo descargado de un sitio web confiable es malicioso, puede añadir este archivo a las exclusiones.

También puede crear una lista general de exclusiones para conexiones cifradas. En este caso, Kaspersky Endpoint Security no analiza el tráfico HTTPS de las direcciones web de confianza cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control Web están haciendo su trabajo.

Exportación e importación de la lista de direcciones web de confianza

Puede exportar la lista de direcciones web de confianza a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir gran cantidad de direcciones web del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de direcciones web de confianza o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de direcciones web de confianza en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas web**.
4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, seleccione la ficha **Direcciones web de confianza**.
6. Para exportar la lista de direcciones web de confianza:
   a. Seleccione las direcciones web de confianza que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna dirección web de confianza, Kaspersky Endpoint Security exportará todas las direcciones web.
   b. Haga clic en el enlace **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de direcciones web de confianza y seleccione la carpeta en la que desee guardar este archivo.
   d. Guarde el archivo.
      Kaspersky Endpoint Security exporta la lista completa de direcciones web de confianza al archivo XML.
7. Para importar la lista de direcciones de confianza:
   a. Haga clic en el enlace **Importar**.
      En la ventana que se abre, seleccione el archivo XML del que importar la lista de direcciones de confianza.
   b. Abra el archivo.
      Si el equipo ya tiene una lista de direcciones de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.

Cómo exportar e importar una lista de direcciones web de confianza en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección de comunicaciones y web → Protección frente a amenazas web**.

5. Para exportar la lista de exclusiones en el bloque **Lista de reglas**:

   a. Seleccione las direcciones web de confianza que desea exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de direcciones web de confianza a un archivo JSON en la carpeta de descargas predeterminada.

6. Para importar una lista de exclusiones en el bloque **Lista de reglas**:

   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que importar la lista de direcciones de confianza.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de direcciones de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

7. Guarde los cambios.

Protección frente a amenazas en el correo

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

Protección frente a amenazas en el correo puede analizar tanto los mensajes entrantes como los salientes. La aplicación es compatible con POP3, SMTP, IMAP y NNTP en los siguientes clientes de correo:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Para analizar el tráfico en los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, debe añadir el certificado de Kaspersky a la tienda de certificados y seleccionar su tienda propia de certificados.

Protección frente a amenazas en el correo no es compatible con otros protocolos y clientes de correo.

Es posible que Protección frente a amenazas en el correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, Protección frente a amenazas en el correo incluye una extensión para Microsoft Office Outlook. La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección frente a amenazas en el correo admite las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365. En equipos basados en Arm, la extensión Protección frente a amenazas en el correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64.

El componente Protección frente a amenazas en el correo no analiza los mensajes si el programa de correo se abre en un navegador.

Cuando se detecta un archivo malicioso en un archivo adjunto, Kaspersky Endpoint Security añade información sobre la acción realizada en el asunto del mensaje, por ejemplo: *[El mensaje ha sido procesado] <asunto del mensaje>*.

Activación y desactivación de Protección frente a amenazas en el correo

De forma predeterminada, el componente Protección frente a amenazas en el correo está activado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para la Protección frente a amenazas en el correo, la aplicación puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que la configuración del nivel de seguridad de correo **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky (vea la tabla más abajo). Puede seleccionar uno de los niveles de seguridad del correo electrónico preinstalados o configurar un nivel de seguridad del correo electrónico personalizado. Si ha cambiado la configuración del nivel de seguridad del correo, siempre puede volver a la configuración recomendada del nivel de seguridad del correo.

Al trabajar con el cliente de correo electrónico Mozilla Thunderbird, si se utilizan filtros para mover mensajes fuera de la carpeta Bandeja de entrada, el componente Protección frente a amenazas en el correo no analiza en busca de virus y otras amenazas los mensajes de correo electrónico transmitidos mediante el protocolo IMAP.

Cómo activar o desactivar el componente Protección frente a amenazas en el correo en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.
4. Utilice la casilla de verificación **Protección frente a amenazas en el correo** para activar o desactivar el componente.

5. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:

   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:

     - **Máximo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo analiza los mensajes más exhaustivamente. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico avanzado. El nivel de seguridad de correo Máximo se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo electrónico gratuito desde una red doméstica sin protección centralizada del correo electrónico.

     - **Recomendado**. El nivel de seguridad de correo electrónico que proporciona el equilibrio perfecto entre el rendimiento de la aplicación y la seguridad del correo electrónico. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico de correo. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.

     - **Mínimo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo solamente analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza archivos adjuntos en mensajes de correo electrónico. Con este nivel de seguridad, el componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico a una velocidad máxima y con un uso mínimo de recursos del sistema operativo. Se recomienda el nivel de seguridad de correo Mínimo para su uso en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una LAN empresarial con protección centralizada del correo electrónico.

   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** y defina su propia configuración del componente (consulte la tabla siguiente).

     Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Predeterminado**.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos:

   - **Desinfectar; eliminar si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante o saliente, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación eliminará el objeto infectado. La aplicación añade información sobre la acción realizada al asunto del mensaje, por ejemplo: *[Se ha procesado el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, la aplicación intenta desinfectar el objeto. Si el objeto no se puede desinfectar, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

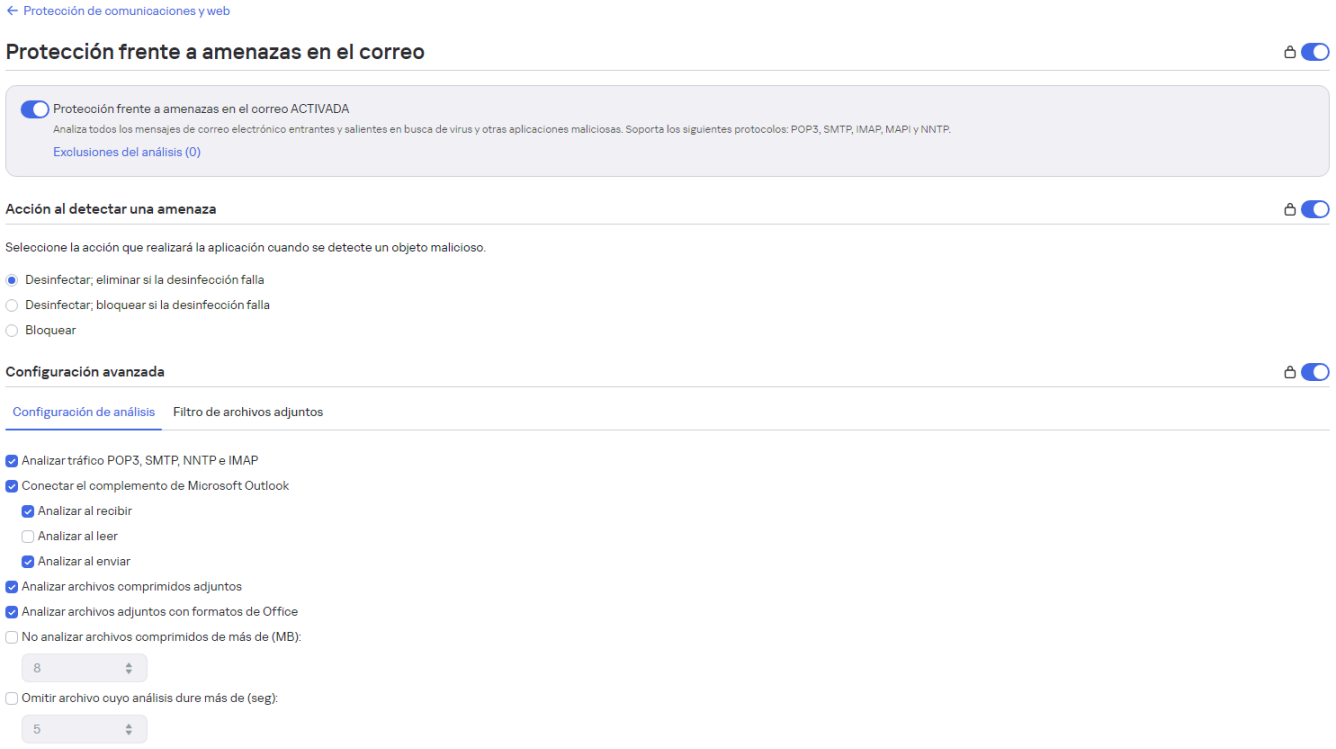
   - **Bloquear**. Si se detecta un objeto infectado en un mensaje entrante, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el componente Protección frente a amenazas en el correo en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección de comunicaciones y web** → **Protección frente a amenazas en el correo**.



Configuración de la Protección frente a amenazas en el correo

5. Utilice interruptor **Protección frente a amenazas en el correo ACTIVADA** para activar o desactivar el componente.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos:

   - **Desinfectar; eliminar si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante o saliente, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación eliminará el objeto infectado. La aplicación añade información sobre la acción realizada al asunto del mensaje, por ejemplo: *[Se ha procesado el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, la aplicación intenta desinfectar el objeto. Si el objeto no se puede desinfectar, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

   - **Bloquear**. Si se detecta un objeto infectado en un mensaje entrante, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

7. De ser necesario, edite la configuración avanzada de la Protección frente a amenazas en el correo.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el componente Protección frente a amenazas en el correo en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.

3. Utilice interruptor **Protección frente a amenazas en el correo** para activar o desactivar el componente.

4. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:

   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:

     - **Alto**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo analiza los mensajes más exhaustivamente. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico avanzado. El nivel de seguridad de correo Máximo se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo electrónico gratuito desde una red doméstica sin protección centralizada del correo electrónico.

     - **Recomendado**. El nivel de seguridad de correo electrónico que proporciona el equilibrio perfecto entre el rendimiento de la aplicación y la seguridad del correo electrónico. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico de correo. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.

     - **Bajo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo solamente analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza archivos adjuntos en mensajes de correo electrónico. Con este nivel de seguridad, el componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico a una velocidad máxima y con un uso mínimo de recursos del sistema operativo. Se recomienda el nivel de seguridad de correo Mínimo para su uso en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una LAN empresarial con protección centralizada del correo electrónico.

   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina su propia configuración del componente (consulte la tabla siguiente).

     Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Restaurar nivel de seguridad recomendado**.

5. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos:

   - **Desinfectar; eliminar si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante o saliente, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación eliminará el objeto infectado. La aplicación añade información sobre la acción realizada al asunto del mensaje, por ejemplo: *[Se ha procesado el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, la aplicación intenta desinfectar el objeto. Si el objeto no se puede desinfectar, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

   - **Bloquear**. Si se detecta un objeto infectado en un mensaje entrante, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

6. Guarde los cambios.

Configuración de Protección frente a amenazas en el correo recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
Cobertura de protección	**Mensajes entrantes y salientes**	La *Cobertura de protección* incluye objetos que el componente comprueba cuando se ejecuta: Mensajes entrantes y salientes o Solo mensajes entrantes. Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar que los archivos infectados se envíen en archivos. También puede activar el análisis de mensajes salientes si desea evitar que se envíen archivos en formatos particulares, como archivos de audio y vídeo, por ejemplo.
Conectar el complemento de Microsoft Outlook	**Activa**	Si esta casilla está seleccionada, los mensajes de correo electrónico que se transmitan a través de los protocolos POP3, SMTP, NNTP e IMAP se analizarán con la extensión integrada en Microsoft Outlook. Si el correo se analiza usando la extensión para Microsoft Outlook, se recomienda usar el Cached Exchange Mode. Para información más detallada sobre el Modo caché de Exchange y recomendaciones sobre su uso, consulte la Base de conocimientos de Microsoft.
Analizar archivos adjuntos	**Activa**	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar archivos adjuntos con formatos de Microsoft Office	**Activa**	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
Filtro de archivos adjuntos	**Renombrar los adjuntos de los tipos seleccionados**	Si se selecciona esta opción, el componente Protección frente a amenazas en el correo cambia el último carácter de la extensión en archivos adjuntos de los tipos especificados con el símbolo de barra baja (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.
Análisis heurístico	**Análisis medio**	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
Acción al detectar una amenaza	**Desinfectar; eliminar si la desinfección falla**	Cuando se detecta un objeto infectado en un mensaje entrante o saliente, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación eliminará el objeto infectado. La aplicación añade información sobre la acción realizada al asunto del mensaje, por ejemplo: *[Se ha procesado el mensaje] <asunto del mensaje>*.

Modificación de las acciones que se van a realizar en mensajes de correo electrónico infectados

De forma predeterminada, el componente Protección frente a amenazas en el correo automáticamente intenta desinfectar todos los mensajes de correo electrónico infectados que se detecten. Si la desinfección falla, el componente Protección frente a amenazas en el correo elimina los mensajes de correo infectados.

Para cambiar la acción que se debe realizar con los mensajes de correo electrónico infectados:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.

3. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security cuando se detecta un mensaje infectado.

   - **Desinfectar; eliminar si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante o saliente, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación eliminará el objeto infectado. La aplicación añade información sobre la acción realizada al asunto del mensaje, por ejemplo: *[Se ha procesado el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, la aplicación intenta desinfectar el objeto. Si el objeto no se puede desinfectar, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

   - **Bloquear**. Si se detecta un objeto infectado en un mensaje entrante, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

4. Guarde los cambios.

Formación la cobertura de protección del componente de Protección frente a amenazas en el correo

La *cobertura de protección* hace referencia a los objetos que son analizados por el componente cuando este está activo. Las coberturas de protección de los distintos componentes tienen distintas propiedades. Las propiedades de la cobertura de protección del componente Protección frente a amenazas en el correo incluyen los parámetros para integrarlo en clientes de correo, así como el tipo de mensajes de correo electrónico y los protocolos de correo electrónico cuyo tráfico analiza este componente. De forma predeterminada, Kaspersky Endpoint Security analiza los mensajes de correo entrante y saliente, así como el tráfico, a través de los protocolos POP3, SMTP, NNTP e IMAP, y se integra en los clientes de correo electrónico Microsoft Office Outlook.

Para formar la cobertura de protección del componente de Protección frente a amenazas en el correo:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Cobertura de protección**, seleccione los mensajes a analizar:

   - **Mensajes entrantes y salientes**.

   - **Solo mensajes entrantes**.

   Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar que los archivos infectados se envíen en archivos. También puede activar el análisis de mensajes salientes si desea evitar que se envíen archivos en formatos particulares, como archivos de audio y vídeo, por ejemplo.

Si elige analizar solo los mensajes entrantes, recomendamos que lleve a cabo un único análisis de todos los mensajes salientes, ya que existe la posibilidad de que su equipo tenga gusanos del correo electrónico que se distribuyan por correo. Esto ayuda a evitar problemas provocados por un envío masivo e incontrolado por correo electrónico de mensajes infectados desde su equipo.

5. En el bloque **Conectividad**, haga lo siguiente:

   - Si quiere que el componente Protección frente a amenazas en el correo analice los mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que el equipo del usuario los reciba, active la casilla de verificación **Analizar tráfico POP3, SMTP, NNTP e IMAP**.

     Si no quiere que el componente Protección frente a amenazas en el correo analice los mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen al equipo del usuario, desactive la casilla de verificación **Analizar tráfico POP3, SMTP, NNTP e IMAP**. En este caso, los mensajes son analizados por la extensión de la Protección frente a amenazas en el correo incorporada al cliente de correo de Microsoft Office Outlook después de que llegan al equipo del usuario si se selecciona la casilla de verificación **Conectar el complemento de Microsoft Outlook**.

     Si utiliza un cliente de correo que no sea Microsoft Office Outlook, el componente Protección frente a amenazas en el correo no analiza los mensajes que se transmiten a través de los protocolos POP3, SMTP, NNTP e IMAP cuando la casilla de verificación **Analizar tráfico POP3, SMTP, NNTP e IMAP** está desactivada.

   - Si desea permitir el acceso a la configuración del componente Protección frente a amenazas en el correo desde Microsoft Office Outlook y activar el análisis de los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que llegan al equipo utilizando la extensión incorporada a Microsoft Office Outlook, seleccione la casilla de verificación **Conectar el complemento de Microsoft Outlook**.

     Si desea bloquear el acceso a la configuración del componente Protección frente a amenazas de correo desde Microsoft Office Outlook y no desea que los mensajes transmitidos por POP3, SMTP, NNTP, IMAP y MAPI se analicen con la extensión para Microsoft Office Outlook una vez que estén en el equipo, desactive la casilla de verificación **Conectar el complemento de Microsoft Outlook**.

     La extensión Protección frente a amenazas en el correo se integra en el programa de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

6. Guarde los cambios.

Analizar archivos compuestos adjuntos a mensajes de correo electrónico

Puede activar o desactivar el análisis de adjuntos del mensaje, limitar el tamaño máximo de los adjuntos de los mensajes para su análisis y limitar la duración máxima del análisis del adjunto del mensaje.

Para configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Análisis de archivos compuestos**, establezca la configuración del análisis:

   - **Analizar archivos adjuntos con formatos de Microsoft Office**. Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.

   - **Analizar archivos adjuntos**. Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).

     Si, durante el análisis, la aplicación detecta una contraseña para un archivo en el texto del mensaje, esta contraseña se utilizará para analizar el contenido del archivo en busca de aplicaciones maliciosas. En este caso, la contraseña no se guardará. Un archivo de descomprime durante el análisis. Si ocurre un error con la aplicación durante el proceso de descomprimir, puede eliminar manualmente los archivos descomprimidos que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tienen el prefijo PR.

   - **No analizar archivos comprimidos de más de N MB (de 1 a 9999)**. Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en el correo excluye del análisis los archivos adjuntos de los mensajes de correo electrónico si su tamaño supera el valor especificado. Si se desactiva la casilla de verificación, el componente Protección frente a amenazas en el correo analiza archivos adjuntos de cualquier tamaño.

   - **No comprobar archivos durante más de N segundos (de 1 a 9999)**. Si se selecciona la casilla de verificación, el tiempo asignado para analizar los archivos adjuntos a los mensajes de correo electrónico se limita al período especificado.

5. Guarde los cambios.

Filtro de archivos adjuntos de mensajes de correo electrónico

El filtrado de adjuntos no se aplica a los mensajes de correo electrónico salientes.

Las aplicaciones maliciosas se pueden distribuir en forma de adjuntos del correo electrónico. Puede configurar el filtrado según el tipo de adjuntos del mensaje de modo que los archivos de los tipos especificados se renombran o eliminan automáticamente. Al volver a asignar un nombre a un tipo determinado de adjunto, Kaspersky Endpoint Security es capaz de proteger su equipo contra la ejecución automática de una aplicación maliciosa.

Para configurar el filtrado de archivos adjuntos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Filtro de archivos adjuntos**, lleve a cabo una de estas acciones:

   - **Desactivar el filtrado**. Si se selecciona esta opción, el componente Protección frente a amenazas en el correo no filtra archivos que están adjuntos a mensajes de correo electrónico.

   - **Renombrar los adjuntos de los tipos seleccionados**. Si se selecciona esta opción, el componente Protección frente a amenazas en el correo cambia el último carácter de la extensión en archivos adjuntos de los tipos especificados con el símbolo de barra baja (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.

   - **Eliminar los adjuntos de los tipos seleccionados**. Si se selecciona esta opción, el componente Protección frente a amenazas en el correo elimina los archivos adjuntos de los tipos especificados.

5. Si seleccionó la opción **Renombrar los adjuntos de los tipos seleccionados** o **Eliminar los adjuntos de los tipos seleccionados** durante el paso anterior, seleccione las casillas situadas junto a los tipos de archivos pertinentes.

6. Guarde los cambios.

Exportación e importación de extensiones para filtrado de adjuntos

Puede exportar la lista de extensiones de filtro de archivos adjuntos a un archivo XML. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de extensiones o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de extensiones de filtro de archivos adjuntos en la Consola de administración (MMC)

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección de comunicaciones y web → Protección frente a amenazas en el correo**.

5. Para exportar la lista de extensiones en el bloque de **Filtro de archivos adjuntos**:

   a. Seleccione las extensiones que desea exportar.

   b. Haga clic en el enlace **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de extensiones y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

   Kaspersky Endpoint Security exporta la lista completa de extensiones al archivo XML.

6. Para importar la lista de extensiones en el bloque de **Filtro de archivos adjuntos**:

    a. Haga clic en el enlace **Importar**.

    b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de extensiones.

    c. Abra el archivo.

    Si el equipo ya tiene una lista de extensiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

7. Guarde los cambios.

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.

4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.

5. Se abre una ventana; en ella, seleccione la pestaña **Filtro de archivos adjuntos**.

6. Para exportar la lista de extensiones:

    a. Seleccione las extensiones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

    b. Haga clic en el enlace **Exportar**.

    c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de extensiones y seleccione la carpeta en la que desee guardar este archivo.

    d. Guarde el archivo.

    Kaspersky Endpoint Security exporta la lista completa de extensiones al archivo XML.

7. Para importar la lista de extensiones:

    a. Haga clic en el enlace **Importar**.

    b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de extensiones.

    c. Abra el archivo.

    Si el equipo ya tiene una lista de extensiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

8. Guarde los cambios.

Análisis de correos electrónicos en Microsoft Office Outlook

Durante la instalación de Kaspersky Endpoint Security, la extensión Protección frente a amenazas en el correo se incrusta en Microsoft Office Outlook (en adelante, también denominado Outlook). La extensión permite analizar mensajes a nivel de cliente de correo en lugar de a nivel de protocolo. Además de los mensajes, la extensión le permite analizar objetos recibidos a través de la interfaz MAPI desde los repositorios de Microsoft Exchange (por ejemplo, objetos en el Calendario). Este análisis se lleva a cabo en el cliente de correo.

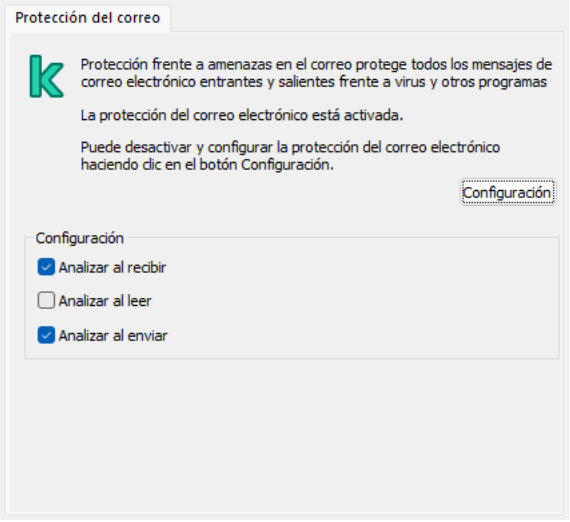
Puede abrir la configuración del componente Protección frente a amenazas en el correo desde Outlook y especificar en qué momento desea que se analicen los mensajes de correo electrónico en busca de virus y otras amenazas.

La extensión Protección frente a amenazas en el correo admite las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365.

En equipos basados en Arm, la extensión Protección frente a amenazas en el correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64.

En Outlook, los mensajes entrantes de correo electrónico se analizan primero con el componente Protección frente a amenazas en el correo (seleccionando la casilla de verificación Analizar tráfico POP3, SMTP, NNTP e IMAP en la interfaz de Kaspersky Endpoint Security) y, a continuación, con la extensión Protección frente a amenazas en el correo para Outlook. Si el componente Protección frente a amenazas en el correo detecta un objeto malicioso en un mensaje, le alerta sobre ello.

La configuración del componente Protección frente a amenazas en el correo se puede definir directamente en Outlook si la extensión para Microsoft Office Outlook está conectada en la interfaz de Kaspersky Endpoint Security (vea la figura a continuación).



Configuración del componente Protección frente a amenazas en el correo para Outlook

Los mensajes salientes son analizados primero por la extensión Protección frente a amenazas en el correo para Outlook y, a continuación, los analiza el componente Protección frente a amenazas en el correo.

Al analizar el correo electrónico con la extensión Protección frente a amenazas en el correo para Outlook, recomendamos utilizar el modo caché de Exchange Server (Use Cached Exchange Mode). Para información más detallada sobre el Modo caché de Exchange y recomendaciones sobre su uso, consulte la Base de conocimientos de Microsoft.

Cómo configurar el modo de funcionamiento de la extensión Protección frente a amenazas en el correo para Outlook en la Consola de administración (MMC)

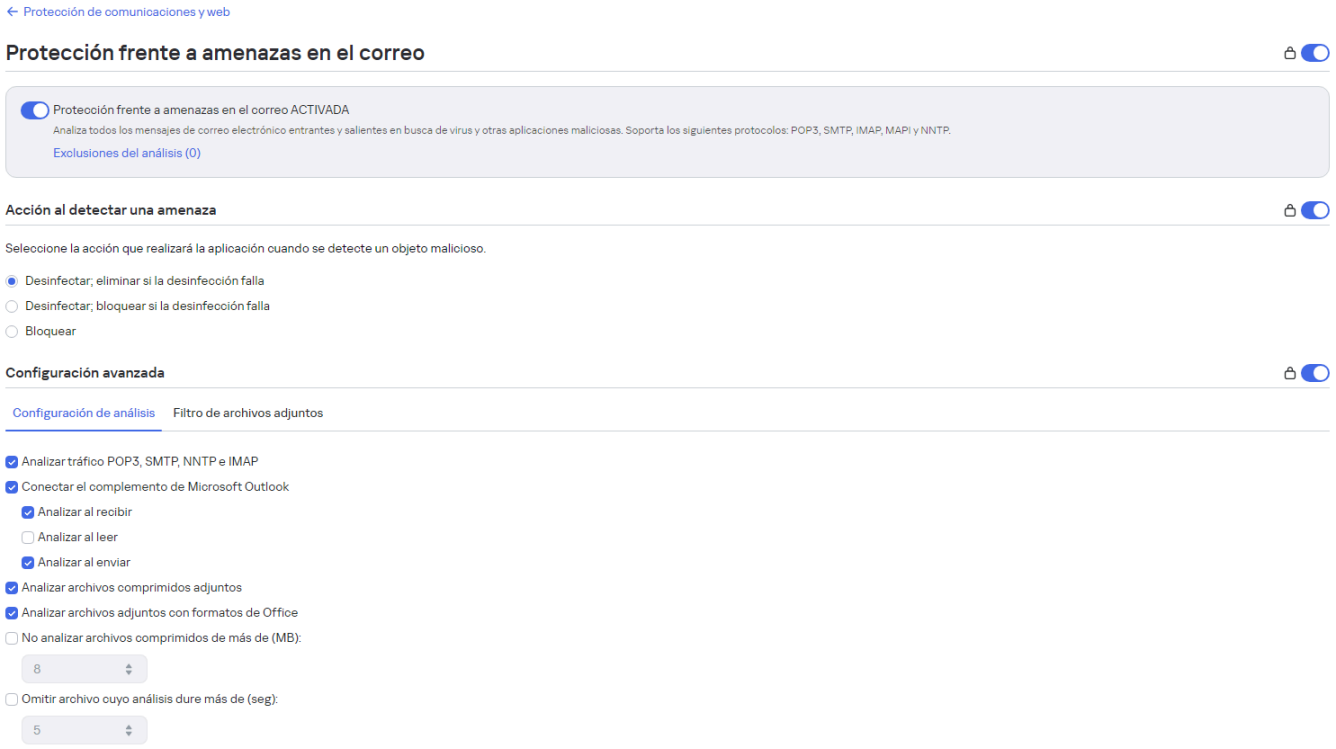
1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en el correo**.
5. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
6. En la ventana que se abre, en el bloque **Conectividad**, seleccione la casilla **Conectar el complemento de Microsoft Outlook**.
7. Haga clic en **Configuración**.
8. En la ventana **Protección del correo**, haga lo siguiente:
   - Seleccione la casilla de verificación **Analizar al recibir** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes entrantes cuando llegan al buzón de correo.
   - Seleccione la casilla de verificación **Analizar al leer** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes entrantes cuando el usuario los abra.
   - Seleccione la casilla de verificación **Analizar al enviar** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes salientes cuando se envían.
9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar el modo de funcionamiento de la extensión Protección frente a amenazas en el correo para Outlook en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección de comunicaciones y web → Protección frente a amenazas en el correo**.



Configuración de la Protección frente a amenazas en el correo

5. En **Configuración avanzada**, seleccione la pestaña **Configuración de análisis**.

6. Seleccione la casilla **Conectar el complemento de Microsoft Outlook**.

7. Configure el modo de funcionamiento de la extensión:

   - Seleccione la casilla de verificación **Analizar al recibir** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes entrantes cuando llegan al buzón de correo.
   - Seleccione la casilla de verificación **Analizar al leer** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes entrantes cuando el usuario los abra.
   - Seleccione la casilla de verificación **Analizar al enviar** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes salientes cuando se envían.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Análisis de correos electrónicos en Thunderbird, MyOffice, R7-Office

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. Para los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, la aplicación obtiene acceso a los mensajes solo en el *nivel de protocolo* (POP3, SMTP, IMAP, NNTP).

Para analizar el tráfico en los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, debe añadir el certificado de Kaspersky a la tienda de certificados y seleccionar su tienda propia de certificados.

El componente Protección frente a amenazas en el correo no analiza los mensajes si el programa de correo se abre en un navegador.

Protección frente a amenazas en el correo en tiempo real

Protección frente a amenazas en el correo puede analizar tanto los mensajes entrantes como los salientes. De forma predeterminada, el componente Protección frente a amenazas en el correo automáticamente intenta desinfectar todos los mensajes de correo electrónico infectados que se detecten. Si la desinfección falla, el componente Protección frente a amenazas en el correo elimina los mensajes de correo infectados. Cuando se detecta un archivo malicioso en un archivo adjunto, Kaspersky Endpoint Security añade información sobre la acción realizada en el asunto del mensaje, por ejemplo: *[El mensaje ha sido procesado] <asunto del mensaje>*.

Al trabajar con el cliente de correo electrónico Mozilla Thunderbird, si se utilizan filtros para mover mensajes fuera de la carpeta Bandeja de entrada, el componente Protección frente a amenazas en el correo no analiza en busca de virus y otras amenazas los mensajes de correo electrónico transmitidos mediante el protocolo IMAP.

Análisis antimalware en bases de datos de correo

La Protección frente a amenazas en el correo evita la infección del equipo a nivel de protocolo, pero si el equipo se había infectado antes de instalar Kaspersky Endpoint Security, la aplicación puede detectar la amenaza en las bases de datos de correo mediante la tarea *Análisis antimalware*. La aplicación no desinfecta ni elimina los archivos infectados en las bases de datos de correo, independientemente de la configuración de la tarea. Esto se debe a que Kaspersky Endpoint Security no desglosa los mensajes de Thunderbird, MyOffice y P7-Office en sus distintas partes (encabezado, cuerpo y archivos adjuntos) del mismo modo que los mensajes de Microsoft Office Outlook. La aplicación solo añade información sobre los objetos detectados a la lista de amenazas activas.

Para eliminar amenazas activas:

1. Busque y elimine manualmente el mensaje con el objeto detectado en la interfaz del cliente de correo.

   La aplicación muestra información sobre el objeto detectado en la lista de amenazas activas.

Ejemplo de tarjeta de objeto detectado:

!	**HEUR:Trojan.PDF.Phish.gen** Objeto: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Realice la operación de compactación de la base de datos.

   Cuando se elimina un mensaje en la interfaz de usuario, el cliente de correo solo agrega una marca de eliminación. El cliente de correo elimina realmente el mensaje solo después de una compactación de la base de datos. Para obtener detalles sobre la compactación de la base de datos, consulte la ayuda de su cliente de correo (por ejemplo, Mozilla Thunderbird).

3. Ejecute la tarea *Análisis antimalware* de nuevo y asegúrese de que la amenaza ya no esté presente.

Si, por cualquier motivo, no es posible eliminar los mensajes con archivos infectados en ese momento, puede procesar dichas amenazas en la interfaz de usuario de Kaspersky Endpoint Security. Para los archivos del cliente de correo electrónico, dispone de dos opciones para procesar una amenaza: **Ignorar** y **Añadir a las exclusiones**. Para evitar que la aplicación añada estos objetos a la lista de amenazas activas durante un nuevo análisis, añádalos a la lista de exclusiones del análisis.

Protección frente a amenazas en la red

El componente *Protección frente a amenazas en la red* (también denominado Intrusion Detection System, IDS) supervisa el tráfico de red entrante en busca de actividad característica de los ataques de red. Cuando la aplicación detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante. Las bases de datos de la aplicación ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos. La lista de ataques de red que detecta el componente Protección frente a amenazas en la red se actualiza durante las actualizaciones de módulos de aplicaciones y bases de datos.

Activación y desactivación de Protección frente a amenazas en la red

De forma predeterminada, Protección frente a amenazas en la red está activado y funcionando en modo óptimo. Kaspersky Endpoint Security monitoriza el tráfico de red entrante en busca de actividad característica de los ataques de red y bloquea estos ataques.

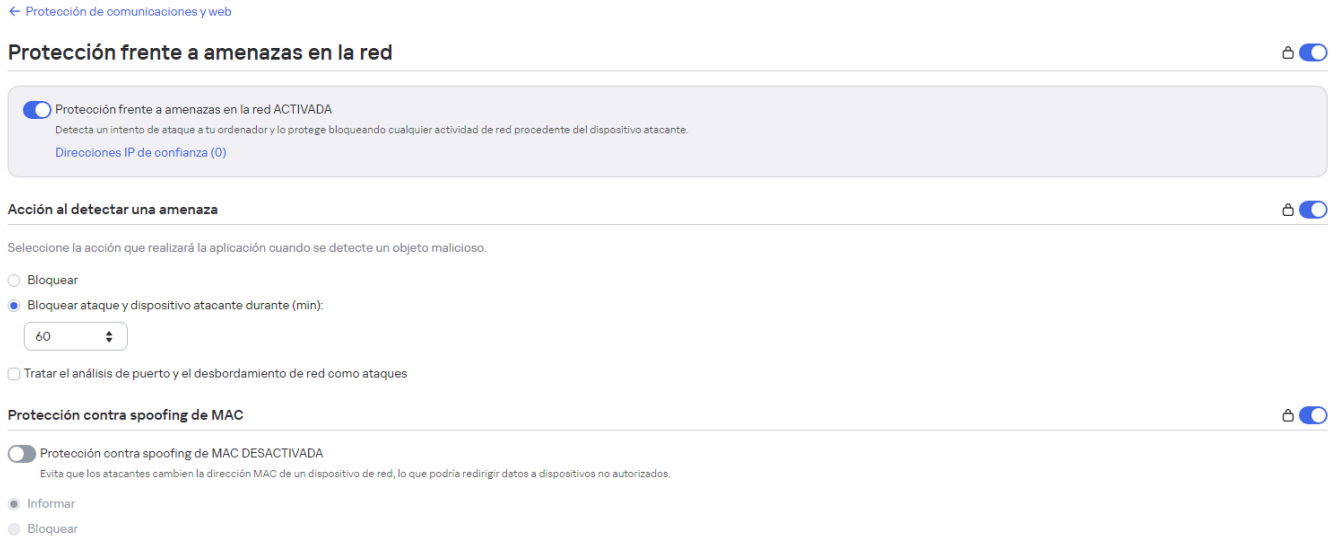
Cómo activar o desactivar la Protección frente a amenazas en la red en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.
4. Utilice la casilla de verificación **Protección frente a amenazas en la red** para activar o desactivar el componente.
5. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar Protección frente a amenazas en la red en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección de comunicaciones y web** → **Protección frente a amenazas en la red**.

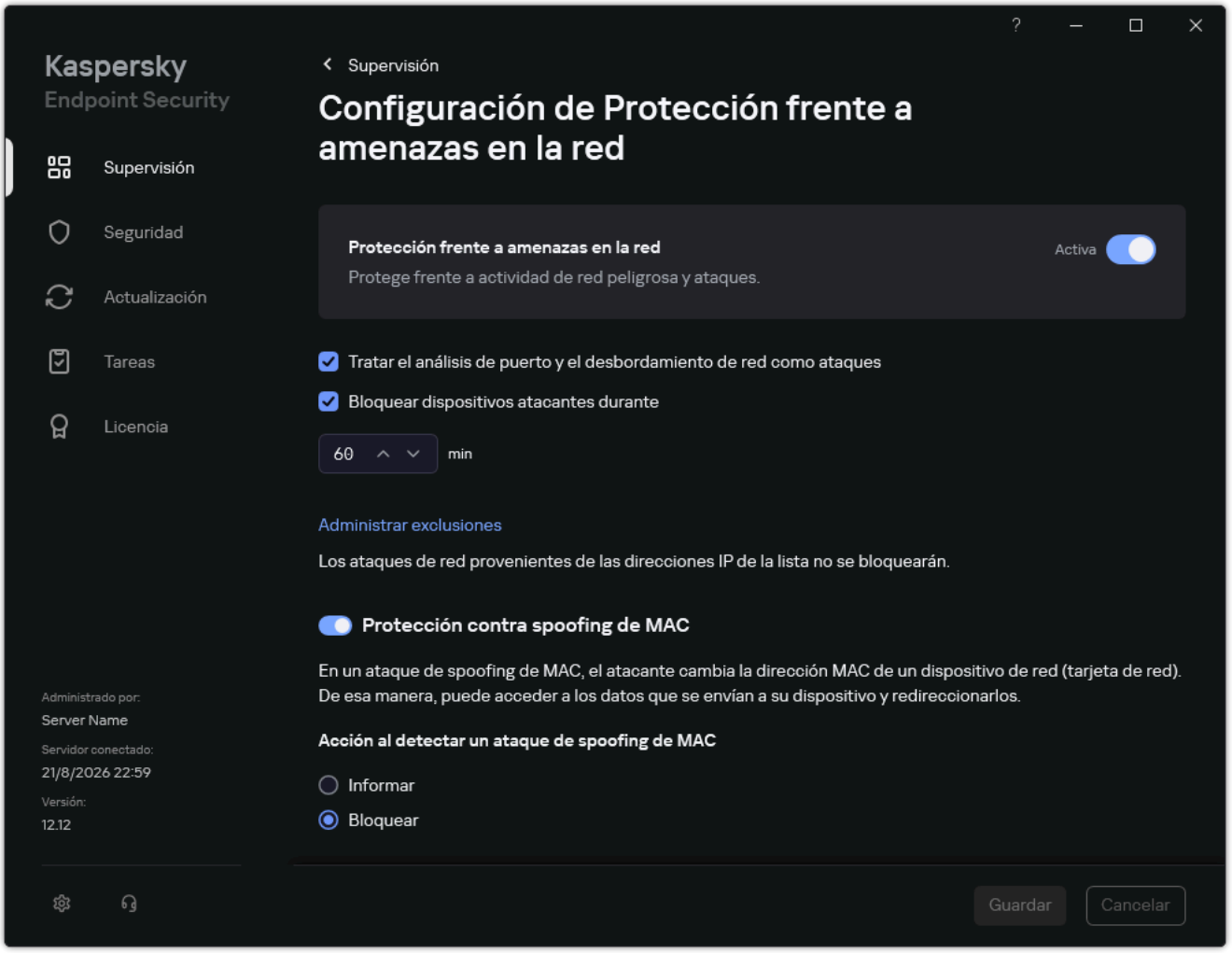


Parámetros de Protección frente a amenazas en la red

5. Utilice interruptor **Protección frente a amenazas en la red ACTIVADA** para activar o desactivar el componente.
6. Guarde los cambios.

Cómo activar o desactivar la Protección frente a amenazas en la red en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.



Parámetros de Protección frente a amenazas en la red

3. Utilice interruptor **Protección frente a amenazas en la red** para activar o desactivar el componente.
4. Guarde los cambios.

Bloquear un equipo atacante

Si el componente Protección frente a amenazas en la red está activado, Kaspersky Endpoint Security bloquea automáticamente las amenazas en la red. Además, la aplicación puede bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado. De forma predeterminada, Kaspersky Endpoint Security bloquea el equipo durante una hora.

Cómo bloquear un equipo atacante en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.

4. En **Configuración de Protección frente a amenazas en la red**, seleccione la casilla **Bloquear dispositivos atacantes durante N min**.

   Si esta opción está activada, el componente Protección frente a amenazas en la red añade al equipo atacante a la lista de bloqueados. Esto quiere decir que el componente Protección frente a amenazas en la red bloquea la conexión de red del equipo atacante después del primer intento de ataque de red durante el período de tiempo especificado. Este bloqueo protege automáticamente al equipo del usuario frente a posibles ataques de red desde la misma dirección en el futuro. El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 999 minutos.

5. Establezca una duración de bloqueo diferente para un equipo atacante en el campo a la derecha de la casilla **Bloquear dispositivos atacantes durante N min**.

6. Guarde los cambios.

Cómo bloquear un equipo atacante en Web Console

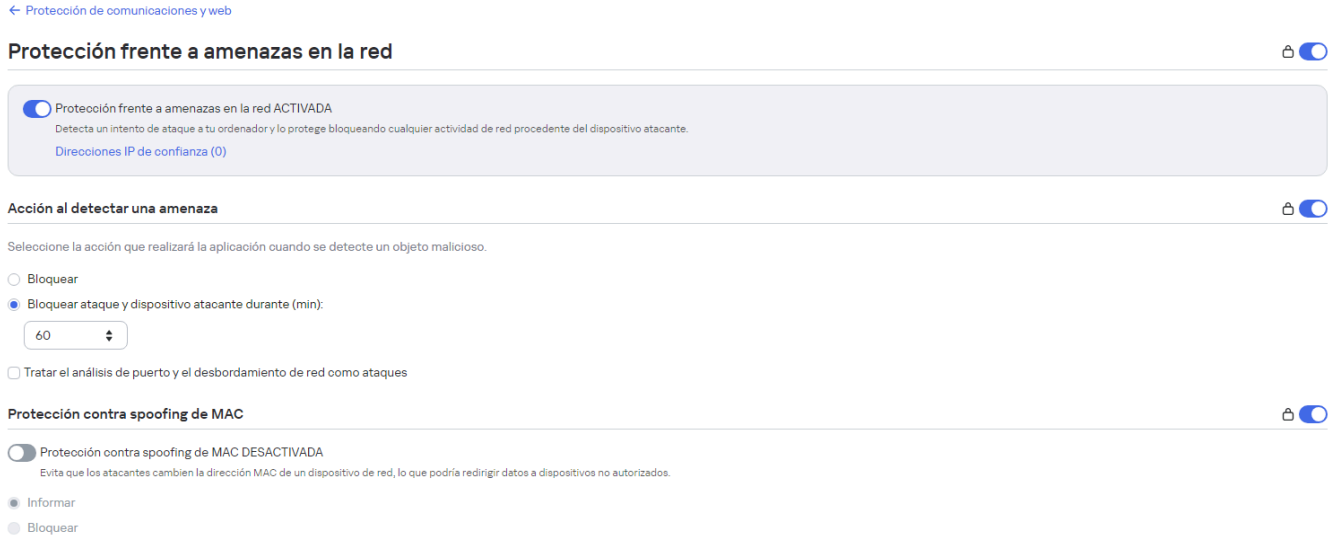
1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección de comunicaciones y web → Protección frente a amenazas en la red**.



Parámetros de Protección frente a amenazas en la red

5. En el bloque **Acción al detectar una amenaza**, seleccione la casilla de verificación **Bloquear ataque y dispositivo atacante durante (min)**.

   Si esta opción está activada, el componente Protección frente a amenazas en la red añade al equipo atacante a la lista de bloqueados. Esto quiere decir que el componente Protección frente a amenazas en la red bloquea la conexión de red del equipo atacante después del primer intento de ataque de red durante el período de tiempo especificado. Este bloqueo protege automáticamente al equipo del usuario frente a posibles ataques de red desde la misma dirección en el futuro. El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 999 minutos.

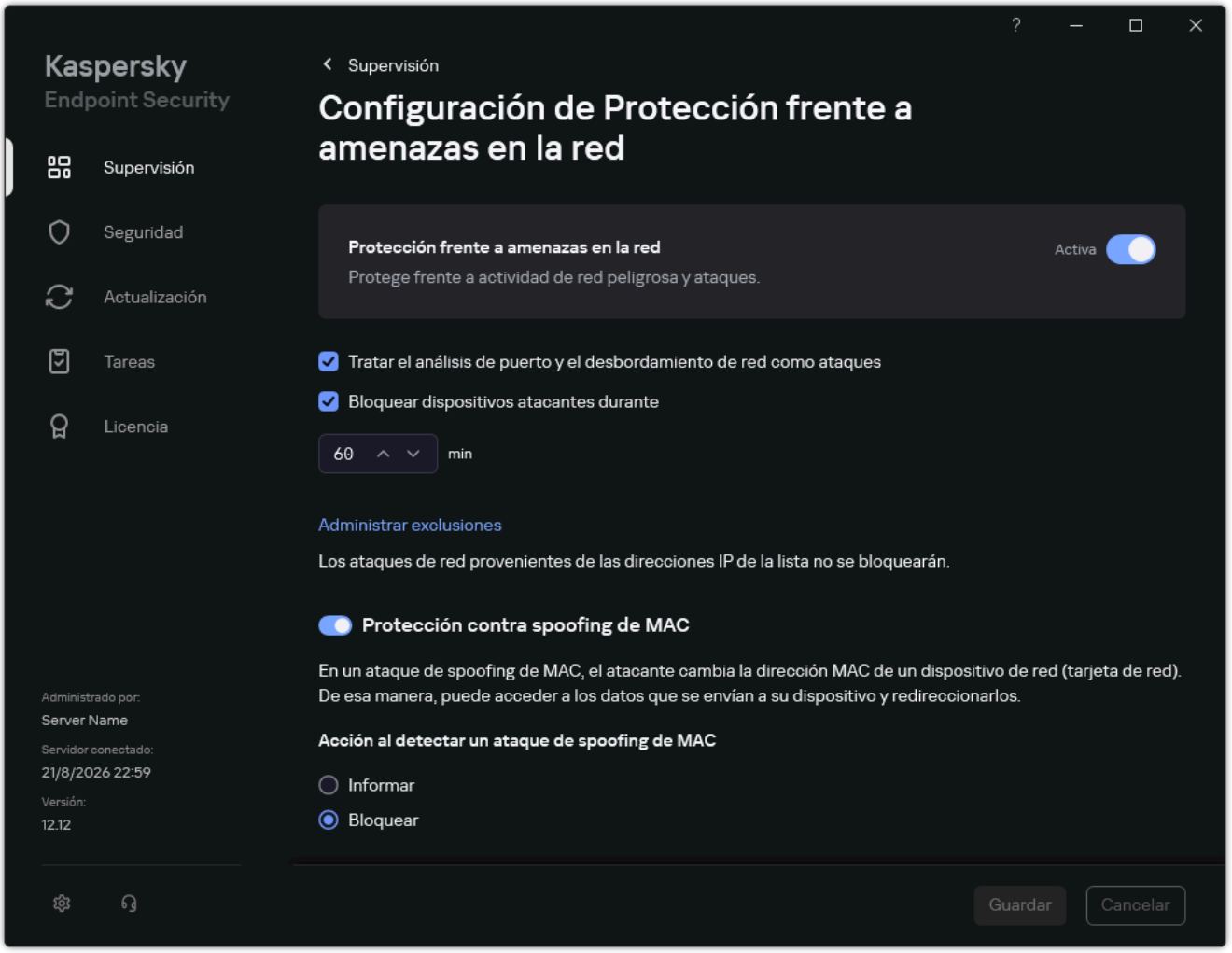
6. Cambia la duración del bloqueo del equipo atacante.

7. Guarde los cambios.

Cómo bloquear un equipo atacante en la interfaz de usuario de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.



Parámetros de Protección frente a amenazas en la red

3. Active el interruptor **Bloquear dispositivos atacantes durante N min**.

   Si esta opción está activada, el componente Protección frente a amenazas en la red añade al equipo atacante a la lista de bloqueados. Esto quiere decir que el componente Protección frente a amenazas en la red bloquea la conexión de red del equipo atacante después del primer intento de ataque de red durante el período de tiempo especificado. Este bloqueo protege automáticamente al equipo del usuario frente a posibles ataques de red desde la misma dirección en el futuro. El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 999 minutos.

4. Establezca una duración de bloqueo diferente para un equipo atacante en el campo que hay bajo el interruptor **Bloquear dispositivos atacantes durante N min**.

5. Guarde los cambios.

Como resultado, cuando Kaspersky Endpoint Security detecta un intento de ataque de red contra el equipo de un usuario, bloqueará todas las conexiones de red con el equipo atacante. Kaspersky Endpoint Security crea el evento de *Ataque de red detectado*. El evento contiene información sobre el equipo atacante: direcciones IP y MAC.

Puede ver la dirección MAC del equipo atacante solo en la interfaz de usuario de la aplicación o en la consola de Kaspersky Security Center versión 15.1 o posterior.



Notificación sobre la detección de ataques a la red

Kaspersky Endpoint Security desbloquea el equipo cuando se agota el tiempo especificado. La consola de Kaspersky Security Center no proporciona herramientas para monitorizar equipos bloqueados además de los eventos *Ataque de red detectado* del informe. Solo puede ver una lista de equipos bloqueados en la interfaz de la aplicación. Esta función la proporciona la herramienta *Monitor de red*. También puedes usar la herramienta Monitor de red para desbloquear un equipo.

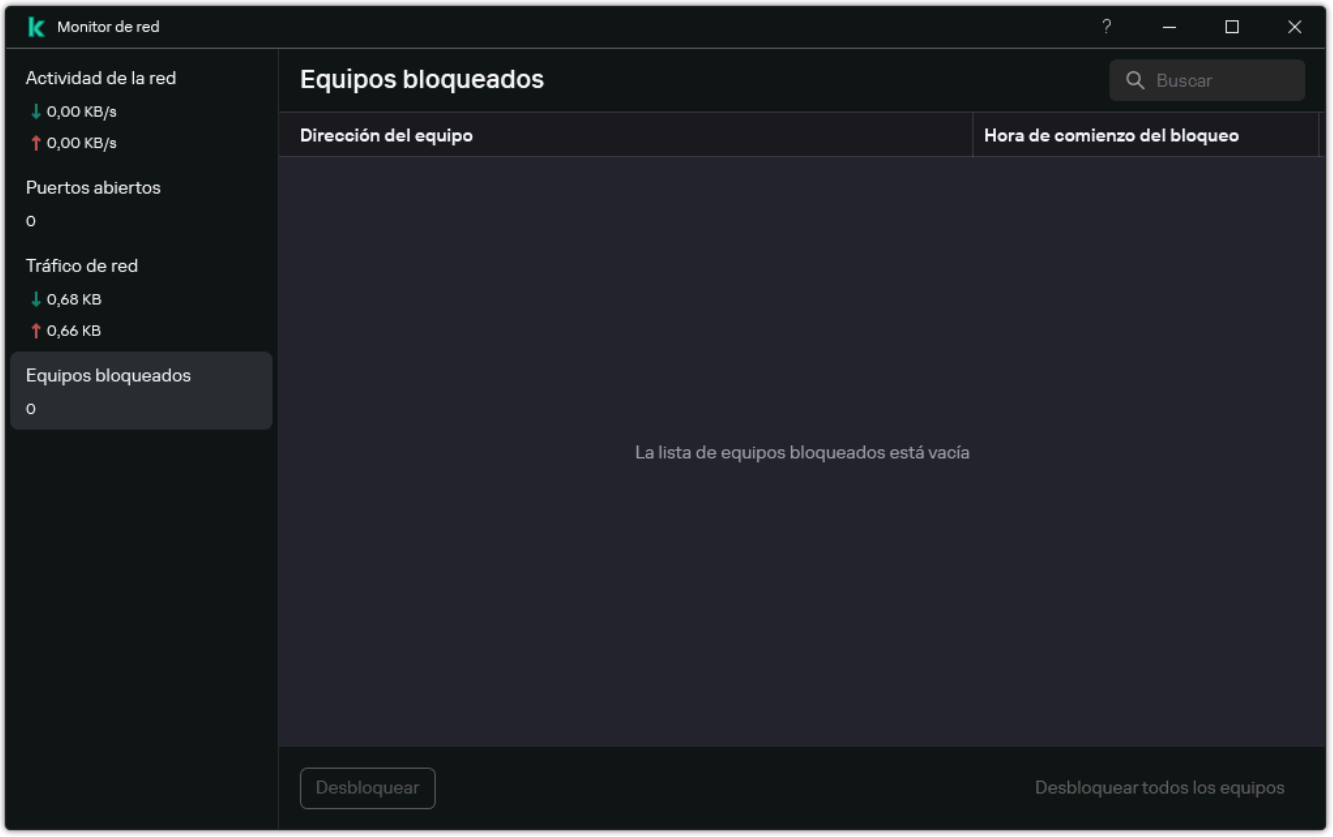
Para desbloquear un equipo:

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.
2. Vaya a la pestaña **Equipos bloqueados**.

   Esto abre una lista de equipos bloqueados (consulte la figura que aparece más abajo).

   Kaspersky Endpoint Security borra la lista de rechazados al reiniciar la aplicación y cuando se cambian los ajustes de Protección frente a amenazas en la red.

3. Seleccione el equipo que desea desbloquear y haga clic en **Desbloquear**.



Lista de equipos bloqueados

Configurar direcciones de exclusiones de bloqueo

Kaspersky Endpoint Security puede reconocer un ataque de red y bloquear una conexión de red no segura que transmita una gran cantidad de paquetes (por ejemplo, desde cámaras de vigilancia). Para trabajar con dispositivos de confianza, puede añadir las direcciones IP de estos dispositivos a la lista de exclusiones. También puede seleccionar el protocolo y el puerto que se van a usar para la comunicación y permitir actividades de red específicas.

Cómo configurar direcciones de exclusiones de bloqueo en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.
5. En el bloque **Configuración de Protección frente a amenazas en la red**, haga clic en el botón **Exclusiones**.
6. En la ventana que se abre, haga clic en el botón **Añadir**.
7. Introduzca la dirección IP del equipo desde el que no se deben bloquear los ataques de red.

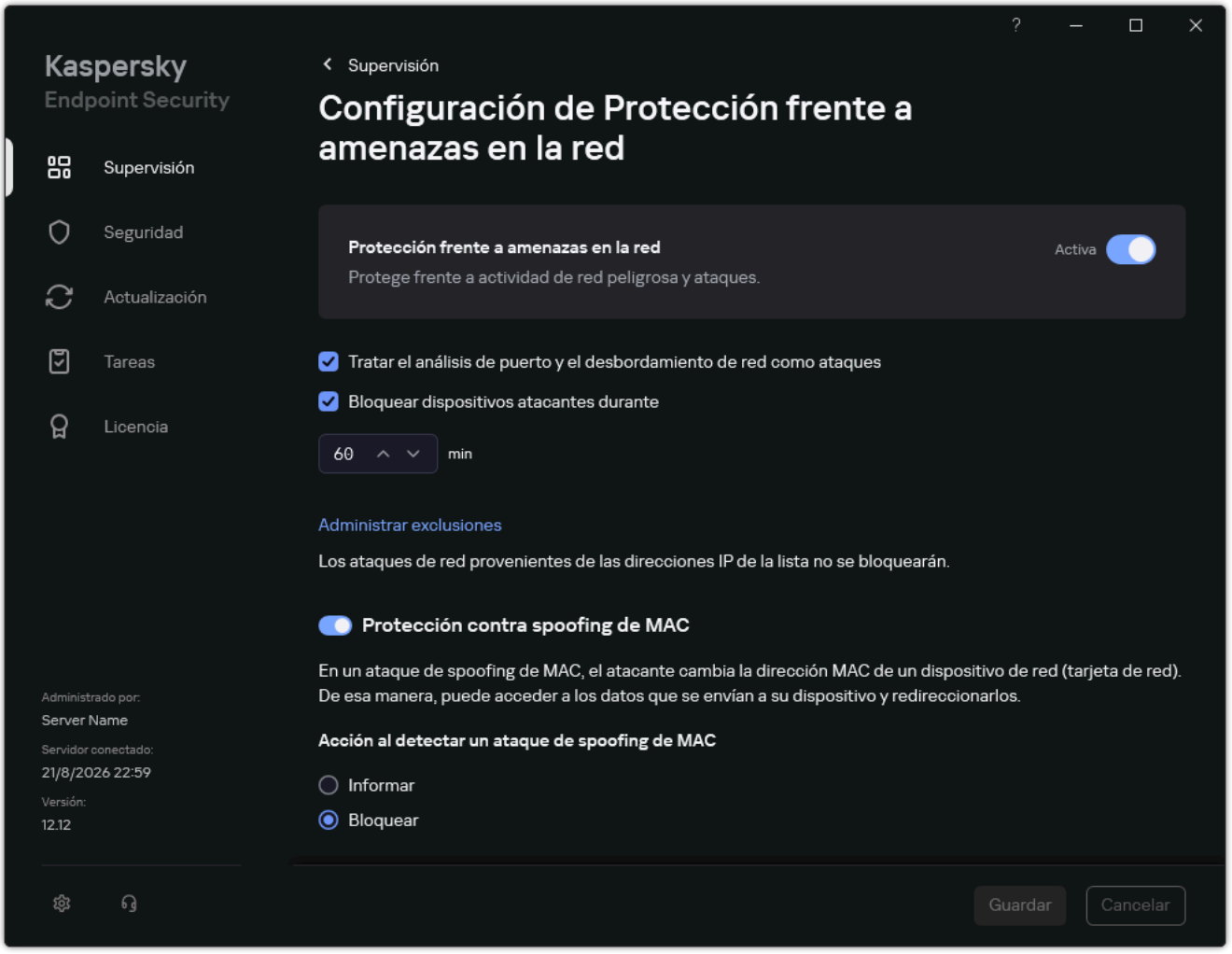
   Si es necesario, seleccione el protocolo y los puertos a través de los cuales se transmiten los datos.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar las direcciones excluidas del bloqueo en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Zona de confianza**.
5. En la ventana que se abre, haga clic en el vínculo **Direcciones IP**.
   Esto abre una ventana que contiene una lista de direcciones IP de confianza.
6. En la ventana que se abre, haga clic en el botón **Añadir**.
7. Introduzca la dirección IP del equipo desde el que no se deben bloquear los ataques de red.
   Si es necesario, especifique la subred.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar direcciones de exclusiones de bloqueo en la interfaz de usuario de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.



Parámetros de Protección frente a amenazas en la red

3. Haga clic en el enlace **Administrar exclusiones**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. Introduzca la dirección IP del equipo desde el que no se deben bloquear los ataques de red.

   Si es necesario, seleccione el protocolo y los puertos a través de los cuales se transmiten los datos.
6. Guarde los cambios.

Exportación e importación de la lista de exclusiones de bloqueo

Puede exportar la lista de exclusiones a un archivo XML. Luego puede modificar el archivo para, por ejemplo, añadir una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de exclusiones en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.
4. En el bloque **Configuración de Protección frente a amenazas en la red**, haga clic en el botón **Exclusiones**.
5. Para exportar la lista de reglas:
   a. Seleccione las exclusiones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna exclusión, Kaspersky Endpoint Security exportará todas las exclusiones.
   b. Haga clic en el botón → **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
   d. Guarde el archivo.
      Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
6. Para importar la lista de exclusiones:
   a. Haga clic en el botón → **Importar**.
   b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
   c. Abra el archivo.
      Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
7. Guarde los cambios.

Cómo exportar e importar una lista de exclusiones en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección de comunicaciones y web → Protección frente a amenazas en la red**.
5. En la parte superior de la ventana, haga clic en el vínculo **Direcciones IP de confianza**.
   Se abre la lista de exclusiones.

6. Para exportar la lista de reglas:

   a. Seleccione las exclusiones que desea exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de exclusiones a un archivo JSON en la carpeta de descargas predeterminada.

7. Para importar la lista de exclusiones:

   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que importar la lista de exclusiones.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

8. Guarde los cambios.

Configuración de Protección frente a amenazas en la red por tipo

Kaspersky Endpoint Security le permite administrar la protección contra los siguientes tipos de ataques a la red:

- *Inundación de red* es un ataque a los recursos de red de una organización (como servidores web). Este ataque consiste en enviar una gran cantidad de solicitudes para sobrecargar el ancho de banda de los recursos de la red. Cuando esto sucede, los usuarios no pueden acceder a los recursos de red de la organización.

- Un ataque de tipo *"Port scan"* consiste en el escaneo de puertos UDP, TCP, puertos y servicios de red en el equipo. Este ataque permite al atacante identificar el grado de vulnerabilidad del equipo antes de realizar tipos de ataques de red más peligrosos. Los ataques de tipo "Port scan" también permiten al atacante identificar el sistema operativo en el equipo y seleccionar los ataques de red apropiados para este sistema operativo.

- Los *ataques de spoofing de MAC* consisten en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Como resultado, un atacante puede redirigir los datos enviados a un dispositivo a otro dispositivo y obtener acceso a esos datos. Kaspersky Endpoint Security le permite saber si se detecta uno de ataques MAC Spoofing y bloquearlo.

Puede activar la detección de este tipo de ataques en caso de que algunas de sus aplicaciones permitidas realicen operaciones típicas de este tipo de ataques. Esto ayudará a evitar falsas alarmas.

De forma predeterminada, Kaspersky Endpoint Security no supervisa los ataques de inundación de red, ataques de tipo "Port scan" y spoofing de MAC.

No puede configurar exclusiones independientes para estos tipos de ataques. Esto significa que, aunque se añadan direcciones IP individuales a la zona de confianza, Kaspersky Endpoint Security bloquea el equipo atacante si se detecta un ataque de este tipo. Puede activar o desactivar la detección de estos ataques.

No recomendamos activar la protección contra suplantación de MAC en máquinas virtuales en la infraestructura de Microsoft Hyper-V. Debido a las características específicas de la plataforma Microsoft Hyper-V, Kaspersky Industrial CyberSecurity for Nodes puede bloquear el hipervisor debido a resultados falsos positivos.

Cómo configurar Protección frente a amenazas en la red por tipo en la Consola de administración (MMC)

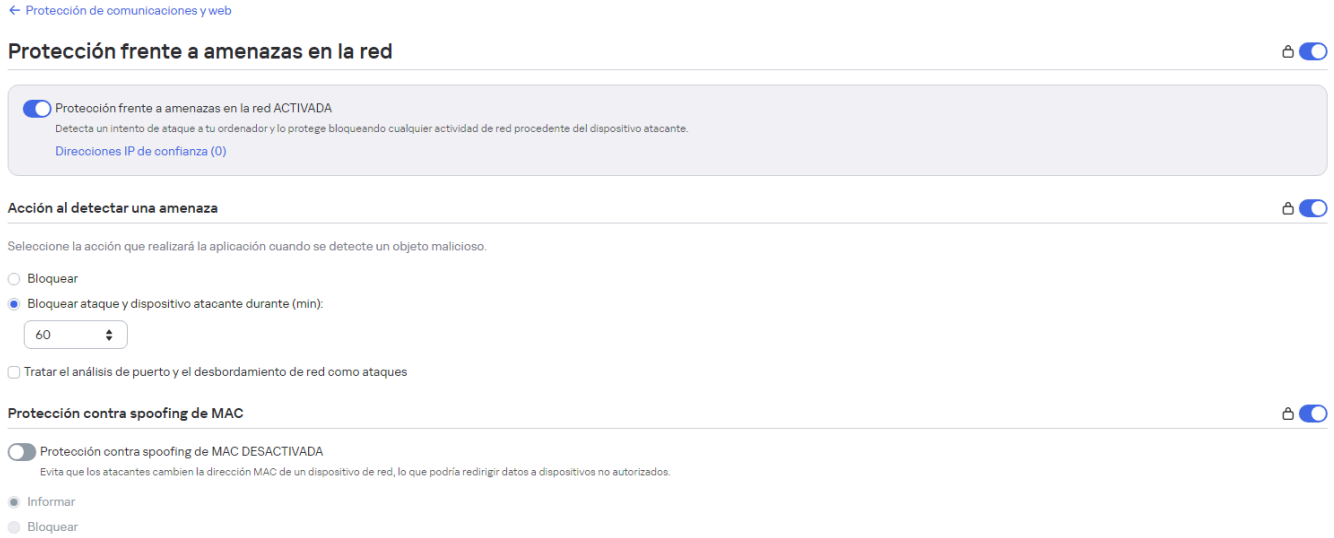
1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.
4. Utilice la casilla **Tratar el análisis de puerto y el desbordamiento de red como ataques** para activar o desactivar la detección de estos ataques.

   Si esta función está activada, Kaspersky Endpoint Security supervisa el tráfico de red en busca de análisis de puertos y ataques de inundación de red. Si se detecta uno de estos comportamientos, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación proporciona información sobre el equipo que realiza las solicitudes. Esta información es necesaria para una ofrecer respuesta oportuna. Sin embargo, Kaspersky Endpoint Security no bloquea el equipo que realiza las solicitudes, porque dicho tráfico puede ser algo normal en la red corporativa.
5. En el bloque **Modo de protección contra spoofing de MAC**, seleccione una de las opciones siguientes:
   - **No detectar spoofing de MAC**.
   - **Informar**.
   - **Bloquear**.
6. Guarde los cambios.

Cómo configurar Protección frente a amenazas en la red por tipo en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección de comunicaciones y web → Protección frente a amenazas en la red**.



Parámetros de Protección frente a amenazas en la red

5. Utilice la casilla **Tratar el análisis de puerto y el desbordamiento de red como ataques** para activar o desactivar la detección de estos ataques.

   Si esta función está activada, Kaspersky Endpoint Security supervisa el tráfico de red en busca de análisis de puertos y ataques de inundación de red. Si se detecta uno de estos comportamientos, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación proporciona información sobre el equipo que realiza las solicitudes. Esta información es necesaria para una ofrecer respuesta oportuna. Sin embargo, Kaspersky Endpoint Security no bloquea el equipo que realiza las solicitudes, porque dicho tráfico puede ser algo normal en la red corporativa.

6. En **Protección contra spoofing de MAC**, configure la detección de ataques de spoofing de MAC:

   a. Utilice el interruptor **Protección contra spoofing de MAC ACTIVADA** para activar o desactivar la detección de estos ataques.

   b. Seleccione la acción que se realizará cuando se detecte un ataque de spoofing de MAC:

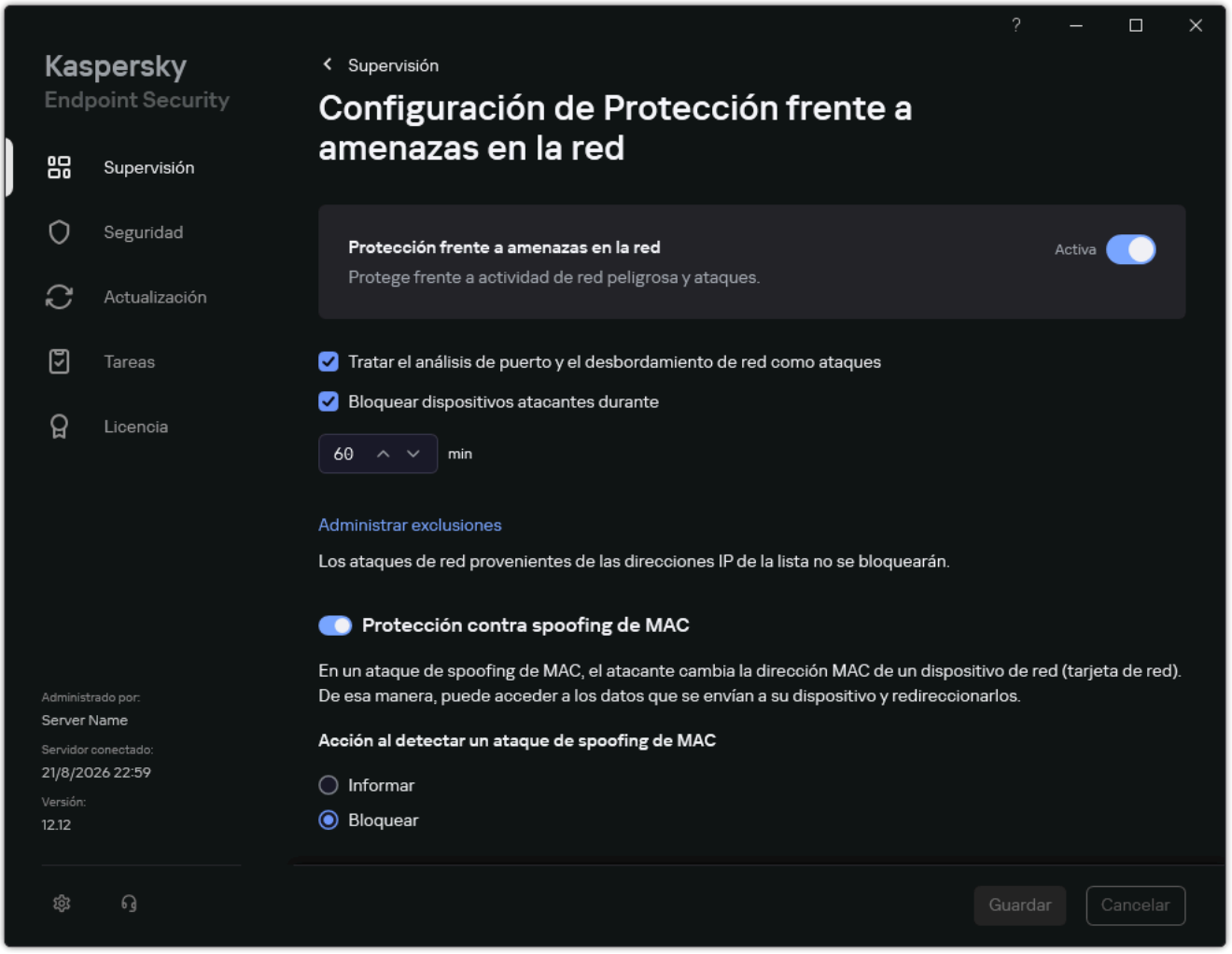
      - **Informar**.
      - **Bloquear**.

7. Guarde los cambios.

Cómo configurar Protección frente a amenazas en la red por tipo en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Protección frente a amenazas en la red**.



Parámetros de Protección frente a amenazas en la red

3. Utilice el interruptor **Tratar el análisis de puerto y el desbordamiento de red como ataques** para activar o desactivar la detección de estos ataques.

   Si esta función está activada, Kaspersky Endpoint Security supervisa el tráfico de red en busca de análisis de puertos y ataques de inundación de red. Si se detecta uno de estos comportamientos, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación proporciona información sobre el equipo que realiza las solicitudes. Esta información es necesaria para una ofrecer respuesta oportuna. Sin embargo, Kaspersky Endpoint Security no bloquea el equipo que realiza las solicitudes, porque dicho tráfico puede ser algo normal en la red corporativa.

4. Utilice el interruptor **Protección contra spoofing de MAC** para activar o desactivar la detección de estos ataques.

5. En el bloque **Acción al detectar un ataque de spoofing de MAC**, seleccione una de las opciones siguientes:

   - **Informar**.
   - **Bloquear**.

6. Guarde los cambios.

Firewall

El componente Firewall bloquea las conexiones no autorizadas a un equipo mientras se trabaja en Internet o en una red local. Firewall también controla la actividad de red de las aplicaciones en el equipo. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. De forma automática, el firewall crea las reglas de red necesarias para que funcionen la aplicación y el Agente de red. Como resultado, el firewall abre varios puertos en el equipo. Los puertos se abren según la función del equipo (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en el equipo, consulte la Ayuda de Kaspersky Security Center.

Reglas de red

Puede configurar las reglas de la red en los siguientes niveles:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones a los paquetes de red, con independencia de la aplicación. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security tiene reglas de paquetes de red predefinidas con permisos recomendados por los expertos de Kaspersky.
- *Reglas de red de la aplicación*. Las reglas de red de la aplicación imponen restricciones sobre la actividad de red de una aplicación concreta. No solo influyen en las características del paquete de red, sino también en la aplicación concreta a la que va dirigida la aplicación concreta o que emitió este paquete de red.

El componente Prevención de intrusiones en el host proporciona el acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de *derechos de aplicación*.

Durante el primer inicio de la aplicación, Firewall realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

   Se le recomienda participar en Kaspersky Security Network para ayudar a Firewall a trabajar con más eficacia.
3. Coloca la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima*, *No fiable*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la configuración del componente Prevención de intrusiones en el host. Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea la actividad de red de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza *Restricción máxima* se les niega el uso de cualquier conexión de red.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. Si se añade actividad de red a varias reglas, Firewall regula la actividad de red en función de la regla con la prioridad más alta.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si tanto las reglas de paquetes de red como las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se gestiona de acuerdo con las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan de una manera especial. La regla para aplicaciones de la red incluye reglas de acceso en función del estado de la red: *Red pública*, *Red local*, *Red de confianza*. Por ejemplo, a las aplicaciones del grupo de confianza *Restricción máxima* se les niega cualquier actividad de red en redes de cualquier estado de manera predeterminada. Si se especifica una regla de red para una aplicación individual (aplicación principal), los subprocesos de otras aplicaciones se ejecutarán de acuerdo con la regla de red de la aplicación principal. Si no hay una regla de red para la aplicación, los subprocesos se ejecutarán de acuerdo con la regla de acceso a la red del grupo de confianza de la aplicación.

Por ejemplo, ha prohibido cualquier actividad de red en redes de todos los estados para todas las aplicaciones, excepto el navegador X. Si inicia la instalación del navegador Y (subproceso) desde el navegador X (aplicación principal), el instalador del navegador Y accederá a la red y descargará los archivos necesarios. Después de la instalación, se negarán las conexiones de red al navegador Y de acuerdo con la configuración del Firewall. Para prohibir la actividad de red del instalador del navegador Y como un subproceso, debe asignar una regla de red para el instalador del navegador Y.

Tipos de conexión de red

Firewall le permite controlar la actividad de la red en función del tipo de conexión de red. Kaspersky Endpoint Security recibe el tipo de conexión de red del sistema operativo del equipo. El tipo de conexión de red en el sistema operativo lo establece el usuario al configurar la conexión. Puede cambiar el tipo de conexión de red en la configuración de Kaspersky Endpoint Security. Firewall supervisará la actividad de la red en función del tipo de red especificado en la configuración de Kaspersky Endpoint Security, y no en del sistema operativo.

Están disponibles los siguientes tipos de conexión de red:

- **Red pública**. La red no está protegida por aplicaciones antivirus, firewalls ni filtros (como la red wifi de una cafetería). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos a través de carpetas compartidas y acceso remoto al escritorio de este ordenador. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.

  Firewall asigna el tipo *Red pública* a Internet de forma predeterminada. No se puede cambiar el tipo de Internet.

- **Red local**. Red para usuarios con acceso restringido a archivos e impresoras en este ordenador (por ejemplo, para una LAN corporativa o una red doméstica).

- **Red de confianza**. Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.

Compatibilidad con Firewall de Windows Defender

El sistema operativo tiene su propio Firewall integrado: *Firewall de Windows Defender*. La aplicación se comporta de forma diferente según el tipo de sistema operativo:

- **Estación de trabajo**. El uso de Kaspersky Firewall y Firewall de Windows Defender de forma simultánea puede provocar errores en el funcionamiento del sistema operativo. Por lo tanto, Kaspersky Endpoint Security dispone de un mecanismo que impide el uso simultáneo de ambos Firewalls. Al activar Kaspersky Firewall, el sistema operativo desactiva automáticamente Firewall de Windows Defender. Al desactivar Kaspersky Firewall, el sistema operativo vuelve a activar automáticamente Firewall de Windows Defender para mantener protegido el equipo.

- **Servidor**. Kaspersky Firewall y Firewall de Windows Defender son incompatibles entre sí. El instalador de Kaspersky Endpoint Security elimina automáticamente Firewall de Windows Defender al instalar la aplicación.

Activación y desactivación de Firewall

De forma predeterminada, Firewall está activado y las opciones en el modo óptimo.

Cómo activar o desactivar Firewall en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Firewall**.
4. Utilice la casilla de verificación **Firewall** para activar o desactivar el componente.
5. Guarde los cambios.

Cómo activar o desactivar Firewall en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Protección de comunicaciones y web** → **Firewall**.
5. Utilice interruptor **Firewall ACTIVADO** para activar o desactivar el componente.
6. Guarde los cambios.

Cómo activar o desactivar Firewall en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Utilice interruptor **Firewall** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si se activa el Firewall, Kaspersky Endpoint Security controla la actividad de la red y bloquea las conexiones de red no autorizadas a su equipo, y también bloquea la actividad de red no autorizada de las aplicaciones en su equipo. El componente Protección frente a amenazas en la red también controla la actividad de red. El componente Protección frente a amenazas en la red (también denominado Intrusion Detection System, IDS) supervisa el tráfico de red entrante en busca de actividad característica de los ataques de red.

Kaspersky Endpoint Security registra los eventos de ataques de red en sus informes, independientemente de la configuración del Firewall. Incluso si el Firewall bloquea la conexión de red utilizando reglas para así evitar un ataque de red, el componente Protección frente a amenazas en la red registra los eventos de ataque de red. Esto es necesario para generar información estadística acerca de los ataques de red en los equipos de su organización.

Modificación del tipo de conexión de red

Firewall asigna el tipo *Red pública* a Internet de forma predeterminada. No se puede cambiar el tipo de Internet.

Para cambiar el tipo de la conexión de red:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en **Redes disponibles**.
4. Seleccione la conexión de red cuyo tipo quiere cambiar.

5. En la columna **Tipo de red**, seleccione el tipo de conexión de red:

   - **Red pública**. La red no está protegida por aplicaciones antivirus, firewalls ni filtros (como la red wifi de una cafetería). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos a través de carpetas compartidas y acceso remoto al escritorio de este ordenador. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.

   - **Red local**. Red para usuarios con acceso restringido a archivos e impresoras en este ordenador (por ejemplo, para una LAN corporativa o una red doméstica).

   - **Red de confianza**. Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.

6. Guarde los cambios.

Gestión de las reglas de paquetes de red

Puede realizar las siguientes acciones mientras gestiona las reglas de paquetes de red:

- Crear una nueva regla de paquetes de red.

  Puede crear una nueva regla de paquetes de red mediante la creación de un conjunto de condiciones y acciones que se aplican a los paquetes de red y los flujos de datos.

- Activar o desactivar una regla de paquetes de red.

  Todas las reglas de paquetes de red creadas por Firewall tienen el estado *Activado* de forma predeterminada. Cuando una regla de paquetes de red está activada, Firewall aplica esta regla.

  Puede desactivar cualquier regla de paquetes de red que esté seleccionada en la lista de reglas de paquetes de red. Cuando una regla de paquetes de red está desactivada, Firewall deja de aplicar temporalmente esta regla.

  > Con el estado *Activado*, se añade de forma predeterminada una nueva regla de paquetes de red personalizada a la lista de reglas de paquetes de red.

- Modificar los parámetros de una regla de paquetes de red ya existente.

  Tras crear una nueva regla de paquetes de red, siempre puede volver a modificar sus parámetros y modificarlos si es necesario.

- Cambiar la acción de Firewall para una regla de paquetes de red.

  En la lista de reglas de paquetes de red, puede modificar la acción que Firewall realiza para detectar la actividad de red que cumple con una regla de paquetes de red concreta.

- Cambiar la prioridad de una regla de paquetes de red.

  Puede incrementar o reducir la prioridad de una regla de paquetes de red que esté seleccionada en la lista.

- Eliminar una regla de paquetes de red.

  Puede eliminar una regla de paquetes de red para que Firewall deje de aplicar esta regla cuando detecte actividad de red y para que esta regla no se muestre en la lista de reglas de paquetes de red con el estado *Desactivado*.

Crear una regla de paquetes de red

El firewall filtra toda la actividad de red en el equipo de acuerdo con las reglas de paquetes de red. Las reglas de paquetes de red contienen condiciones (por ejemplo, dirección, protocolo) que el firewall aplica para controlar las conexiones de red del equipo. Las reglas de paquetes de red también especifican la acción que realiza el firewall con la conexión que coincide con la regla (permitir o bloquear la conexión).

Recomendaciones para crear reglas de paquetes de red

Puede especificar una dirección IP o un rango de direcciones IP para filtrar la actividad de la red. También puede especificar un nombre DNS.

Si se utiliza un nombre DNS en una regla, Kaspersky Endpoint Security resuelve este nombre DNS en una dirección IP y, posteriormente, trata la regla como si se hubiera especificado dicha dirección IP en ella.

Kaspersky Endpoint Security puede resolver nombres DNS en los siguientes casos:

- Inicio de la aplicación
- Cambio de la configuración de Firewall

Cuando la aplicación resuelve nombres DNS desde el equipo en el que está instalada, se puede realizar un gran número de consultas al servidor DNS. Para evitarlo, recomendamos utilizar direcciones IP en lugar de nombres DNS al crear reglas.

En algunos casos, el uso de nombres DNS en los nombres de paquetes de red puede no ser seguro porque el propietario del servidor DNS puede modificar los parámetros del registro DNS. Un actor malintencionado también puede falsificar mensajes DNS y eludir las reglas del firewall.

Puede controlar las conexiones de red por nombres DNS usando reglas de Control web. Si necesita especificar un nombre DNS en las reglas del firewall:

- Garantice la seguridad de la LAN corporativa.
- Garantice la seguridad del almacenamiento en caché y los servidores DNS autorizados.
- Active la protección del registro de DNS contra modificaciones.

Al crear reglas de paquetes de red, recuerde que estas tienen prioridad sobre las reglas para aplicaciones.

Métodos para crear reglas de paquetes de red

Puede crear una regla de paquetes de red de las siguientes maneras:

- Utilice la herramienta Monitor de red.

  Monitor de red es una herramienta diseñada para la visualización de información sobre la actividad de la red del equipo de un usuario en tiempo real. Esto es conveniente porque no es necesario configurar todos los parámetros de las reglas. Algunos parámetros del Firewall se insertarán automáticamente a partir de los datos del Monitor de red. El Monitor de red está disponible solo en la interfaz de la aplicación.

- Configure los parámetros del Firewall.

  Esto le permite ajustar la configuración del Firewall. Puede crear reglas para cualquier actividad de la red, aunque no haya actividad de red en el momento dado.

Cómo utilizar la herramienta Monitor de red para crear una regla de paquete de red en la interfaz de la aplicación

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.
2. Vaya a la pestaña **Actividad de la red**.

   La pestaña **Actividad de la red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes.
3. En el menú contextual de una conexión de red, seleccione **Crear una regla de paquete de red**.

   Se abren las propiedades de la regla de red.
4. Configure el estado **Activo** para la regla del paquete.
5. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
6. Configure los parámetros de la regla de red (consulte la tabla a continuación).

   Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de la regla de red se completará automáticamente.
7. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.
8. Haga clic en **Guardar**.

   La nueva regla de red se añadirá a la lista.
9. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de red.
10. Guarde los cambios.

Cómo usar la configuración del Firewall para crear una regla de paquetes de red en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.

3. Haga clic en **Reglas para paquetes**.

   Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.

4. Usando la lista desplegable **Añadir**, seleccione la ubicación de la regla en la lista: en la parte superior de la lista, en la parte inferior de la lista o junto a la regla seleccionada.

   La posición de la regla en la lista determina la prioridad de la regla. La regla situada en la parte superior de la lista tiene la máxima prioridad.

5. Configure el estado **Activo** para la regla del paquete.

6. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.

7. Configure los parámetros de la regla de red (consulte la tabla a continuación).

   Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de la regla de red se completará automáticamente.

8. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.

9. Haga clic en **Guardar**.

   La nueva regla de red se añadirá a la lista.

10. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de red.

11. Guarde los cambios.

Cómo crear una regla de paquetes de red en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Firewall**.

4. En el bloque **Configuración del Firewall**, haga clic en el botón **Configuración**.

   Se abre la lista de reglas de paquetes de red y la lista de reglas de red de la aplicación.

5. Vaya a la pestaña **Reglas de paquetes de red**.

   Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.

6. Usando la lista desplegable **Añadir**, seleccione la ubicación de la regla en la lista: en la parte superior de la lista, en la parte inferior de la lista o junto a la regla seleccionada.

   La posición de la regla en la lista determina la prioridad de la regla. La regla situada en la parte superior de la lista tiene la máxima prioridad.

7. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.

8. Configure los parámetros de la regla de red (consulte la tabla a continuación).

   Puede seleccionar una plantilla de regla predeterminada haciendo clic en el botón . Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de la regla de red se completará automáticamente.

9. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.

10. Guarde la nueva regla de red.

11. Utilice los botones **Subir**/**Bajar** para establecer la prioridad de la regla de red.

12. Guarde los cambios.

El Firewall controlará los paquetes de red de acuerdo con la regla. Puede desactivar una regla de paquete de la operación del Firewall sin eliminarla de la lista. Para hacerlo, desactive la casilla de verificación junto al objeto.

Cómo crear una regla de paquetes de red en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione **Protección de comunicaciones y web** → **Firewall**.

5. Seleccione la pestaña **Reglas de paquetes de red**.

   Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.

6. Haga clic en **Añadir**.

   Esto abre el formulario para una nueva regla de red.

7. Introduzca manualmente el nombre del servicio de red en el campo **Nombre de la regla**.

8. Configure los parámetros de la regla de red (consulte la tabla a continuación).

   Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Seleccionar plantilla de reglas**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de la regla de red se completará automáticamente.

9. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.

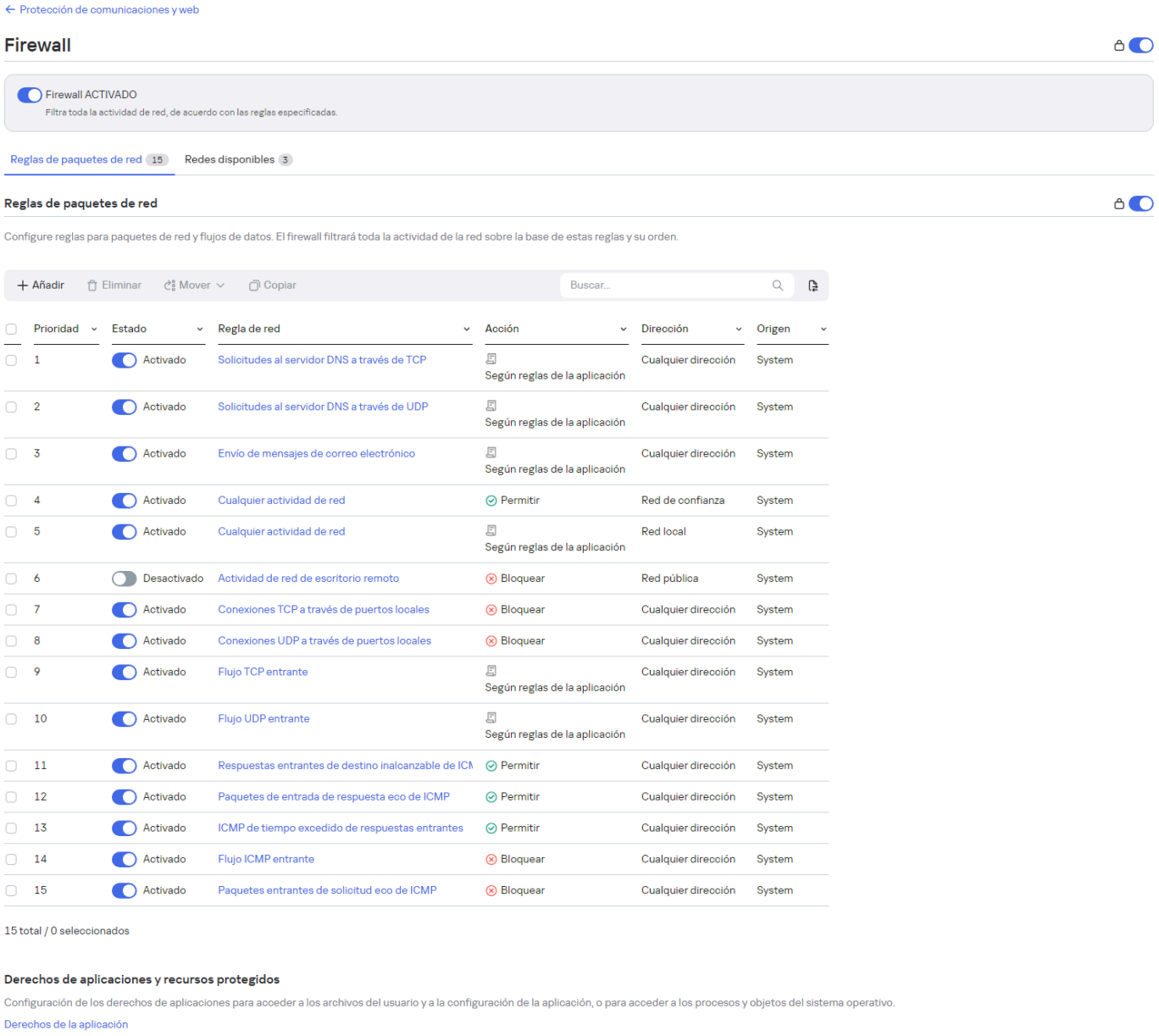
10. Guarde la nueva regla de red.

    La nueva regla de red se añadirá a la lista.

11. Utilice el botón **Mover** para establecer la prioridad de la regla de red.

12. Guarde los cambios.

El Firewall controlará los paquetes de red de acuerdo con la regla. Puede desactivar una regla de paquete de la operación del Firewall sin eliminarla de la lista. Utilice el interruptor de la columna **Estado** para activar o desactivar la regla de paquetes.



Reglas de paquetes de Firewall

Configuración de reglas de paquetes de red

Parámetro	Descripción
Acción	**Permitir**. **Bloquear**. **Por reglas de la aplicación**. Si se selecciona esta opción, Firewall aplica las reglas de red de la aplicación a la conexión de red.
Protocolo	Controle la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE. Si se seleccionan ICMP o ICMPv6 como el protocolo, puede definir el código y el tipo de paquete ICMP. Si se selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto de los equipos local y remoto entre los que se debe supervisar la conexión. Intervalo de valores posibles para los números de puerto: 0-65535. En cada campo puede introducir varios valores separados por `,` o especificar un rango de valores usando `-`. Por ejemplo: • `100,101` • `100-130` • `100,110-130`

Parámetro	Descripción
Dirección	**Entrante (paquete)**. El Firewall aplica la regla de red a todos los paquetes de red entrantes. **Entrante**. Firewall aplica la regla de red a todos los paquetes de red enviados por medio de una conexión iniciada por un equipo remoto. **Entrante/Saliente**. El Firewall aplica la regla de red a todos los paquetes de red entrantes y salientes. **Saliente (paquete)**. El Firewall aplica la regla de red a todos los paquetes de red salientes. **Saliente**. El Firewall aplica la regla de red a todos los paquetes de red enviados mediante una conexión de red iniciada por el equipo del usuario.
Adaptadores de red	Adaptadores de red que pueden enviar o recibir paquetes de red. Especificar la configuración de los adaptadores de red permite distinguir entre los paquetes de red enviados o recibidos por los adaptadores de red con direcciones IP idénticas.
Período de vida (TTL)	Limitar el control de los paquetes de red por su vida útil (Time to Live, TTL).
Direcciones remotas	Direcciones de red de los equipos remotos que puedan enviar y recibir paquetes de red. El Firewall aplica una regla de red al rango especificado de direcciones de la red remota. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP, especificar un rango de direcciones IP o seleccionar una subred (redes de confianza, redes locales, redes públicas). También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web. Si en la regla del paquete de red ha añadido un nombre DNS para el que no se ha podido determinar la dirección IP, Kaspersky Endpoint Security mostrará una advertencia. En la lista de reglas de paquetes de red de Web Console, se añade una columna con una descripción del error. En la Consola de administración (MMC), la descripción del error no está disponible. Estas reglas de paquetes se resaltan en color.
Direcciones locales	Direcciones de red de los equipos que puedan enviar o recibir paquetes de red. Firewall aplica una regla de la red al rango especificado de direcciones de red local. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP o especificar un rango de direcciones IP. La aplicación almacena direcciones locales solo si se especifica una lista de direcciones remotas. Es decir, se ha seleccionado el valor **Direcciones de la lista** para **Direcciones remotas** y se ha añadido al menos una dirección. En ocasiones, la dirección local no se puede obtener para las aplicaciones. Si este es el caso, este parámetro se ignora.

Activación o desactivación de una regla de paquetes de red

Para activar o desactivar una regla de paquetes de red:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.
3. Haga clic en **Reglas para paquetes**.
   Esto abre una lista de reglas de paquetes de red predeterminadas, definidas por el componente Firewall.
4. Seleccione la regla de los paquetes de red pertinente en la lista.
5. Utilice el interruptor en la columna **Estado** para activar o desactivar la regla.
6. Guarde los cambios.

Modificación de la acción de Firewall para una regla de paquetes de red

Para cambiar la acción de Firewall que se aplica a una regla de paquetes de red:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.
3. Haga clic en **Reglas para paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminadas, definidas por el componente Firewall.
4. Selecciónela en la lista de reglas de paquetes de red y haga clic en el botón **Editar**.
5. En la lista desplegable **Acción**, seleccione la acción que debe realizar Firewall cuando detecte este tipo de actividad de red:

   - **Permitir**.
   - **Bloquear**.
   - **Por reglas de la aplicación**. Si se selecciona esta opción, Firewall aplica las reglas de red de la aplicación a la conexión de red.
6. Guarde los cambios.

Modificación de la prioridad de una regla de paquetes de red

La prioridad de una regla de paquetes de red viene determinada por su posición en la lista de reglas de paquetes de red. La regla de paquetes de red situada más arriba en la lista de reglas de paquetes de red tiene la máxima prioridad.

Cada una de las reglas de paquetes de red creadas manualmente se añade al final de la lista de reglas de paquetes de red y tienen la menor prioridad.

Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba abajo. En función de cada una de las reglas de paquetes de red procesadas que se aplican a una determinada conexión de red, Firewall permite o bloquea el acceso de red a la dirección y al puerto especificados en la configuración de esta conexión de red.

Para modificar la prioridad de la regla de paquetes de red:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.
3. Haga clic en **Reglas para paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminadas, definidas por el componente Firewall.
4. En la lista, seleccione la regla de paquetes de red cuya prioridad quiere cambiar.

5. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de red.

6. Guarde los cambios.

Exportación e importación de reglas de paquetes de red

Puede exportar la lista de reglas de paquetes de red a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de reglas del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de paquetes de red o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de reglas de paquetes de red en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas → Firewall**.

4. En el bloque **Configuración del Firewall**, haga clic en el botón **Configuración**.

   Se abre la lista de reglas de paquetes de red y la lista de reglas de red de la aplicación.

5. Vaya a la pestaña **Reglas de paquetes de red**.

6. Para exportar la lista de reglas de paquetes de red:

   a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.

   b. Haga clic en el enlace **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.

7. Para importar una lista de reglas de paquetes de red:

   a. Haga clic en el enlace **Importar**.

      En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

8. Guarde los cambios.

Cómo exportar e importar una lista de reglas de paquetes de red en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Protección de comunicaciones y web** → **Firewall**.
5. Para exportar la lista de reglas, en el bloque **Reglas de paquetes de red**:

   a. Seleccione las reglas que quiera exportar.

   b. Haga clic en el botón → **Exportar**.

   Kaspersky Endpoint Security exporta la lista de reglas a un archivo JSON en la carpeta de descargas predeterminada.
6. Para importar la lista de reglas, en el bloque **Reglas de paquetes de red**:

   a. Haga clic en el botón → **Importar**.

   En la ventana que se abre, seleccione el archivo JSON del que desea importar la lista de reglas.

   b. Abra el archivo.

   Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.
7. Guarde los cambios.

Definir reglas de paquetes de red en XML

Firewall permite exportar reglas de paquetes de red en formato XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de reglas del mismo tipo.

El archivo XML contiene dos nodos principales: `Rules` y `Resources`. El nodo `Rules` enumera reglas de paquetes de red. Este nodo contiene reglas configuradas de forma predeterminada (*reglas predefinidas*) y reglas añadidas por el usuario (*reglas personalizadas*).

Marcado de reglas de paquetes de red

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Parámetro	Descripción	Valor
`<key name="0000">`	Prioridad de la regla. Cuanto menor sea el valor, mayor será la prioridad.	Entero El valor de la prioridad debe constar de cuatro dígitos. Los nodos del archivo XML deben ordenarse por valor de prioridad, comenzando por `0000`.
`RuleId`	ID de la regla.	**Reglas predefinidas** `100`: **Solicitudes al servidor DNS a través de TCP**. `101`: **Solicitudes al servidor DNS a través de UDP**. `102`: **Envío de mensajes de correo electrónico**. `110`: **Cualquier actividad de red** (Redes de confianza). `125`: **Cualquier actividad de red** (Redes locales). `130`: **Actividad de red de escritorio remoto**. `131`: **Conexiones TCP a través de puertos locales**. `132`: **Conexiones UDP a través de puertos locales**. `133`: **Flujo TCP entrante**. `134`: **Flujo UDP entrante**. `137`: **Respuestas entrantes de destino inalcanzable de ICMP**. `138`: **Paquetes de entrada de respuesta eco de ICMP**. `140`: **ICMP de tiempo excedido de respuestas entrantes**. `142`: **Flujo ICMP entrante**. `266`: **Paquetes entrantes de solicitud eco de ICMPv6**.
`RuleState`	Estado de la regla.	`0`: regla predefinida desactivada `1`: regla predefinida activada `2`: regla personalizada desactivada `3`: regla personalizada activada
`RuleTypeId`	ID del tipo de regla.	`4`: regla de paquete de red.
`AppIdEx`	ID de la aplicación a la que pertenece la regla de paquete de red.	Si la regla no pertenece a ninguna aplicación, el valor es `0`.
`ResIdEx`	ID principal del recurso con configuración de reglas. Puede usar este identificador para ubicar un bloque con configuración de reglas en el nodo `Resources`.	Entero
`ResIdEx2`	ID del tipo de red.	`0`: **Cualquier dirección**. `50`: **Redes de confianza**. `51`: **Redes locales**. `52`: **Redes públicas**. `<Network Identifier>`: **Direcciones de la lista** (las direcciones se definen manualmente).
`AccessFlag`	Valor del parámetro **Acción**.	`0`: **Permitir**. `2`: **Según reglas de la aplicación**. `3`: **Bloquear**. `4`: **Permitir** y **Registrar eventos**. `6`: **Según reglas de la aplicación** y **Registrar eventos**. `7`: **Bloquear** y **Registrar eventos**.
`</key>`		

El nodo `Resources` contiene configuraciones de reglas de paquetes de red. Las configuraciones de las reglas de paquetes de red personalizadas se enumeran en el bloque `<key name="0004">`.

Marcado de reglas de paquetes de red personalizadas

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Configuración de reglas de paquetes de red personalizadas

Parámetro	Descripción	Valor
`<key name="Data">`	ID del bloque de parámetros.	Entero
`RemotePorts`	Valor del parámetro **Puertos remotos**.	Lista de rangos de puertos remotos.
`LocalPorts`	Valor del parámetro **Puertos locales**.	Lista de rangos de puertos locales.

Parámetro	Descripción	Valor
`AdapterBindings`	Valor del parámetro **Adaptadores de red**.	`IpAddresses`: valor del parámetro **Direcciones IP**. `MacAddresses`: valor del parámetro **Direcciones MAC**. `AdapterName`: nombre del adaptador de red. `InterfaceType`: valor del parámetro **Tipo de interfaz**: • `0`: **Otro**. • `1`: **LoopBack**. • `2`: **Red cableada (Ethernet)**. • `3`: **Red inalámbrica (wifi)**. • `4`: **Túnel**. • `5`: **Conexión PPP**. • `6`: **Conexión PPPoE**. • `7`: **Conexión VPN**. • `8`: **Conexión por módem**.
`unique`	ID interno de la estructura.	Entero Se recomienda no cambiar este parámetro.
`Proto`	Valor del parámetro **Protocolo**.	`0`: desactivado. `1`: **ICMP**. `2`: **IGMP**. `6`: **TCP**. `17`: **UDP**. `47`: **GRE**. `58`: **ICMPv6**.
`Direction`	Valor del parámetro **Dirección**.	`1`: **Entrante (paquete)**. `2`: **Saliente (paquete)**. `3`: **Entrante/Saliente**. `4`: **Entrante**. `5`: **Saliente**.

Parámetro	Descripción	Valor
`IcmpType`	Valor del parámetro **Tipo de ICMP**.	**Protocolo ICMP** `0`: **Respuesta de eco** (ICMP) o desactivado. `3`: **No se puede alcanzar el destino** (ICMP). `4`: **Apagado de la fuente**. `5`: **Redirigir**. `6`: **Alternar dirección host**. `8`: **Solicitud de eco**. `9`: **Anuncio de enrutador**. `10`: **Solicitud de enrutador**. `11`: **Tiempo excedido**. `12`: **Problema de parámetros**. `13`: **Marca de tiempo**. `14`: **Respuesta de marca de tiempo**. `15`: **Solicitud de información**. `16`: **Respuesta de información**. `17`: **Solicitud de máscara de dirección**. `18`: **Respuesta de máscara de dirección**. `30`: **Traceroute**. `31`: **Error de conversión de datagrama**. `32`: **Redirección de host móvil**. `33`: **IPv6 Where-Are-You**. `34`: **IPv6 I-Am-Here**. `35`: **Solicitud de registro móvil**. `36`: **Respuesta de registro móvil**. `37`: **Solicitud de nombre de dominio**. `38`: **Respuesta de nombre de dominio**. `40`: **Photuris**. **Protocolo ICMPv6** `1`: **No se puede alcanzar el destino**. `2`: **Paquete demasiado grande**. `3`: **Tiempo excedido**. `4`: **Problema de parámetros**. `128`: **Solicitud de eco**. `129`: **Respuesta de eco**. `130`: **Consulta de escucha de multidifusión**. `131`: **Informe de escucha de multidifusión**. `132`: **Escucha de multidifusión terminada**. `133`: **Solicitud de enrutador**. `134`: **Anuncio de enrutador**. `135`: **Solicitud de vecino**. `136`: **Aviso de vecino**. `137`: **Redirigir mensaje**. `138`: **Renumeración de enrutador**. `139`: **Consulta de información del nodo ICMP**. `141`: **Mensaje inverso de solicitud de descubrimiento de vecino**. `142`: **Mensaje inverso de aviso de descubrimiento de vecino**. `143`: **Informe de escucha de multidifusión, versión 2**.

Parámetro	Descripción	Valor
		`144`: **Mensaje inicial de solicitud de descubrimiento de dirección de agente**. `145`: **Mensaje inicial de respuesta de descubrimiento de dirección de agente**. `146`: **Solicitud de prefijo móvil**. `147`: **Aviso de prefijo móvil**. `148`: **Mensaje de solicitud de ruta de certificación**. `149`: **Mensaje de aviso de ruta de certificación**. `151`: **Anuncio de enrutador de multidifusión**. `152`: **Solicitud de enrutador de multidifusión**. `153`: **Terminación de enrutador de multidifusión**.
`IcmpCode`	Valor del parámetro **Código ICMP**.	`0`: **Código 0** o desactivado. `1`: **Código 1**. `2`: **Código 2**.
`Flags`	Puntero de atributos de estructura.	Entero Se recomienda no cambiar este parámetro.
`TTL`	Valor del parámetro **Período de vida (TTL)**.	Valor en segundos. Si está desactivado, el valor es `0`.
`</key>`		
`Id`	ID principal del recurso (consulte el nodo `Rules`).	Entero
`ParentID`	ID del grupo principal.	Entero Se recomienda no cambiar este parámetro.
`Flags`	Estado de la regla.	`6`: regla desactivada. `38`: regla activada.
`Name`	Nombre de la regla de paquete de red.	Cadena

Gestionar reglas de red de la aplicación

De forma predeterminada, Kaspersky Endpoint Security agrupa todas las aplicaciones que están instaladas en el equipo por el nombre del proveedor del software cuyo archivo o actividad de red monitoriza. Los grupos de aplicaciones, a su vez, se clasifican en grupos de confianza. Todas las aplicaciones y grupos de aplicaciones heredan las propiedades de su grupo principal: reglas de control de aplicaciones, reglas de red de la aplicación y su prioridad de ejecución.

Al igual que el componente de Prevención de intrusiones en el host, el componente Firewall aplica de forma predeterminada las reglas de red para un grupo de aplicaciones cuando filtra la actividad de red de todas las aplicaciones del grupo. El grupo de aplicaciones define los derechos de las aplicaciones dentro del grupo a acceder a diferentes conexiones de red.

De forma predeterminada, Firewall crea un conjunto de reglas de red para cada grupo de aplicaciones que Kaspersky Endpoint Security detecta en el equipo. Puede cambiar la acción que Firewall aplica a las reglas de red del grupo de aplicaciones que se crean de forma predeterminada. No puede modificar, eliminar, desactivar o cambiar la prioridad de las reglas de red del grupo de aplicaciones que se crean de forma predeterminada.

También puede crear una regla de red para una aplicación individual. Tal regla tendrá una prioridad más alta que la regla de red del grupo al cual la aplicación pertenece.

Crear una regla de red de aplicaciones

De manera predeterminada, la actividad de las aplicaciones se controlada a través de reglas de red definidas para el grupo de confianza al que Kaspersky Endpoint Security asignó la aplicación en el primer inicio. Si es necesario, puede crear reglas de red para un grupo de confianza completo, para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza.

Las reglas de red definidas manualmente tienen una prioridad más alta que las reglas de red que se determinaron para un grupo de confianza. En otras palabras, si las reglas de aplicación definidas manualmente difieren de las reglas de aplicación determinadas para un grupo de confianza, el Firewall controla la actividad de la aplicación de acuerdo con las reglas definidas en forma manual para las aplicaciones.

De forma predeterminada, el Firewall crea las siguientes reglas de red para cada aplicación:

- Cualquier actividad de red en redes de confianza.
- Cualquier actividad de red en redes locales.
- Cualquier actividad de red en redes públicas.

Kaspersky Endpoint Security controla la actividad de red de las aplicaciones de acuerdo con las reglas de red predefinidas de la siguiente manera:

- Fiable y Restricción mínima: se permite toda la actividad de red.
- Restricción máxima y No fiable: toda la actividad de la red está bloqueada.

Las reglas de aplicación predefinidas no se pueden editar ni eliminar.

Puede crear una regla de red para aplicación de las siguientes formas:

- Utilice la herramienta Monitor de red.

  Monitor de red es una herramienta diseñada para la visualización de información sobre la actividad de la red del equipo de un usuario en tiempo real. Esto es conveniente porque no es necesario configurar todos los parámetros de las reglas. Algunos parámetros del Firewall se insertarán automáticamente a partir de los datos del Monitor de red. El Monitor de red está disponible solo en la interfaz de la aplicación.

- Configure los parámetros del Firewall.

  Esto le permite ajustar la configuración del Firewall. Puede crear reglas para cualquier actividad de la red, aunque no haya actividad de red en el momento dado.

Al crear reglas de red para aplicaciones, recuerde que las reglas de paquetes de red tienen prioridad sobre las reglas de red de la aplicación.

Cómo utilizar la herramienta Monitor de red para crear una regla de red para aplicación en la interfaz de la aplicación

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.
2. Vaya a la pestaña **Actividad de la red** o **Puertos abiertos**.

   La pestaña **Actividad de la red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes.

   La pestaña **Puertos abiertos** muestra todos los puertos de red abiertos del equipo.
3. En el menú contextual de una conexión de red, seleccione **Cree una regla de red para la aplicación**.

   Se abre la ventana de propiedades y reglas de la aplicación.
4. Seleccione la pestaña **Reglas de red**.

   Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
5. Haga clic en **Añadir**.

   Se abren las propiedades de la regla de red.
6. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (consulte la tabla a continuación).

   Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de la regla de red se completará automáticamente.
8. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.
9. Haga clic en **Guardar**.

   La nueva regla de red se añadirá a la lista.
10. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de red.
11. Guarde los cambios.

Cómo utilizar la configuración del Firewall para crear una regla de red para aplicación en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.

3. Haga clic en **Reglas para aplicaciones**.

   Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere crear una regla de red.

5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la pestaña **Reglas de red**.

7. Haga clic en **Añadir**.

   Se abren las propiedades de la regla de red.

8. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.

9. Configure los parámetros de la regla de red (consulte la tabla a continuación).

   Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de la regla de red se completará automáticamente.

10. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.

11. Haga clic en **Guardar**.

    La nueva regla de red se añadirá a la lista.

12. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de red.

13. Guarde los cambios.

Cómo crear una regla de red para aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Firewall**.

4. En el bloque **Configuración del Firewall**, haga clic en el botón **Configuración**.

   Se abre la lista de reglas de paquetes de red y la lista de reglas de red de la aplicación.

5. Vaya a la pestaña **Reglas de red de la aplicación**.

6. Haga clic en **Añadir**.

7. En la ventana que se abre, introduzca los criterios de búsqueda para la aplicación para la que quiera crear una regla de red.

   Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres * y ? al introducir una máscara.

8. Haga clic en **Actualizar**.

   Kaspersky Endpoint Security buscará la aplicación en la lista consolidada de aplicaciones instaladas en equipos administrados. Kaspersky Endpoint Security mostrará una lista de aplicaciones que coincidan con sus criterios de búsqueda.

9. Seleccione la aplicación pertinente.

10. En la lista desplegable **Añadir aplicación seleccionada al grupo de confianza**, seleccione **Grupos predeterminados** y haga clic en **Aceptar**.

    La aplicación se añadirá al grupo predeterminado.

11. Seleccione la aplicación correspondiente y luego seleccione **Derechos de la aplicación** en el menú contextual de la aplicación.

    Se abre la ventana de propiedades y reglas de la aplicación.

12. Seleccione la pestaña **Reglas de red**.

    Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.

13. Haga clic en **Añadir**.

    Se abren las propiedades de la regla de red.

14. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.

15. Configure los parámetros de la regla de red (consulte la tabla a continuación).

    Puede seleccionar una plantilla de regla predeterminada haciendo clic en el botón . Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de la regla de red se completará automáticamente.

16. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.

17. Guarde la nueva regla de red.

18. Utilice los botones **Subir**/**Bajar** para establecer la prioridad de la regla de red.

19. Guarde los cambios.

Cómo crear una regla de red para aplicación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione **Protección de comunicaciones y web** → **Firewall**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de la aplicación**.

   Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.

6. Vaya a la pestaña **Derechos de la aplicación**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.

7. En el bloque **Aplicaciones**, haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir una aplicación a un grupo de confianza.

8. Seleccione el grupo de confianza correspondiente para la aplicación.

9. Seleccione el tipo **Aplicación**. Ir al paso siguiente.

   Si desea crear una regla de red para varias aplicaciones, seleccione el tipo **Grupo** y defina un nombre para el grupo de aplicaciones.

10. En la lista de aplicaciones abiertas, seleccione las aplicaciones para las que quiere crear una regla de red.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

11. Finalice el asistente.

    La aplicación se añadirá al grupo de confianza.

12. En la parte izquierda de la ventana, seleccione la aplicación relevante.

13. En la parte derecha de la ventana, seleccione **Reglas de red** en la lista desplegable.

    Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.

14. Haga clic en **Añadir**.

    Se abren las propiedades de la regla de aplicaciones.

15. Introduzca manualmente el nombre del servicio de red en el campo **Nombre de la regla**.

16. Configure los parámetros de la regla de red (consulte la tabla a continuación).

    Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Seleccionar plantilla de reglas**. Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de la regla de red se completará automáticamente.

17. Si desea que las acciones de la regla de red se reflejen en el informe, seleccione la casilla de verificación **Registrar eventos**.

18. Guarde la nueva regla de red.

    La nueva regla de red se añadirá a la lista.

19. Utilice el botón **Mover** para establecer la prioridad de la regla de red.

20. Guarde los cambios.

Parámetro	Descripción
Acción	**Permitir**. **Bloquear**.
Protocolo	Controle la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE. Si se seleccionan ICMP o ICMPv6 como el protocolo, puede definir el código y el tipo de paquete ICMP. Si se selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto de los equipos local y remoto entre los que se debe supervisar la conexión. Intervalo de valores posibles para los números de puerto: 0-65535. En cada campo puede introducir varios valores separados por `,` o especificar un rango de valores usando `-`. Por ejemplo: • `100,101` • `100-130` • `100,110-130`
Dirección	**Entrante**. **Entrante/Saliente**. **Saliente**.
Direcciones remotas	Direcciones de red de los equipos remotos que puedan enviar y recibir paquetes de red. El Firewall aplica una regla de red al rango especificado de direcciones de la red remota. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP, especificar un rango de direcciones IP o seleccionar una subred (redes de confianza, redes locales, redes públicas). También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web. Si en la regla del paquete de red ha añadido un nombre DNS para el que no se ha podido determinar la dirección IP, Kaspersky Endpoint Security mostrará una advertencia. En la lista de reglas de paquetes de red de Web Console, se añade una columna con una descripción del error. En la Consola de administración (MMC), la descripción del error no está disponible. Estas reglas de paquetes se resaltan en color.
Direcciones locales	Direcciones de red de los equipos que puedan enviar o recibir paquetes de red. Firewall aplica una regla de la red al rango especificado de direcciones de red local. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP o especificar un rango de direcciones IP. La aplicación almacena direcciones locales solo si se especifica una lista de direcciones remotas. Es decir, se ha seleccionado el valor **Direcciones de la lista** para **Direcciones remotas** y se ha añadido al menos una dirección. En ocasiones, la dirección local no se puede obtener para las aplicaciones. Si este es el caso, este parámetro se ignora.

Activar y desactivar una regla de red de la aplicación

Para activar o desactivar una regla de red de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.
3. Haga clic en **Reglas para aplicaciones**.
   Esto abre la lista de reglas de la aplicación.
4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere crear o editar una regla de red.
5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.
   Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la pestaña **Reglas de red**.

7. En la lista de reglas de red para un grupo de aplicaciones, seleccione la regla de red pertinente.

   Se abre la ventana de propiedades de la regla de red.

8. Configure el estado **Activo** o **Inactivo** de la regla de red.

   No puede desactivar una regla de red del grupo de aplicaciones que Firewall haya creado de forma predeterminada.

9. Guarde los cambios.

Modificación de la acción de Firewall para una regla de red de la aplicación

Puede cambiar la acción de Firewall que se aplica a las reglas de red para una aplicación o grupo de aplicaciones creado de forma predeterminada y cambiar la acción de Firewall por una única regla de red del grupo de aplicaciones personalizada.

Para cambiar la acción del Firewall sobre todas las reglas de red para una aplicación o grupo de aplicaciones:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.

3. Haga clic en **Reglas para aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. Si desea cambiar la acción del Firewall que se aplica a todas las reglas de red que se crean de forma predeterminada, seleccione una aplicación o grupo de aplicaciones de la lista. Las reglas de red creadas manualmente no se cambian.

5. Haga clic derecho para abrir el menú contextual, seleccione **Reglas de red** y luego seleccione la acción que desea asignar:

   - **Heredar**.
   - **Permitir**.
   - **Bloquear**.

6. Guarde los cambios.

Para cambiar la respuesta de Firewall para las reglas de red de una aplicación o un grupo de aplicaciones:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.

3. Haga clic en **Reglas para aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. En la lista, seleccione la aplicación o el grupo de aplicaciones para las cuales desea cambiar la acción para una regla de red.

5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la pestaña **Reglas de red**.

7. Seleccione la regla de red para la cual desea cambiar la acción del Firewall.

8. En la columna **Permiso**, haga clic con el botón derecho para acceder al menú contextual y seleccione la acción que quiere asignar:

   - **Heredar**.
   - **Permitir**.
   - **Rechazar**.
   - **Registrar eventos**.

9. Guarde los cambios.

Modificación de la prioridad de una regla de red de la aplicación

La prioridad de una regla de red depende de su posición en la lista de reglas. Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de red, de arriba abajo. En función de cada una de las reglas de red aplicables a una determinada conexión de red, Firewall permite o bloquea el acceso a la red a la dirección y al puerto indicados en la configuración de esta conexión de red.

Las reglas de red creadas manualmente tienen una prioridad más alta que las reglas de red predeterminadas.

No puede cambiar la prioridad de las reglas de red del grupo de aplicaciones que se crean de forma predeterminada.

Para cambiar la prioridad de una regla de red:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas → Firewall**.

3. Haga clic en **Reglas para aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere cambiar la prioridad de una regla de red.

5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la pestaña **Reglas de red**.

7. Seleccione la conexión de red cuya prioridad quiera cambiar.

8. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de red.

9. Guarde los cambios.

Monitor de red

Monitor de red es una herramienta diseñada para la visualización de información sobre la actividad de la red del equipo de un usuario en tiempo real.

Para iniciar el Monitor de red:

En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.

Se abre la ventana Monitor de red. En esta ventana, se muestra información sobre la actividad de red del equipo en cuatro pestañas:

- La pestaña **Actividad de la red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes. En esta pestaña, también puede crear reglas de paquetes de red para el funcionamiento del Firewall.
- La pestaña **Puertos abiertos** muestra todos los puertos de red abiertos del equipo. En esta pestaña, también puede crear reglas de paquetes de red y reglas de aplicación para el funcionamiento del Firewall.
- La pestaña **Tráfico de red** muestra el volumen de tráfico de red entrante y saliente entre el equipo del usuario y otros equipos de la red a los que el usuario está conectado actualmente.
- La pestaña **Equipos bloqueados** incluye las direcciones IP de los equipos remotos cuya actividad de red ha bloqueado el componente Protección frente a amenazas en la red después de detectar intentos de ataques de red desde dichas direcciones IP.

Prevención de exploits

El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para hacerlo, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malicioso. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

El componente Prevención de exploits también supervisa los puertos de red en busca de procesos de aplicaciones que puedan poner en peligro la seguridad del equipo. La aplicación obtiene información sobre dichos procesos con bases de datos antivirus.

Activación y desactivación de Prevención de vulnerabilidades

De forma predeterminada, Prevención de exploits está activada y las opciones en el modo óptimo. Kaspersky Endpoint Security monitoriza los archivos ejecutables que usan las aplicaciones vulnerables. Si Kaspersky Endpoint Security detecta que se ha ejecutado un archivo ejecutable desde una aplicación vulnerable por otra persona distinta del usuario, Kaspersky Endpoint Security realizará la acción seleccionada (por ejemplo, bloqueará la operación).

Cómo activar o desactivar Prevención de exploits en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Prevención de exploits**.
4. Utilice la casilla de verificación **Prevención de exploits** para activar o desactivar el componente.
5. Seleccione la acción correspondiente en el bloque **Al detectar vulnerabilidades**:
   - **Bloquear**. Si este elemento está seleccionado, al detectar una vulnerabilidad de seguridad, Kaspersky Endpoint Security bloquea el funcionamiento de la vulnerabilidad y crea una entrada de registro con información relevante.
   - **Informar**. Si este elemento está seleccionado, cuando Kaspersky Endpoint Security detecte una vulnerabilidad registrará un evento que contenga información sobre la vulnerabilidad y añadirá información sobre esta vulnerabilidad a la lista de amenazas activas.
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar Prevención de exploits en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Análisis de comportamiento → Prevención de exploits**.
5. Utilice interruptor **Prevención de exploits** para activar o desactivar el componente.

6. Seleccione la acción correspondiente en el bloque **Acción al detectar una amenaza**:

   - **Bloquear**. Si este elemento está seleccionado, al detectar una vulnerabilidad de seguridad, Kaspersky Endpoint Security bloquea el funcionamiento de la vulnerabilidad y crea una entrada de registro con información relevante.

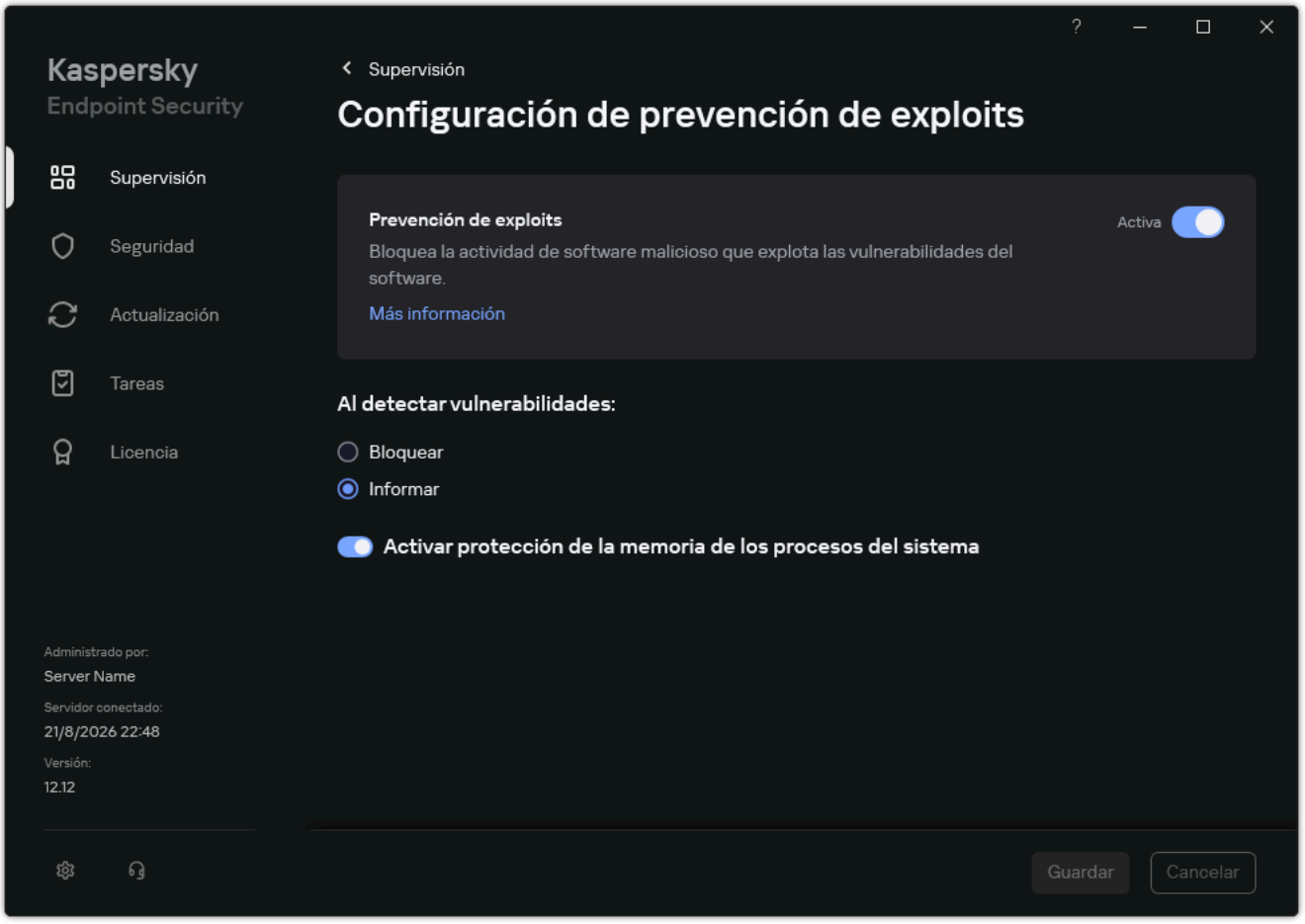
   - **Informar**. Si este elemento está seleccionado, cuando Kaspersky Endpoint Security detecte una vulnerabilidad registrará un evento que contenga información sobre la vulnerabilidad y añadirá información sobre esta vulnerabilidad a la lista de amenazas activas.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar Prevención de exploits en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Prevención de exploits**.



Configuración de prevención de exploits

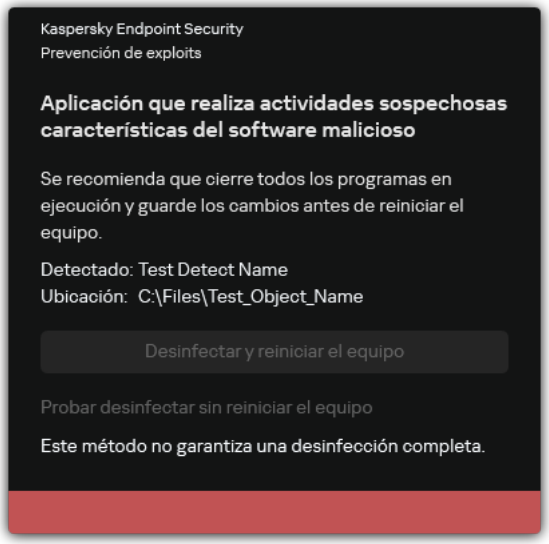
3. Utilice interruptor **Prevención de exploits** para activar o desactivar el componente.

4. Seleccione la acción correspondiente en el bloque **Al detectar vulnerabilidades**:

   - **Bloquear**. Si este elemento está seleccionado, al detectar una vulnerabilidad de seguridad, Kaspersky Endpoint Security bloquea el funcionamiento de la vulnerabilidad y crea una entrada de registro con información relevante.

   - **Informar**. Si este elemento está seleccionado, cuando Kaspersky Endpoint Security detecte una vulnerabilidad registrará un evento que contenga información sobre la vulnerabilidad y añadirá información sobre esta vulnerabilidad a la lista de amenazas activas.

5. Guarde los cambios.



Notificación sobre amenazas activas

Protección de la memoria de los procesos del sistema

De forma predeterminada, la protección de la memoria de procesos del sistema está activada. Kaspersky Endpoint Security bloquea los procesos externos que intentan acceder a los procesos del sistema.

Cómo activar o desactivar la protección de la memoria de los procesos del sistema en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de exploits**.

4. Utilice la casilla de verificación **Activar protección de la memoria de los procesos del sistema** para activar o desactivar la opción.

5. Guarde los cambios.

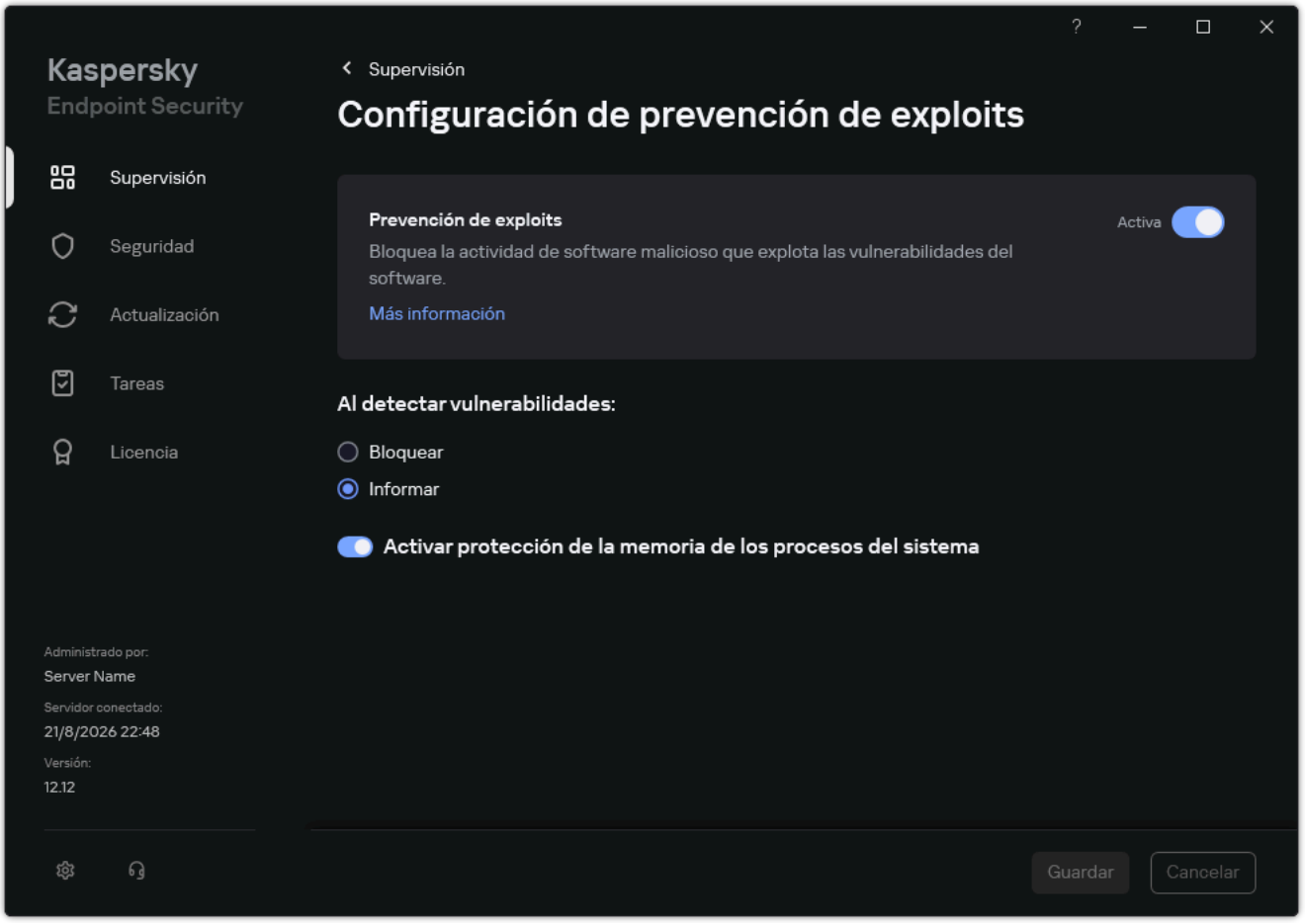
Cómo activar o desactivar la protección de la memoria de los procesos del sistema en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Análisis de comportamiento** → **Prevención de exploits**.
5. Utilice el interruptor **Protección de la memoria de los procesos del sistema ACTIVADA** para activar o desactivar esta función.
6. Guarde los cambios.

Cómo activar o desactivar la protección de la memoria de los procesos del sistema en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de exploits**.



Configuración de prevención de exploits

3. Utilice el interruptor **Activar protección de la memoria de los procesos del sistema** para activar o desactivar esta función.
4. Guarde los cambios.

Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones de su equipo y ofrece esta información a otros componentes de protección mejorar su rendimiento. El componente Detección de comportamientos utiliza firmas de patrones de actividad peligrosa (Behavior stream signatures, BSS) para aplicaciones. Si la actividad de la aplicación coincide con una BSS Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security se basa en bases de datos de reglas heurísticas ofrece protección proactiva al equipo.

El componente Detección de comportamiento también supervisa los puertos de red en busca de procesos de aplicaciones que puedan poner en peligro la seguridad del equipo. La aplicación obtiene información sobre dichos procesos con bases de datos antivirus.

De forma predeterminada, la Detección de comportamiento está activada y se ejecuta en el modo recomendado por los expertos de Kaspersky. Cuando se detecta actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación maliciosa.

No se recomienda desactivar la Detección de Comportamiento a menos que sea absolutamente necesario porque reduce la eficacia de los componentes de protección. Los componentes de protección pueden solicitar datos obtenidos por el componente Detección de comportamiento para detectar amenazas.

Cómo activar o desactivar Detección de comportamiento en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Detección de comportamiento**.
5. Utilice la casilla de verificación **Detección de comportamiento** para activar o desactivar el componente.
6. Seleccione la acción correspondiente en el bloque **Acción al detectar actividad de software malicioso**:
   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.
   - **Bloquear**. Si se selecciona este elemento, al detectar una actividad maliciosa, Kaspersky Endpoint Security termina la aplicación.
   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware, Kaspersky Endpoint Security añade información sobre la actividad maliciosa de la aplicación a la lista de amenazas activas.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar Detección de comportamiento en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

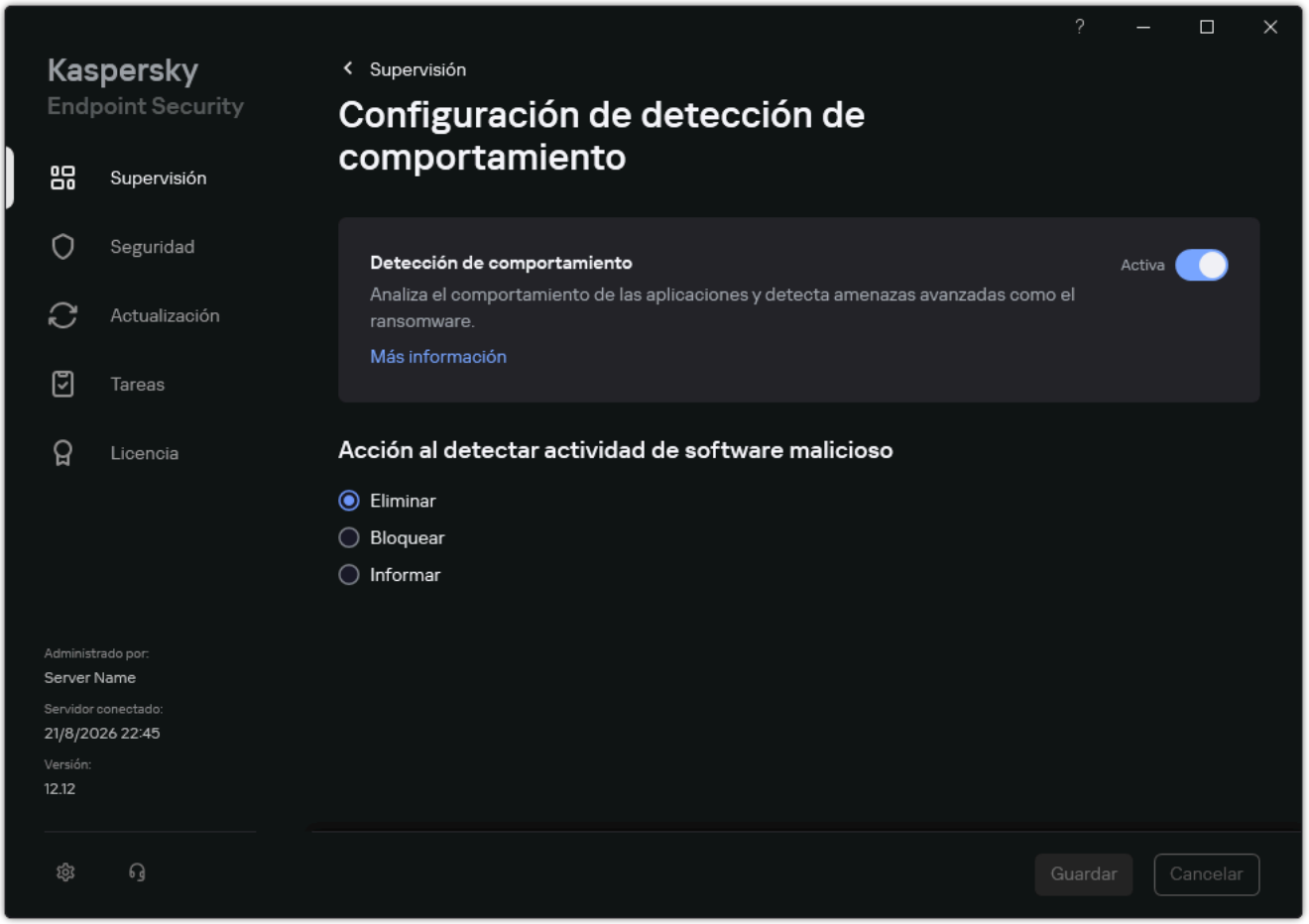
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Análisis de comportamiento → Detección de comportamiento**
5. Utilice interruptor **Detección de comportamiento ACTIVADA** para activar o desactivar el componente.
6. Seleccione la acción correspondiente en el bloque **Acción al detectar una amenaza**:

   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.
   - **Bloquear**. Si se selecciona este elemento, al detectar una actividad maliciosa, Kaspersky Endpoint Security termina la aplicación.
   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware, Kaspersky Endpoint Security añade información sobre la actividad maliciosa de la aplicación a la lista de amenazas activas.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar Detección de comportamiento en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Detección de comportamiento**.



Configuración de detección de comportamiento

3. Utilice interruptor **Detección de comportamiento** para activar o desactivar el componente.

4. Seleccione la acción correspondiente en el bloque **Acción al detectar actividad de software malicioso**:

   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.

   - **Bloquear**. Si se selecciona este elemento, al detectar una actividad maliciosa, Kaspersky Endpoint Security termina la aplicación.

   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware, Kaspersky Endpoint Security añade información sobre la actividad maliciosa de la aplicación a la lista de amenazas activas.

5. Guarde los cambios.

Como resultado, si la Detección de comportamiento está activada, Kaspersky Endpoint Security utilizará firmas de flujo de comportamiento para analizar la actividad de las aplicaciones en el sistema operativo.

Anti-Cryptor

A partir de Kaspersky Endpoint Security 12.12 para Windows, la protección de las carpetas compartidas contra el cifrado externo que solía ser parte del componente Detección de comportamiento es un componente independiente, Anti-Cryptor.

El componente solo supervisa operaciones con los archivos ubicados en dispositivos de almacenamiento con el sistema de archivos NTFS y que no están cifrados con el sistema EFS.

El componente Anti-Cryptor analiza la actividad en las carpetas compartidas. Si esta actividad coincide con un tipo de comportamiento típico del cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.

Para que el componente Anti-Cryptor funcione, debe activar el componente Detección de comportamiento.

Si Kaspersky Endpoint Security detecta un intento de modificar los archivos de las carpetas compartidas, realiza las siguientes acciones:

- Bloquea el acceso a la modificación de archivos en la sesión que ha iniciado la actividad maliciosa (el archivo será de solo lectura).
- Crea copias de seguridad de los archivos que se están modificando.
- Añade una entrada a informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.
- Además, si el componente Motor de reparación está activado, Kaspersky Endpoint Security restaura los archivos modificados desde las copias de seguridad.

Activación y desactivación de la protección de carpetas compartidas frente al cifrado externo

De forma predeterminada, la protección de las carpetas compartidas contra el cifrado externo está activada y funciona según las recomendaciones de los expertos de Kaspersky. Para configurar esta función, puede crear una cobertura de protección y configurar exclusiones, si es necesario. De forma predeterminada, la aplicación identifica automáticamente las carpetas compartidas y supervisa la actividad de los archivos en todas las carpetas. Cuando se detecta un intento de cifrar externamente archivos en carpetas compartidas, Kaspersky Endpoint Security bloquea la sesión del usuario remoto durante una hora (de forma predeterminada).

Después de instalar Kaspersky Endpoint Security, la protección de carpetas compartidas contra el cifrado externo estará limitada hasta que el equipo se reinicie.

Cómo activar o desactivar la protección de las carpetas compartidas contra el cifrado externo en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Anti-Cryptor**.
4. Utilice la casilla **Anti-Cryptor** para activar o desactivar la detección de actividad típica del cifrado externo.
5. Seleccione la acción pertinente que llevará a cabo la aplicación cuando se detecte un intento de modificar archivos en carpetas compartidas:
   - **Bloquear conexión durante N minutos**. Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar archivos en carpetas compartidas, bloquea el acceso a la modificación del archivo para la sesión que ha iniciado la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación está activado y la opción **Bloquear conexión durante N minutos** está seleccionada, se restauran los archivos modificados a partir de las copias de seguridad.

   - **Informar**. Si se selecciona esta opción, al detectar un intento de modificar archivos de carpetas compartidas, Kaspersky Endpoint Security añade información sobre este intento a la lista de amenazas activas, añade una entrada a informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.
6. Si es necesario, edite una cobertura de protección y defina exclusiones.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar la protección de las carpetas compartidas contra el cifrado externo en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Análisis de comportamiento** → **Anticifrado**.
5. Utilice el interruptor **Anticifrado ACTIVADO** para activar o desactivar la detección de actividad típica del cifrado externo.

6. Seleccione la acción pertinente que llevará a cabo la aplicación cuando se detecte un intento de modificar archivos en carpetas compartidas:

   - **Bloquear conexión durante (min) N minutos**. Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar archivos en carpetas compartidas, bloquea el acceso a la modificación del archivo para la sesión que ha iniciado la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación está activado y la opción **Bloquear conexión durante (min) N minutos** está seleccionada, se restauran los archivos modificados a partir de las copias de seguridad.

   - **Informar**. Si se selecciona esta opción, al detectar un intento de modificar archivos de carpetas compartidas, Kaspersky Endpoint Security añade información sobre este intento a la lista de amenazas activas, añade una entrada a informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.

7. Si es necesario, edite una cobertura de protección y defina exclusiones.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar la protección de las carpetas compartidas contra el cifrado externo en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Anti-Cryptor**.

3. Utilice la casilla **Protección de carpetas compartidas frente a cifrado externo** para activar o desactivar la detección de actividad típica del cifrado externo.

4. Utilice la casilla **Protección de carpetas compartidas frente a cifrado externo** para activar o desactivar la detección de actividad típica del cifrado externo.

5. Seleccione la acción pertinente que llevará a cabo la aplicación cuando se detecte un intento de modificar archivos en carpetas compartidas:

   - **Bloquear conexión durante (min) N minutos**. Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar archivos en carpetas compartidas, bloquea el acceso a la modificación del archivo para la sesión que ha iniciado la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación está activado y la opción **Bloquear conexión durante (min) N minutos** está seleccionada, se restauran los archivos modificados a partir de las copias de seguridad.

   - **Informar**. Si se selecciona esta opción, al detectar un intento de modificar archivos de carpetas compartidas, Kaspersky Endpoint Security añade información sobre este intento a la lista de amenazas activas, añade una entrada a informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.

6. Si es necesario, edite una cobertura de protección y defina exclusiones.

7. Guarde los cambios.

Configuración del período de bloqueo de un equipo que no es de confianza

Un *equipo que no es de confianza* es un equipo remoto que está realizando una actividad maliciosa o cifrando datos. De forma predeterminada, Kaspersky Endpoint Security bloquea la sesión del usuario remoto durante una hora. Cuando el período de bloqueo expira, Kaspersky Endpoint Security elimina el equipo de la lista de bloqueo y restaura el acceso a la carpeta compartida.

Cómo configurar el período de bloqueo de un equipo que no es de confianza en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Anti-Cryptor**.
4. En el bloque **Acción al detectar una amenaza**, seleccione **Bloquear conexión durante N min**.
5. Configure el período de bloqueo de un equipo que no sea de confianza y que esté participando en una actividad maliciosa o cifrando de datos.
6. Guarde los cambios.

Cómo configurar el período de bloqueo de un equipo que no es de confianza en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Análisis de comportamiento → Anticifrado**.
5. En **Acción al detectar una amenaza**, configure el período de bloqueo de un equipo que no sea de confianza y que esté participando en una actividad maliciosa o cifrando de datos.
6. Guarde los cambios.

Cómo configurar el período de bloqueo de un equipo que no es de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Anti-Cryptor**.
3. En el bloque **Acción al detectar una amenaza**, seleccione **Bloquear conexión durante (min)**.

4. Configure el período de bloqueo de un equipo que no sea de confianza y que esté participando en una actividad maliciosa o cifrando de datos.

5. Guarde los cambios.

Como resultado, el equipo remoto se bloqueará. Para desbloquear el equipo remoto, puede reiniciar Kaspersky Endpoint Security.

Edición de la cobertura de protección

La *cobertura de protección* es una lista de rutas a carpetas compartidas en las que Kaspersky Endpoint Security supervisa la actividad de los archivos. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. De forma predeterminada, la aplicación identifica automáticamente las carpetas compartidas y supervisa la actividad de los archivos en todas las carpetas.

Excluir una carpeta de la cobertura de protección puede reducir el número de falsos positivos si su organización usa cifrado de datos al intercambiar archivos mediante carpetas compartidas. Por ejemplo, la Detección de comportamiento puede arrojar falsos positivos si el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Esta actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, añada dicha carpeta a las exclusiones.

> También puede excluir equipos de los que no se deban gestionar intentos de cifrado externos.

Cómo editar una cobertura de protección en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Anti-Cryptor**.

4. En el bloque **Cobertura de protección**, seleccione **Solo las carpetas compartidas especificadas**.

5. En la lista de carpetas, haga clic en **Añadir**.

6. Se abre una ventana; en ella, introduzca la ruta a la carpeta compartida que desea incluir en la cobertura de protección (por ejemplo, `C:\Share`).

   > Para agregar una carpeta compartida a la cobertura de protección, use una ruta de acceso local.

7. Haga clic en **Aceptar**.

8. Si es necesario, defina las exclusiones de la cobertura de protección:

   a. En el bloque **Exclusiones del análisis**, haga clic en el botón **Por máscara**.

   b. En la ventana que se abre, haga clic en el botón **Añadir**.

c. En la ventana que aparece, especifique una extensión de archivo en formato `*.<file extension>` o una ruta de carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

La aplicación no admite algunas extensiones de archivo de exclusión. Por lo tanto, puede especificar una exclusión como `*.docx` o `**\Folder\**`.

Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura de la protección. Para hacerlo, desactive la casilla de verificación junto al objeto.

9. Guarde los cambios.

Cómo editar una cobertura de protección en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Análisis de comportamiento** → **Anticifrado**.
5. En el bloque **Cobertura de protección**, seleccione **Solo las carpetas compartidas especificadas**.
6. En la lista de carpetas, haga clic en **Añadir**.
7. Se abre una ventana; en ella, introduzca la ruta a la carpeta compartida que desea incluir en la cobertura de protección (por ejemplo, `C:\Share`).

   Para agregar una carpeta compartida a la cobertura de protección, use una ruta de acceso local.
8. Haga clic en **Aceptar**.
9. Si es necesario, defina las exclusiones de la cobertura de protección:

   a. En la parte superior de la ventana, haga clic en el vínculo **Exclusiones del análisis**.

   b. En la ventana que se abre, haga clic en el botón **Añadir**.

   c. En la ventana que aparece, especifique una extensión de archivo en formato `*.<file extension>` o una ruta de carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

   La aplicación no admite algunas extensiones de archivo de exclusión. Por lo tanto, puede especificar una exclusión como `*.docx` o `**\Folder\**`.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura de la protección. Para hacerlo, desactive la casilla de verificación junto al objeto.
10. Guarde los cambios.

Cómo editar una cobertura de protección en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Anti-Cryptor**.

3. En el bloque **Cobertura de protección**, seleccione **Solo las carpetas compartidas especificadas**.

4. En la lista de carpetas, haga clic en **Añadir**.

5. Se abre una ventana; en ella, introduzca la ruta a la carpeta compartida que desea incluir en la cobertura de protección (por ejemplo, `C:\Share`).

   Para agregar una carpeta compartida a la cobertura de protección, use una ruta de acceso local.

6. Haga clic en **Aceptar**.

7. Si es necesario, defina las exclusiones de la cobertura de protección:

   a. En la parte superior de la ventana, haga clic en el vínculo **Exclusiones por máscara**.

   b. En la ventana que se abre, haga clic en el botón **Añadir**.

   c. En la ventana que aparece, especifique una extensión de archivo en formato `*.<file extension>` o una ruta de carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

      La aplicación no admite algunas extensiones de archivo de exclusión. Por lo tanto, puede especificar una exclusión como `*.docx` o `**\Folder\**`.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura de la protección. Para hacerlo, desactive la casilla de verificación junto al objeto.

8. Guarde los cambios.

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.

3. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.

4. Haga clic en **Añadir**.

5. Haga clic en **Examinar** y seleccione la carpeta compartida.

También puede ingresar la ruta manualmente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `?:\Users\*\Folder\`.

6. En el bloque **Componentes de protección**, seleccione el componente **Detección de comportamiento**.

7. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

8. Seleccione el estado **Activo** para la exclusión.

   Puede utilizar el interruptor para detener una exclusión en cualquier momento.

9. Guarde los cambios.

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Zona de confianza**.

5. En la ventana que se abre, haga clic en el vínculo **Exclusiones del análisis antimalware**.

6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.

7. Seleccione la casilla de verificación **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si se desmarca esta casilla, Kaspersky Endpoint Security ocultará la lista consolidada de exclusiones del análisis en la interfaz de usuario de la aplicación.

8. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una exclusión del análisis a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva exclusión de análisis a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *exclusiones de análisis predefinidas*. También se han añadido exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar exclusiones del análisis predefinidas según el propósito del servidor protegido.

9. Seleccione cómo desea añadir la exclusión **Ruta al archivo o carpeta**.

10. Introduzca la ruta a la carpeta compartida.

    También puede ingresar la ruta manualmente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara:

    - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
    - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

    Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `C:\Users\*\Folder\`.

11. En el bloque **Aplicar exclusión a**, seleccione el componente **Detección de comportamiento**.

12. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

13. Seleccione el estado **Añadir a exclusiones** para la exclusión.

    Puede utilizar el interruptor para detener una exclusión en cualquier momento.

14. Guarde los cambios.

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
4. En el bloque **Exclusiones de análisis y aplicaciones de confianza → Exclusiones del análisis**, haga clic en el botón **Configuración**.

   Esto abre una ventana que incluye una lista de exclusiones.

5. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.
6. Seleccione la casilla de verificación **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si se desmarca esta casilla, Kaspersky Endpoint Security ocultará la lista consolidada de exclusiones del análisis en la interfaz de usuario de la aplicación.

7. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una exclusión del análisis a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva exclusión de análisis a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *exclusiones de análisis predefinidas*. También se han añadido exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar exclusiones del análisis predefinidas según el propósito del servidor protegido.

8. Haga clic en **Añadir**.
9. En el bloque **Propiedades**, seleccione la casilla de verificación **Archivo o carpeta**.
10. Haga clic en el enlace **Seleccionar archivo o carpeta** del bloque **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para modificarlos)** para abrir la ventana **Nombre de archivo o carpeta**.
11. Haga clic en **Examinar** y seleccione la carpeta compartida.

También puede ingresar la ruta manualmente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `?:\Users\*\Folder\`.

12. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

13. Haga clic en el enlace del bloque **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para modificarlos)** para abrir la ventana **Componentes de protección**.

14. Active la casilla ubicada junto al componente **Detección de comportamiento**.

15. Guarde los cambios.

Adición de equipos de confianza para el cifrado de datos externos

Si su organización utiliza cifrado de datos externos en su flujo de trabajo de intercambio de archivos, debe crear una lista de equipos de confianza. Kaspersky Endpoint Security no supervisa el cifrado de datos por parte de equipos de confianza.

El servicio Auditar inicio de sesión debe estar habilitado para permitir que las exclusiones de direcciones protejan las carpetas compartidas del cifrado externo. De forma predeterminada, el servicio Auditar inicio de sesión está desactivado (para obtener información detallada sobre la activación del servicio Auditar inicio de sesión, visite el sitio web de Microsoft).

La funcionalidad para excluir direcciones de la protección de carpetas compartidas no funciona en un equipo remoto si este está encendido antes de que se inicie Kaspersky Endpoint Security. Puede reiniciar este equipo remoto después de que se inicie Kaspersky Endpoint Security para asegurarse de que la funcionalidad para excluir direcciones de la protección de carpetas compartidas funcione en este equipo remoto.

Cómo agregar un equipo de confianza para el cifrado de datos externos en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Anti-Cryptor**.
5. En el bloque **Exclusiones del análisis**, haga clic en el botón **Por nombre o dirección IP**.
6. En la ventana que se abre, haga clic en el botón **Por nombre o dirección IP**.
7. Introduzca la dirección IP, el rango de direcciones IP o los nombres de los equipos desde los que no se deben gestionar los intentos de cifrado externos.

   Ejemplos:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir un equipo de confianza para el cifrado externo de datos en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Zona de confianza**.
5. En la parte derecha de la ventana, haga clic en el vínculo **Exclusiones de Anti-Cryptor**.
6. En la ventana que se abre, haga clic en el botón **Añadir**.
7. Introduzca la dirección IP, el rango de direcciones IP o los nombres de los equipos desde los que no se deben gestionar los intentos de cifrado externos.

   Ejemplos:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo agregar un equipo de confianza para el cifrado de datos externos en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Anti-Cryptor**.
3. En la parte superior de la ventana, haga clic en el vínculo **Exclusiones por nombre o dirección IP**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. Introduzca la dirección IP, el rango de direcciones IP o los nombres de los equipos desde los que no se deben gestionar los intentos de cifrado externos.

   Ejemplos:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. Guarde los cambios.

Exportar e importar una lista de exclusiones a la protección de carpetas compartidas frente a cifrado externo

Puede exportar la lista de exclusiones a un archivo XML. Luego puede modificar el archivo para, por ejemplo, añadir una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de exclusiones en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Anti-Cryptor**.
4. En el bloque **Exclusiones del análisis**, haga clic en el botón **Por nombre o dirección IP**.

5. Para exportar la lista de reglas:

   a. Seleccione las exclusiones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

      Si no seleccionó ninguna exclusión, Kaspersky Endpoint Security exportará todas las exclusiones.

   b. Haga clic en el botón → **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.

6. Para importar la lista de exclusiones:

   a. Haga clic en el botón → **Importar**.

   b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.

   c. Abra el archivo.

      Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

7. Guarde los cambios.

Cómo exportar e importar una lista de exclusiones en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host** → **Análisis de comportamiento** → **Anticifrado**.
5. Haga clic en el enlace **Exclusiones por nombre o dirección IP**.
6. Para exportar la lista de reglas:

   a. Seleccione las exclusiones que desea exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de exclusiones a un archivo JSON en la carpeta de descargas predeterminada.

7. Para importar la lista de exclusiones:

   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que importar la lista de exclusiones.

b. Abra el archivo.

Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

8. Guarde los cambios.

Motor de reparación

El componente Motor de reparación permite a Kaspersky Endpoint Security anular acciones que han sido realizadas por el malware en el sistema operativo.

Al anular la actividad de malware en el sistema operativo, Kaspersky Endpoint Security tramita los siguientes tipos de actividad de malware:

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina archivos ejecutables creados por malware (en todos los medios, excepto en las unidades de red).
  - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado.
  - Restaura los archivos que el malware ha modificado o eliminado.

  La capacidad de recuperar archivos está sujeta a algunas limitaciones.

- **Actividad del Registro**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina las claves del registro que el malware ha creado.
  - No restaura las claves del registro que el malware ha modificado o eliminado.

- **Actividad del sistema**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Finaliza los procesos iniciados por malware.
  - Finaliza los procesos en los que haya penetrado una aplicación maliciosa.
  - No reanuda procesos que el malware haya suspendido.

- **Actividad de red**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Bloquea la actividad de red del malware.
  - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.

La reversión de acciones de malware puede iniciarse durante un análisis antimalware o a pedido de los componentes Protección frente a amenazas en archivos y Detección de comportamiento.

Deshacer las operaciones de un software malicioso (malware) afecta a un conjunto de datos definidos rigurosamente. La anulación no tiene efectos adversos en el sistema operativo ni en la integridad de los datos del equipo.

Cómo activar o desactivar el componente Motor de reparación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Motor de reparación**.
4. Utilice la casilla de verificación **Motor de reparación** para activar o desactivar el componente.
5. Guarde los cambios.

Cómo activar o desactivar el componente Motor de reparación en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas del host → Análisis de comportamiento → Motor de reparación**.
5. Utilice interruptor **Motor de reparación ACTIVADO** para activar o desactivar el componente.
6. Guarde los cambios.

Cómo activar o desactivar el componente Motor de reparación en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Motor de reparación**.
3. Utilice interruptor **Motor de reparación** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si el Motor de reparación está activado, Kaspersky Endpoint Security revertirá las acciones realizadas por aplicaciones maliciosas en el sistema operativo.

Kaspersky Security Network



A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

La función de KSN puede dejar de estar disponible en la aplicación en el territorio de EE. UU.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, los servicios de KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web que se analicen, así como sobre la categoría y reputación de los archivos analizados. Para obtener más información sobre la configuración del acceso a KSN, consulte la Ayuda de Kaspersky Security Center.

El uso de Kaspersky Security Network es voluntario. La aplicación le invita a usar en KSN durante la configuración inicial de la aplicación. Los usuarios podrán reanudar o interrumpir su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el sitio web de Kaspersky contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. El archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación, contiene el texto de la Declaración de Kaspersky Security Network.

La infraestructura de las bases de datos de reputación de Kaspersky

Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura para trabajar con las bases de datos de reputación de Kaspersky:

- *Kaspersky Security Network (KSN).* Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky y, a su vez, envían a Kaspersky información sobre los objetos que se detectan en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos.

- *Kaspersky Private Security Network (KPSN)* es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos. KPSN se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:

  - porque las estaciones de trabajo locales no tienen acceso a Internet;

  - porque, por motivos legales o debido a las directivas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

Activación y desactivación del uso de Kaspersky Security Network

De forma predeterminada, Kaspersky Endpoint Security emplea el modo KSN ampliado. El *modo KSN ampliado* es un modo en el que Kaspersky Endpoint Security envía información adicional a Kaspersky.

Cómo activar o desactivar el uso de KSN en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Kaspersky Security Network**.
4. Utilice interruptor **Kaspersky Security Network** para activar o desactivar el componente.

   Si activó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte las condiciones de uso de la Declaración de Kaspersky Security Network (KSN), si está de acuerdo con ellas.
5. Si es necesario, desactive la casilla **Activar el modo ampliado de KSN**. De manera predeterminada, el modo KSN extendido está activado.
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el uso de KSN en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Kaspersky Security Network**.
5. Utilice interruptor **Uso de Kaspersky Security Network (KSN) ACTIVADO** para activar o desactivar el componente.

   Si activó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte las condiciones de uso de la Declaración de Kaspersky Security Network (KSN), si está de acuerdo con ellas.
6. De ser necesario, desactive la opción **Usar modo KSN extendido** con el interruptor. De manera predeterminada, el modo KSN extendido está activado.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el uso de KSN en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Kaspersky Security Network**.
3. Utilice interruptor **Kaspersky Security Network** para activar o desactivar el componente.

   Si activó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte las condiciones de uso de la Declaración de Kaspersky Security Network (KSN), si está de acuerdo con ellas.

4. De ser necesario, desactive la opción **Activar el modo ampliado de KSN** con el interruptor. De manera predeterminada, el modo KSN extendido está activado.

5. Guarde los cambios.

Como resultado, si el uso de KSN está activado, Kaspersky Endpoint Security usa la información sobre la reputación de archivos, recursos web y aplicaciones recibida de Kaspersky Security Network.

Limitaciones de Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos. Kaspersky Private Security Network le permite utilizar su propia base de datos de reputación local para comprobar la reputación de los objetos (archivos o direcciones web). La reputación de un objeto añadido a la base de datos de reputación local tiene mayor prioridad que uno añadido a KSN/KPSN. Por ejemplo, imagine que Kaspersky Endpoint Security está analizando un equipo y solicita la reputación de un archivo en KSN/KPSN. Si el archivo tiene una reputación *No fiable* en la base de datos de reputación local pero tiene una reputación *De confianza* en KSN/KPSN, Kaspersky Endpoint Security detectará el archivo como *No fiable* y tomará la acción definida para las amenazas detectadas.

Sin embargo, en algunos casos, es posible que Kaspersky Endpoint Security no solicite la reputación de un objeto en KSN/KPSN. Si este es el caso, Kaspersky Endpoint Security no recibirá datos de la base de datos de reputación local de KPSN. Es posible que Kaspersky Endpoint Security no solicite la reputación de un objeto en KSN/KPSN por las siguientes razones:

- Las aplicaciones de Kaspersky utilizan bases de datos de reputación offline. Las bases de datos de reputación offline están diseñadas para optimizar los recursos durante el funcionamiento de las aplicaciones de Kaspersky y para proteger los objetos de importancia crítica en el equipo. Las bases de datos de reputación offline son creadas por expertos de Kaspersky basándose en datos de Kaspersky Security Network. Las aplicaciones de Kaspersky actualizan las bases de datos de reputación offline con bases de datos antivirus de la aplicación específica. Si las bases de datos de reputación offline contienen información sobre un objeto que se está analizando, la aplicación no solicita la reputación de este objeto a KSN/KPSN.

- Las exclusiones de análisis (zona de confianza) se configuran en la configuración de la aplicación. Si este es el caso, la aplicación no tiene en cuenta la reputación del objeto en la base de datos de reputación local.

- La aplicación utiliza tecnologías de optimización de análisis, como iSwift o iChecker, o almacena en caché solicitudes de reputación en KSN/KPSN. Si este es el caso, es posible que la aplicación no solicite la reputación de los objetos analizados anteriormente.

- Para optimizar su carga de trabajo, la aplicación analiza archivos de cierto formato y tamaño. Los expertos de Kaspersky determinan la lista de formatos relevantes y límites de tamaño. Esta lista se actualiza con las bases de datos antivirus de la aplicación. También puede establecer la configuración de optimización del análisis en la interfaz de la aplicación, por ejemplo, para el componente de Protección frente a amenazas en archivos.

- Kaspersky Endpoint Security en modo Light Agent se comunica con los servidores de KSN a través de un servidor proxy de KSN. No se admite la comunicación directa con KSN.

Activar y desactivar el modo Cloud para los componentes de protección

Modo nube es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky.

La funcionalidad del modo Cloud está disponible desde la versión 3.0 de Kaspersky Private Security Network.

Si la aplicación funciona en modo Light Agent, el modo Nube no está disponible.

Cómo activar o desactivar el modo de nube para la protección de componentes en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Kaspersky Security Network**.
4. Utilice la casilla de verificación **Activar modo nube** para activar o desactivar el componente.
5. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el modo de nube para la protección de componentes en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Kaspersky Security Network**.
5. Utilice interruptor **Usar modo nube** para activar o desactivar el componente.
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar o desactivar el modo de nube para la protección de componentes en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas → Kaspersky Security Network**.
3. Utilice interruptor **Activar modo nube** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security descarga una versión ligera o una versión completa de las bases de datos antivirus durante la próxima actualización.

Si no está disponible la versión ligera de bases de datos antivirus, Kaspersky Endpoint Security cambia automáticamente a la versión premium.

Configuración del proxy de KSN

Los equipos de los usuarios que gestionen el servidor de administración de Kaspersky Security Center pueden interactuar con KSN directamente o mediante el servicio KSN Proxy.

Si la aplicación se está ejecutando en modo Light Agent, no se admite la comunicación directa con KSN. Kaspersky Endpoint Security se comunica con los servidores de KSN a través de un servidor proxy de KSN.

El servicio KSN Proxy ofrece las siguientes funcionalidades:

- El equipo del usuario puede consultar y enviar información a KSN, aunque no tenga acceso directo a Internet.
- El servicio KSN Proxy almacena los datos procesados en una caché; con ello, el equipo recibe más rápido la información que solicita y se reduce la congestión en el canal externo de comunicaciones por red.

De forma predeterminada, después de activar KSN y de aceptar la declaración de KSN, la aplicación utiliza un servidor proxy para conectarse con Kaspersky Security Network. El servidor proxy que utiliza la aplicación es el Servidor de administración de Kaspersky Security Center, a través del puerto TCP 13111. De este modo, si el proxy de KSN no está disponible, debe comprobar lo siguiente:

- Que el servicio `ksnproxy` esté en ejecución en el Servidor de administración.
- Que el firewall en el equipo no esté bloqueando el puerto 13111.

Puede configurar el uso del KSN Proxy de la siguiente manera: active o desactive el KSN Proxy y configure el puerto para la conexión. Para hacerlo, necesita abrir las propiedades del Servidor de administración. Para obtener más información sobre la configuración del KSN Proxy, consulte la Ayuda de Kaspersky Security Center. También puede activar o desactivar el KSN Proxy para equipos individuales en la directiva de Kaspersky Endpoint Security.

Cómo activar o desactivar el proxy de KSN en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas → Kaspersky Security Network**.

4. En el bloque de **Configuración del proxy de KSN**, utilice la casilla de verificación **Utilizar Servidor de administración como servidor proxy de KSN** para activar o desactivar la el Proxy de KSN.

5. Si es necesario, active la casilla **Utilizar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible**.

   Cuando esta casilla está activada y el servicio KSN Proxy no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores KSN pueden ubicarse tanto en el lado de Kaspersky como en el lado de terceros (cuando se utiliza Kaspersky Private Security Network).

6. Guarde los cambios.

Cómo activar o desactivar el proxy de KSN en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general → Kaspersky Security Network**.

5. Utilice la casilla de verificación **Usar Servidor de administración como servidor proxy de KSN** para activar o desactivar KSN Proxy.

6. Si es necesario, active la casilla **Usar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible**.

   Cuando esta casilla está activada y el servicio KSN Proxy no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores KSN pueden ubicarse tanto en el lado de Kaspersky como en el lado de terceros (cuando se utiliza Kaspersky Private Security Network). De forma predeterminada, la casilla de verificación está desactivada.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

La dirección del KSN Proxy coincide con la dirección del Servidor de administración. Cuando el nombre de dominio del Servidor de administración se modifica, debe actualizar manualmente la dirección del KSN Proxy.

Para configurar la dirección del proxy de KSN:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione la carpeta **Avanzado → Instalación remota → Paquetes de instalación**.

3. En el menú contextual de la carpeta **Paquetes de instalación**, elija **Propiedades**.

4. En la pestaña **General** de la ventana abierta, especifique la nueva dirección del servidor proxy de KSN.

5. Guarde los cambios.

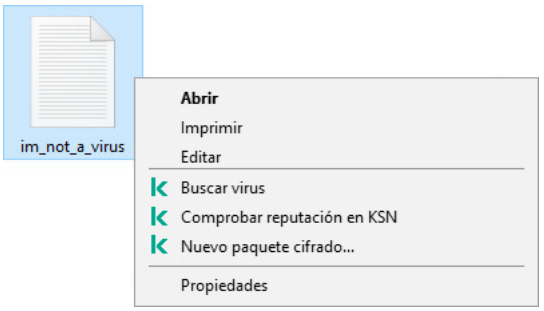
Comprobar la reputación de un archivo en Kaspersky Security Network

Si tiene dudas sobre la seguridad de un archivo, puede comprobar su reputación en Kaspersky Security Network.

Puede comprobar la reputación de un archivo si ha aceptado los términos de la Declaración de Kaspersky Security Network.

Para comprobar la reputación de un archivo en Kaspersky Security Network:

Abra el menú contextual del archivo y seleccione la opción **Comprobar reputación en KSN** (vea la imagen más abajo).



Menú contextual Archivo

Kaspersky Endpoint Security muestra la reputación del archivo:

De confianza (Kaspersky Security Network). La aplicación considera que un archivo es de confianza si se cumplen una o más de las siguientes condiciones:

- El archivo está firmado digitalmente por un proveedor de confianza.
- El archivo tiene una reputación de confianza en Kaspersky Security Network.
- El usuario ha puesto el archivo en el grupo De confianza.

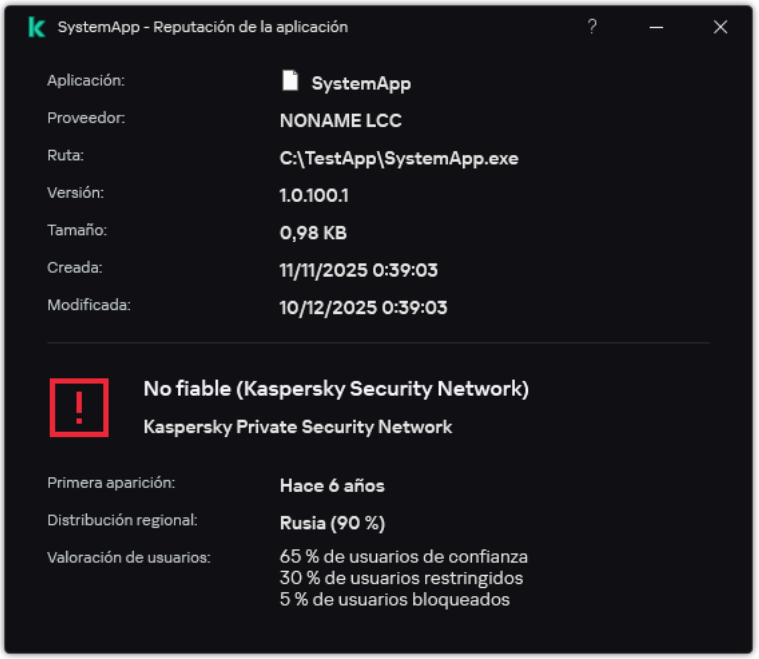
Software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales. Aunque no poseen ninguna función maliciosa, dichas aplicaciones pueden ser aprovechadas por los intrusos. Para obtener más información sobre el software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos personales de un usuario, visite el sitio web de la Enciclopedia de Kaspersky. Puede añadir estas aplicaciones a la lista de confianza.

No fiable (Kaspersky Security Network). Un virus u otra aplicación que representa una amenaza.

Desconocido (Kaspersky Security Network). Kaspersky Security Network no tiene ninguna información sobre el archivo. Puede analizar un archivo utilizando bases de datos antivirus (la opción **Buscar virus** del menú contextual).

Kaspersky Endpoint Security muestra la solución KSN que se utilizó para determinar la reputación del archivo: *Kaspersky Security Network* o *Kaspersky Private Security Network*.

Kaspersky Endpoint Security también muestra información adicional sobre el archivo (vea la imagen más abajo).



Reputación de un archivo en Kaspersky Security Network

Análisis de conexiones cifradas

Tras la instalación, Kaspersky Endpoint Security añade el certificado de Kaspersky al almacenamiento del sistema de certificados de confianza (Tienda de certificados de Windows). Kaspersky Endpoint Security utiliza este certificado para analizar conexiones cifradas. Kaspersky Endpoint Security también incluye el uso del almacenamiento del sistema de certificados de confianza en Firefox y Thunderbird para analizar el tráfico de estas aplicaciones.

Los componentes Control web, Protección frente a amenazas en el correo, Protección frente a amenazas web, Detección de comportamiento y Prevención de exploits pueden descifrar y analizar el tráfico de red que se transmite a través de conexiones cifradas que usen los siguientes protocolos:

- SSL 3.0
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Habilitar el análisis de conexiones cifradas

De forma predeterminada, Kaspersky Endpoint Security no siempre analiza las conexiones cifradas; solo lo hace cuando lo solicitan los componentes de protección.

Cómo activar el análisis de conexiones cifradas en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
5. En el bloque **Análisis de conexiones cifradas**, seleccione el modo de análisis de conexiones cifradas:
   - **Analizar conexiones cifradas**. Kaspersky Endpoint Security no tendrá acceso al contenido de sitios web cuyas direcciones comiencen con `https://`.
   - **Analizar las conexiones cifradas cuando lo soliciten los componentes de protección**. Kaspersky Endpoint Security analizará el tráfico cifrado solo cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control web lo soliciten.
   - **Analizar conexiones cifradas siempre**. Kaspersky Endpoint Security analizará el tráfico de red cifrado incluso cuando los componentes de protección están desactivados.

   Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por aplicaciones de confianza para las que el análisis de tráfico está desactivado. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza solo en la interfaz de Kaspersky Endpoint Security. No puede ver la lista en la Consola de Kaspersky Security Center.
6. Si es necesario, añada exclusiones de análisis: direcciones y aplicaciones de confianza.
7. Establezca la configuración para analizar conexiones cifradas (consulte la tabla a continuación).
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar el análisis de conexiones cifradas en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de red**.
5. En **Análisis de conexiones cifradas**, active el interruptor **Análisis de conexiones cifradas ACTIVADO**.

   Si el interruptor está desactivado, Kaspersky Endpoint Security no tendrá acceso al contenido de sitios web cuyas direcciones comiencen con `https://`.

6. Haga clic en **Configuración** y seleccione el modo de análisis de conexiones cifradas:

   - **Analizar las conexiones cifradas cuando lo soliciten los componentes de protección**. Kaspersky Endpoint Security analizará el tráfico cifrado solo cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control web lo soliciten.

   - **Analizar conexiones cifradas siempre**. Kaspersky Endpoint Security analizará el tráfico de red cifrado incluso cuando los componentes de protección están desactivados.

   Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por aplicaciones de confianza para las que el análisis de tráfico está desactivado. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza solo en la interfaz de Kaspersky Endpoint Security. No puede ver la lista en la Consola de Kaspersky Security Center.

7. Si es necesario, añada exclusiones de análisis: direcciones y aplicaciones de confianza.

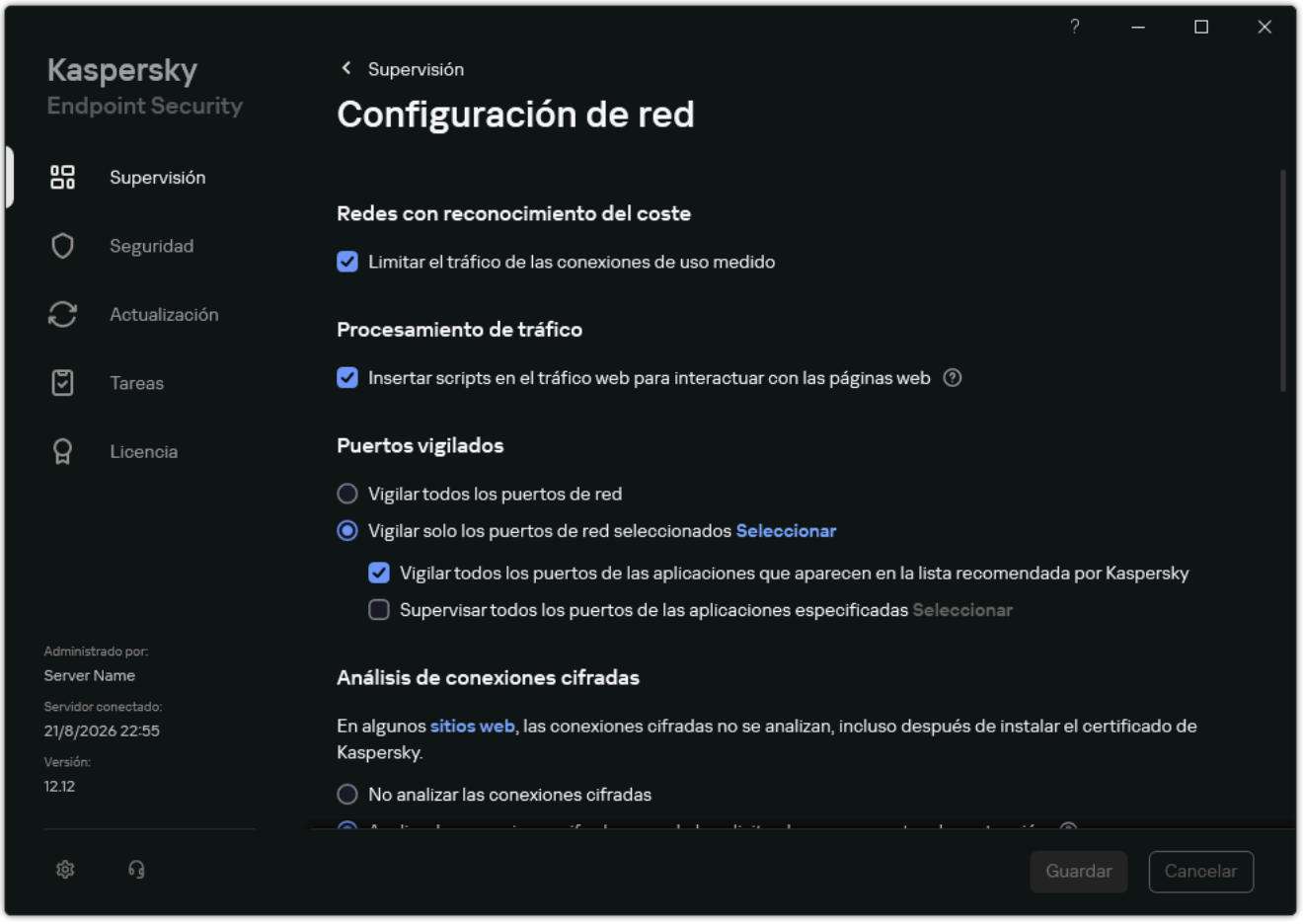
8. Establezca la configuración para analizar conexiones cifradas (consulte la tabla a continuación).

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar el análisis de conexiones cifradas en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Configuración de red**.



Configuración del análisis de conexiones cifradas

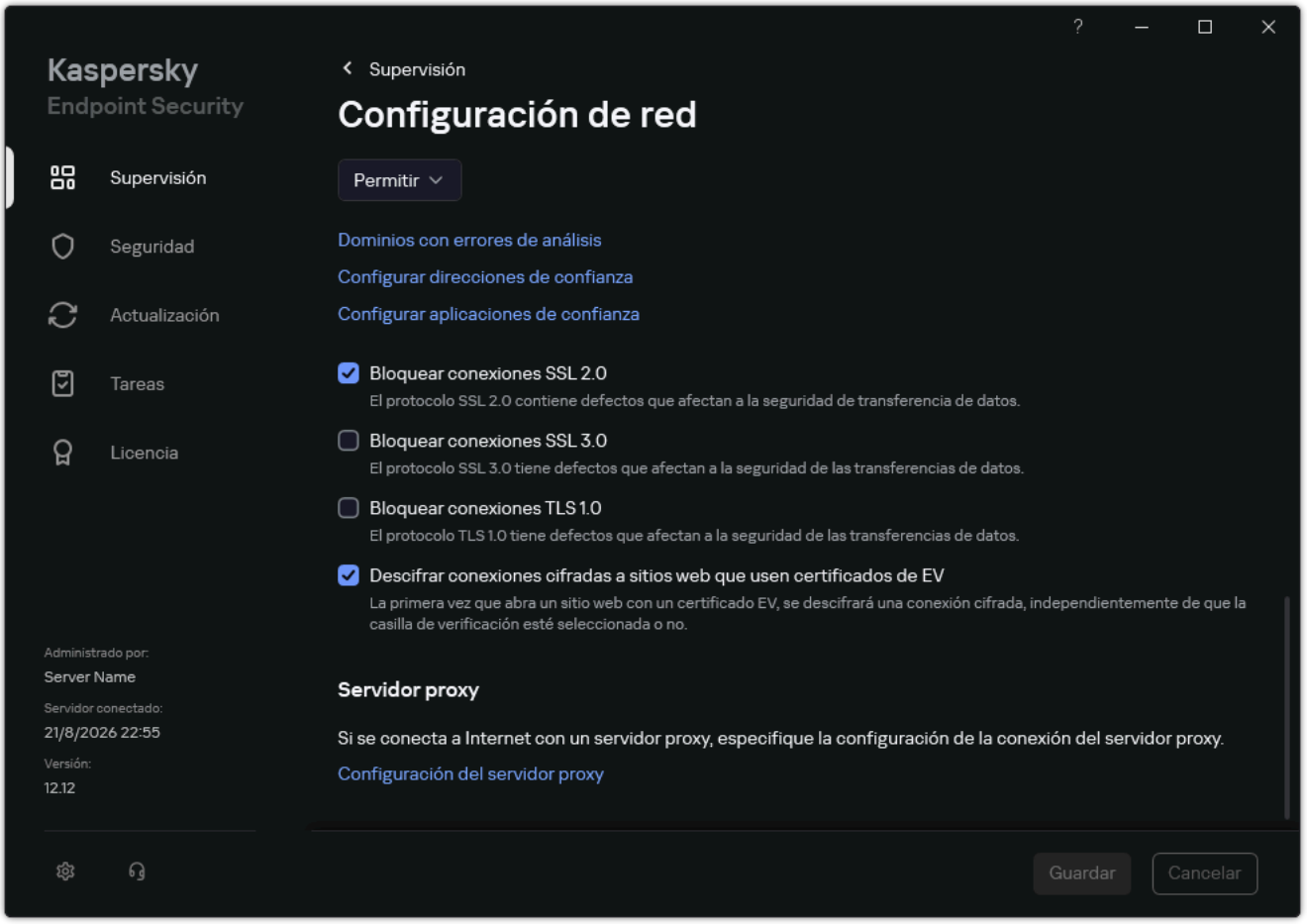
3. En el bloque **Análisis de conexiones cifradas**, seleccione el modo de análisis de conexiones cifradas:

- **No analizar las conexiones cifradas**. Kaspersky Endpoint Security no tendrá acceso al contenido de sitios web cuyas direcciones comiencen con `https://`.
- **Analizar las conexiones cifradas cuando lo soliciten los componentes de protección**. Kaspersky Endpoint Security analizará el tráfico cifrado solo cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control web lo soliciten.
- **Analizar conexiones cifradas siempre**. Kaspersky Endpoint Security analizará el tráfico de red cifrado incluso cuando los componentes de protección están desactivados.

Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por aplicaciones de confianza para las que el análisis de tráfico está desactivado. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza solo en la interfaz de Kaspersky Endpoint Security. No puede ver la lista en la Consola de Kaspersky Security Center.

4. Si es necesario, añada exclusiones de análisis: direcciones y aplicaciones de confianza.

5. Establezca la configuración para analizar conexiones cifradas (consulte la tabla a continuación).



Configuraciones adicionales para analizar conexiones encriptadas

6. Guarde los cambios.

Parámetro	Descripción
Certificados raíz de confianza	Lista de certificados raíz de confianza. Kaspersky Endpoint Security le permite instalar certificados raíz de confianza en equipos de usuarios si, por ejemplo, necesita desplegar un nuevo centro de certificados. La aplicación le permite añadir un certificado a un almacén de certificados especial de Kaspersky Endpoint Security. En este caso, el certificado se considera de confianza solo para la aplicación Kaspersky Endpoint Security. En otras palabras, el usuario puede acceder a un sitio web con el certificado nuevo en el navegador. Si otra aplicación intenta acceder al sitio web, es posible que se produzca un error de conexión debido a un problema de certificados. Para añadir un certificado al almacén de certificados del sistema, debe utilizar las directivas de grupo de Active Directory.
Visitando un dominio cuyo certificado no es de confianza	• **Permitir**. Cuando se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security permite que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para advertirle que acceder a ese dominio en particular no es recomendable e indicarle por qué. La página contiene un enlace para obtener acceso al recurso web solicitado. Si una aplicación o servicio de terceros establece una conexión con un dominio con un certificado que no es de confianza, Kaspersky Endpoint Security crea su propio certificado para analizar el tráfico. El certificado nuevo tiene el estado *No confiable*. Esto es necesario para advertir a la aplicación de terceros sobre la conexión no confiable porque la página HTML no se puede mostrar en este caso y la conexión se puede establecer en segundo plano. • **Bloquear**. Cuando se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security impide que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para explicarle por qué ese dominio en particular se ha bloqueado.
Visitando un dominio con un error de análisis de conexiones cifradas	• **Bloquear**. Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red. • **Permitir y añadir dominio a exclusiones**. Cuando se produce un error al analizar una conexión cifrada, Kaspersky Endpoint Security añade el dominio con el que se presentó el problema a la lista de dominios con errores de análisis y deja de controlar el tráfico de red cifrado que se genera al visitarlo. La lista de dominios con errores de análisis de conexiones cifradas solo puede consultarse a través de la interfaz local de la aplicación. Para borrar el contenido de la lista, deberá seleccionar **Bloquear**. Kaspersky Endpoint Security también genera un evento para el error de análisis de conexión cifrada.
Bloquear conexiones SSL 2.0	Cuando la casilla está marcada, la aplicación supervisa y bloquea las conexiones de red que se establecen con el protocolo SSL 2.0. Cuando la casilla está desmarcada, la aplicación no bloquea las conexiones de red que se establecen con el protocolo SSL 2.0. Sin embargo, la aplicación no supervisa el tráfico de red a través de este protocolo.
Bloquear conexiones SSL 3.0	Cuando la casilla está marcada, la aplicación bloquea las conexiones de red que se establecen con el protocolo SSL 3.0. Cuando la casilla está desmarcada, la aplicación no bloquea las conexiones de red que se establecen con el protocolo SSL 3.0. La aplicación supervisa el tráfico de red a través de este protocolo. Todos los componentes de la aplicación funcionan sin restricciones.
Bloquear conexiones TLS 1.0	Cuando la casilla está marcada, la aplicación bloquea las conexiones de red que se establecen con el protocolo TLS 1.0. Cuando la casilla está desmarcada, la aplicación no bloquea las conexiones de red que se establecen con el protocolo TLS 1.0. La aplicación supervisa el tráfico de red a través de este protocolo. Todos los componentes de la aplicación funcionan sin restricciones.
Descifrar conexiones cifradas a sitios web que usen certificados de EV	Los certificados de EV (Extended Validation Certificate) confirman la autenticidad de los sitios web y mejoran la seguridad de la conexión. Cuando un sitio web cuente con un certificado de EV, verá un candado en la barra de direcciones del navegador. Es posible, además, que la barra de direcciones esté total o parcialmente sombreada en verde. Cuando esta casilla está marcada, la aplicación descifra y controla las conexiones cifradas con sitios web que usan un certificado de EV. Cuando esta casilla no está marcada, la aplicación no tiene acceso al contenido del tráfico HTTPS. Esto significa que la aplicación únicamente puede controlar el tráfico HTTPS sobre la base de la dirección del sitio web (por ejemplo, `https://bing.com`). Cuando visite un sitio web con certificado de EV por primera vez, la conexión cifrada se descifrará independientemente de que la casilla esté o no activada.

Instalación de certificados raíz de confianza

Kaspersky Endpoint Security le permite instalar certificados raíz de confianza en equipos de usuarios si, por ejemplo, necesita desplegar un nuevo centro de certificados. La aplicación le permite añadir un certificado a un almacén de certificados especial de Kaspersky Endpoint Security. En este caso, el certificado se considera de confianza solo para la aplicación Kaspersky Endpoint Security. En otras palabras, el usuario puede acceder a un sitio web con el certificado nuevo en el navegador. Si otra aplicación intenta acceder al sitio web, es posible que se produzca un error de conexión debido a un problema de certificados. Para añadir un certificado al almacén de certificados del sistema, debe utilizar las directivas de grupo de Active Directory.

Cómo instalar certificados raíz de confianza en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
4. En el bloque **Certificados raíz de confianza**, haga clic en el botón **Añadir**.
5. En la ventana que se abre, seleccione un certificado raíz de confianza.
   Kaspersky Endpoint Security es compatible con certificados con extensiones PEM, DER y CRT.
6. Guarde los cambios.

Cómo instalar certificados raíz de confianza en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de red**.
5. Haga clic en el enlace **Certificados raíz de confianza**.
6. En la ventana que se abre, haga clic en **Añadir** y seleccione un certificado raíz de confianza.
   Kaspersky Endpoint Security es compatible con certificados con extensiones PEM, DER y CRT.
7. Guarde los cambios.

Cómo instalar certificados raíz de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Mostrar certificados**.

4. En la ventana que se abre, haga clic en **Añadir** y seleccione un certificado raíz de confianza.

   Kaspersky Endpoint Security es compatible con certificados con extensiones PEM, DER y CRT.

5. Guarde los cambios.

Como resultado, cuando se analice el tráfico, Kaspersky Endpoint Security usa su propio almacén de certificados además del almacén del sistema.

Análisis de conexiones cifradas con un certificado que no es de confianza

Tras la instalación, Kaspersky Endpoint Security añade el certificado de Kaspersky al almacenamiento del sistema de certificados de confianza (Tienda de certificados de Windows). Kaspersky Endpoint Security utiliza este certificado para analizar conexiones cifradas. Al visitar un dominio con un certificado que no es de confianza, puede permitir o denegar el acceso de los usuarios a ese dominio (consulte las instrucciones a continuación).

Si ha permitido que el usuario visite dominios con certificados que no son de confianza, Kaspersky Endpoint Security realiza las siguientes acciones:

- Al visitar un dominio con un certificado que no es de confianza en el *navegador*, Kaspersky Endpoint Security utiliza el certificado de Kaspersky para analizar el tráfico. Kaspersky Endpoint Security muestra una página HTML con una advertencia e información sobre el motivo por el cual no se recomienda visitar el dominio correspondiente (ver la figura a continuación). La página contiene un enlace para obtener acceso al recurso web solicitado. Una vez que el usuario hace clic en el enlace, dispone de una hora para visitar otros recursos alojados en el mismo dominio sin que Kaspersky Endpoint Security le advierta sobre la falta de confianza en el certificado. Kaspersky Endpoint Security también genera un evento sobre el establecimiento de una conexión cifrada con un certificado que no es de confianza.

  > En algunos casos, Kaspersky Endpoint Security no puede mostrar técnicamente una página HTML con una advertencia en el navegador (consulte la figura a continuación). Por ejemplo, si un recurso web usa una versión desactualizada de un protocolo de red y un puerto no estándar. En estos casos, Kaspersky Endpoint Security bloquea el acceso a este dominio y el navegador muestra la ventana `ERR_CONNECTION_RESET` estándar. Para acceder a un recurso web, puede añadir dominio a las exclusiones o utilizar un certificado de confianza.

- Si *una aplicación o servicio de terceros* establece una conexión con un dominio con un certificado que no es de confianza, Kaspersky Endpoint Security crea su propio certificado para analizar el tráfico. El certificado nuevo tiene el estado *No confiable*. Esto es necesario para advertir a la aplicación de terceros sobre la conexión no confiable porque la página HTML no se puede mostrar en este caso y la conexión se puede establecer en segundo plano. Por lo tanto, si una aplicación de terceros tiene herramientas de verificación de certificados integradas, es posible que se termine la conexión. En ese caso, debe ponerse en contacto con el propietario del dominio y configurar una conexión de confianza. Si no es posible establecer una conexión de confianza, puede añadir esa aplicación de terceros a la lista de aplicaciones de confianza. Kaspersky Endpoint Security también genera un evento sobre el establecimiento de una conexión cifrada con un certificado que no es de confianza.

Cómo configurar el análisis de conexiones cifradas con un certificado que no es de confianza en la Consola de Administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
4. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Configuración avanzada**.
5. En la ventana que se abre, seleccione el modo de funcionamiento de la aplicación cuando visite un dominio con un certificado que no sea de confianza: **Permitir** o **Bloquear**.
6. Guarde los cambios.

Cómo configurar el análisis de conexiones cifradas con un certificado que no es de confianza en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de red**.
5. En el bloque **Análisis de conexiones cifradas**, haga clic en el enlace **Configuración**.
6. En la ventana que se abre, seleccione el modo de funcionamiento de la aplicación cuando visite un dominio con un certificado que no sea de confianza: **Permitir conexión** o **Bloquear conexión**.
7. Guarde los cambios.

Cómo configurar el análisis de conexiones cifradas con un certificado que no es de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, seleccione el modo de funcionamiento de la aplicación cuando visite un dominio con un certificado que no sea de confianza: **Permitir** o **Bloquear**.
4. Guarde los cambios.



Advertencia sobre la visita de un dominio cuyo certificado no sea de confianza

Añadir el certificado de Kaspersky a la propia tienda de certificados

Los navegadores y los clientes de correo utilizan el certificado para verificar la seguridad y autenticidad de los recursos web. El certificado también proporciona cifrado de datos entre los recursos web y el usuario. La mayoría de los navegadores y clientes de correo utilizan la tienda de certificados de confianza (tienda de certificados de Windows). Por ejemplo, Google Chrome. Algunos navegadores y clientes de correo utilizan su propia tienda de certificados de forma predeterminada en lugar de la tienda de certificados de Windows. Por ejemplo, Firefox y Thunderbird.

Tras la instalación, Kaspersky Endpoint Security añade el certificado de Kaspersky al almacenamiento del sistema de certificados de confianza (Tienda de certificados de Windows). Si Kaspersky Security Center está implementado en su organización y se está aplicando una directiva a un equipo, Kaspersky Endpoint Security habilita automáticamente el uso de la tienda de certificados de Windows en navegadores y clientes de correo para analizar el tráfico de estas aplicaciones. Si no se aplica una directiva al equipo, puede elegir la tienda de certificados que utilizarán los navegadores y los clientes de correo. Si seleccionó la propia tienda de certificados, añada el certificado de Kaspersky a la tienda manualmente. Esto ayudará a evitar errores al trabajar con tráfico HTTPS.

Para analizar el tráfico en el navegador Mozilla Firefox y el cliente de correo Thunderbird, debe activar el Análisis de conexiones cifradas. Si el Análisis de conexiones cifradas está desactivado, la aplicación no analiza el tráfico en el navegador Mozilla Firefox ni en el cliente de correo Thunderbird. El análisis de conexiones cifradas también se debe activar para analizar el tráfico en los clientes de correo de MyOffice Mail y R7-Office Organizer.

Antes de añadir un certificado al almacén de certificados del navegador o del propio agente de correo, exporte el certificado de Kaspersky desde el Panel de control de Windows (propiedades de Internet). Puede obtener más información sobre cómo añadir un certificado a la tienda; por ejemplo, en el sitio web de soporte técnico de Mozilla.

Puede elegir la tienda de certificados solo en la interfaz local de la aplicación.

Para elegir una tienda de certificados para analizar conexiones cifradas en navegadores y clientes de correo:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, seleccione la casilla de verificación **Para analizar conexiones cifradas en aplicaciones con su propia tienda de certificados, use**.

4. Seleccionar una tienda de certificados:

   - **El almacén de certificados de Windows (recomendado)**. El certificado raíz de Kaspersky se añade a esta tienda durante la instalación de Kaspersky Endpoint Security.

   - **Tienda de certificados propia**. Mozilla Firefox y Thunderbird utilizan sus propias tiendas de certificados. Si se selecciona la tienda de certificados de Mozilla, debe añadir manualmente el certificado raíz de Kaspersky a esta tienda a través de las propiedades del navegador.

     Los clientes de correo MyOffice Mail y R7-Office Organizer también utilizan su propia tienda de certificados.

5. Guarde los cambios.

Exclusión de conexiones cifradas del análisis

La mayoría de los recursos web usan conexiones cifradas. Los expertos de Kaspersky recomiendan que active el análisis de conexiones cifradas. Si el análisis de conexiones cifradas interfiere con la actividad relacionada con el trabajo, puede añadir un sitio web a las exclusiones llamadas *direcciones de confianza*. En este caso, Kaspersky Endpoint Security no analiza el tráfico HTTPS de las direcciones web de confianza cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control Web están haciendo su trabajo.

Si una aplicación de confianza usa una conexión cifrada, puede desactivar el análisis de conexiones cifradas para esta aplicación. Por ejemplo, puede desactivar el análisis de conexiones cifradas para aplicaciones de almacenamiento en la nube que usan la autenticación de dos factores con su propio certificado.

Cómo excluir una dirección web de los análisis de conexiones cifradas en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
5. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Configurar direcciones de confianza**.
6. Haga clic en **Añadir**.
7. Introduzca el nombre de dominio o la dirección IP. Kaspersky Endpoint Security no analizará las conexiones cifradas que se establezcan al visitar el dominio especificado.

   Kaspersky Endpoint Security admite el carácter `*` para introducir una máscara en el nombre de dominio.

   > Kaspersky Endpoint Security no es compatible con el símbolo `*` para direcciones IP. Puede seleccionar un rango de direcciones IP utilizando una máscara de subred (por ejemplo, 198.51.100.0/24).

Ejemplos:

- `domain.com`: el registro incluye las siguientes direcciones: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. El registro es exclusivo de subdominios (por ejemplo, `subdomain.domain.com`).
- `subdomain.domain.com`: el registro incluye las siguientes direcciones: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.
- `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo excluir una dirección web de los análisis de conexiones cifradas en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de red**.
5. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Dominios de confianza**.
6. Haga clic en **Añadir**.
7. Introduzca el nombre de dominio o la dirección IP. Kaspersky Endpoint Security no analizará las conexiones cifradas que se establezcan al visitar el dominio especificado.

   Kaspersky Endpoint Security admite el carácter `*` para introducir una máscara en el nombre de dominio.

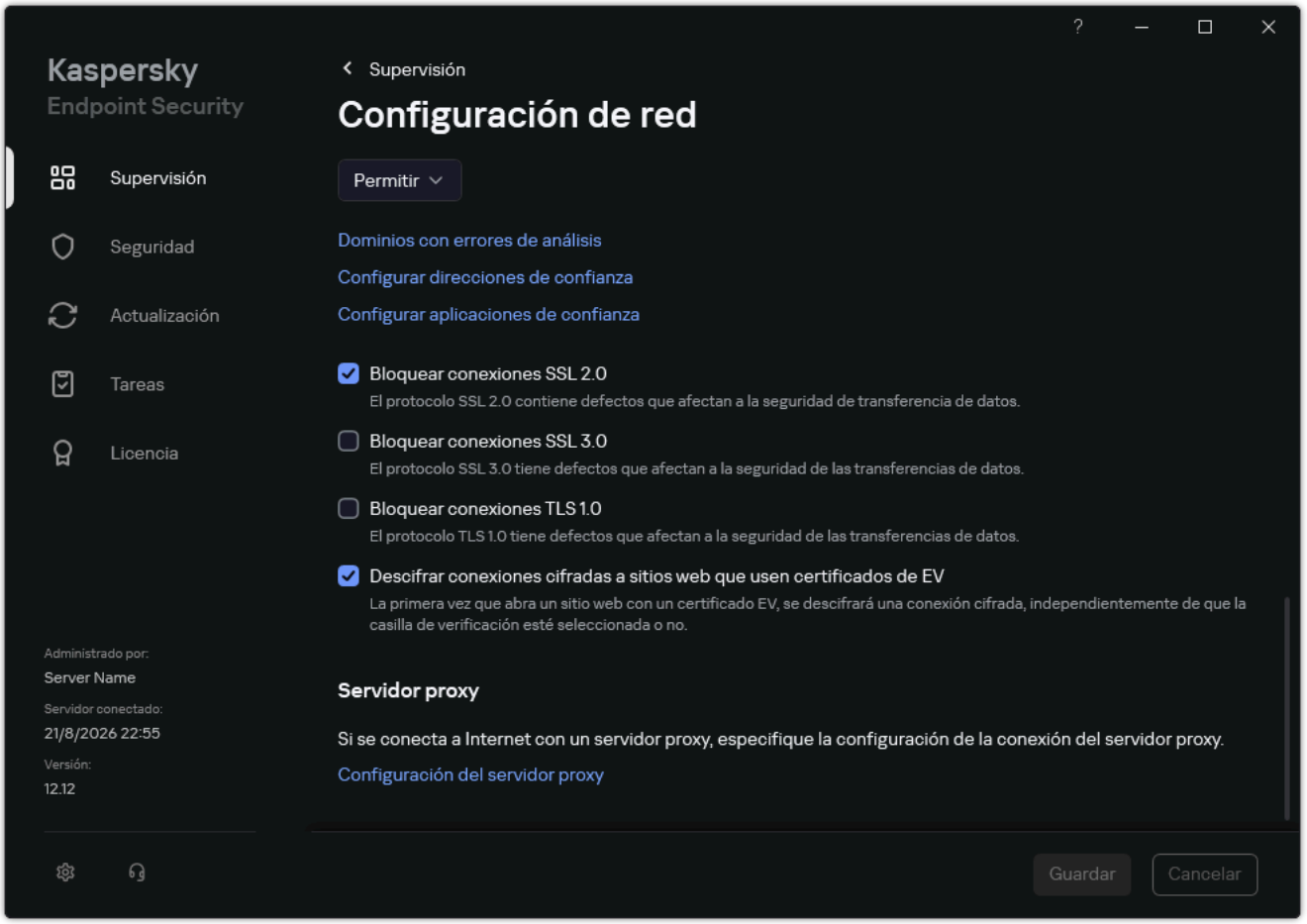
   > Kaspersky Endpoint Security no es compatible con el símbolo `*` para direcciones IP. Puede seleccionar un rango de direcciones IP utilizando una máscara de subred (por ejemplo, 198.51.100.0/24).

   Ejemplos:

   - `domain.com`: el registro incluye las siguientes direcciones: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. El registro es exclusivo de subdominios (por ejemplo, `subdomain.domain.com`).
   - `subdomain.domain.com`: el registro incluye las siguientes direcciones: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.
   - `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo excluir una dirección web de los escaneos de conexión cifrada en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.



Configuración de red de aplicaciones

3. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Configurar direcciones de confianza**.
4. Haga clic en **Añadir**.
5. Introduzca el nombre de dominio o la dirección IP. Kaspersky Endpoint Security no analizará las conexiones cifradas que se establezcan al visitar el dominio especificado.

   Kaspersky Endpoint Security admite el carácter `*` para introducir una máscara en el nombre de dominio.

   Kaspersky Endpoint Security no es compatible con el símbolo `*` para direcciones IP. Puede seleccionar un rango de direcciones IP utilizando una máscara de subred (por ejemplo, 198.51.100.0/24).

Ejemplos:

- `domain.com`: el registro incluye las siguientes direcciones: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. El registro es exclusivo de subdominios (por ejemplo, `subdomain.domain.com`).
- `subdomain.domain.com`: el registro incluye las siguientes direcciones: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.
- `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.

6. Guarde los cambios.

De forma predeterminada, Kaspersky Endpoint Security no analiza las conexiones cifradas cuando se producen errores y añade el sitio web a una lista especial de *dominios con errores de análisis*. Kaspersky Endpoint Security compila una lista separada para cada usuario y no envía datos a Kaspersky Security Center. Puede activar el bloqueo de la conexión cuando se produce un error de análisis. La lista de dominios con errores de análisis de conexiones cifradas solo puede consultarse a través de la interfaz local de la aplicación.

Para ver la lista de dominios con errores de análisis:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Dominios con errores de análisis**.

Se abre una lista de dominios con errores de análisis. Para restablecer la lista, active el bloqueo de la conexión cuando ocurran errores de análisis en la directiva, aplique la directiva y, a continuación, restablezca el parámetro a su valor inicial y vuelva a aplicar la directiva.

Los especialistas de Kaspersky hacen una lista de *excepciones globales*: sitios web de confianza que Kaspersky Endpoint Security no verifica independientemente de la configuración de la aplicación.

Para ver las exclusiones globales aplicadas al análisis de tráfico cifrado:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, haga clic en la lista de enlaces de sitios web de confianza.

Esto abre una lista de sitios web compilada por expertos de Kaspersky. Kaspersky Endpoint Security no analiza las conexiones protegidas para los sitios web de la lista. La lista puede sufrir cambios cada vez que se actualizan las bases de datos y los módulos de Kaspersky Endpoint Security.

Bloqueo del acceso a dominios con certificados que no son de confianza

En algunos casos, al bloquear el acceso a un dominio con un certificado que no es de confianza, Kaspersky Endpoint Security muestra en el navegador una página de advertencia HTML en la que falta el enlace al recurso web solicitado.

Esto puede suceder por las siguientes razones:

- El administrador bloqueó el acceso a un dominio con un certificado que no es de confianza.
- El dominio tiene un certificado que no es de confianza o no es válido, y el servidor web utiliza el mecanismo HTTP Strict Transport Security (HSTS). *HSTS* es un mecanismo de seguridad que impone el uso del protocolo seguro HTTPS para la comunicación entre un cliente y un servidor web. En este caso, no puede acceder al dominio aunque lo haya añadido a la lista de direcciones de confianza. El mecanismo HSTS se describe en RFC 6797.

  En algunos casos, el sitio web se puede abrir directamente en un navegador sin utilizar Kaspersky Endpoint Security. Los navegadores no siempre detectan los certificados revocados, mientras que Kaspersky Endpoint Security comprueba en línea si los certificados están revocados al establecer una conexión. Esto permite que la aplicación detecte un problema con el certificado antes que el navegador y muestre el mensaje de error correspondiente.



Advertencia sobre la visita de un dominio cuyo certificado no sea de confianza

Eliminación de datos

Kaspersky Endpoint Security cuenta con una tarea para eliminar información a distancia de los equipos de los usuarios.

En Kaspersky Endpoint Security, la eliminación de datos funciona:

- en modo silencioso;
- en los discos duros y en las unidades extraíbles;
- en todas las cuentas de usuario del equipo.

Kaspersky Endpoint Security ejecutará la tarea *Eliminación de datos* sin importar el tipo de licencia que se esté utilizando y con independencia de que esta haya caducado.

Modos de eliminación de datos

La tarea ofrece los siguientes modos de eliminación:

- Eliminación de datos inmediata.

  Utilice este modo para, por ejemplo, eliminar información antigua que esté ocupando espacio innecesariamente.

- Eliminación de datos pospuesta.

  Este modo está pensado para, por ejemplo, proteger los datos de un equipo portátil robado o extraviado. Es posible determinar que los datos de un equipo deberán eliminarse automáticamente si este abandona la red corporativa o no se sincroniza con Kaspersky Security Center durante un tiempo prolongado.

No se puede establecer una planificación para eliminar datos en las propiedades de la tarea. Solo puede eliminar datos inmediatamente después de iniciar la tarea manualmente, o configurar la eliminación de datos retrasada si no hay conexión con Kaspersky Security Center.

Limitaciones

La tarea Eliminación de datos tiene las siguientes limitaciones:

- Solo los administradores de Kaspersky Security Center pueden controlar la tarea *Eliminación de datos*. La tarea no puede iniciarse ni detenerse desde la interfaz local de Kaspersky Endpoint Security.
- Para el sistema de archivos NTFS, Kaspersky Endpoint Security elimina solo los nombres de los flujos de datos principales. Los nombres alternativos de flujos de datos no se pueden eliminar.
- Cuando elimina un archivo de enlace simbólico, Kaspersky Endpoint Security también elimina los archivos cuyas rutas se especifican en el enlace simbólico.

Creación de una tarea Eliminación de datos

Para eliminar información de los equipos de los usuarios:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Eliminación de datos**.

c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Eliminación de datos contra robos*).

d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

> Si se añaden nuevos equipos a un grupo de administración dentro del ámbito de la tarea, la tarea de eliminación de datos inmediata se ejecutará en los nuevos equipos únicamente si la tarea se completa en los cinco minutos posteriores a la incorporación de dichos equipos.

5. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

6. Seleccione la tarea **Eliminación de datos** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

7. Seleccione la pestaña **Configuración de la aplicación**.

8. Seleccione el método de eliminación de datos:

   - **Eliminar a través del sistema operativo**. Kaspersky Endpoint Security utilizará los recursos del sistema operativo para eliminar los archivos. Los objetos eliminados no se enviarán a la papelera de reciclaje.
   - **Eliminar por completo, sin posibilidad de recuperación**. Kaspersky Endpoint Security sobrescribirá los archivos con datos aleatorios. Es prácticamente imposible restaurar los datos después de que se eliminen.

9. Si desea posponer la eliminación de datos, seleccione la casilla **Eliminar automáticamente los datos cuando no haya habido conexión con Kaspersky Security Center en más de N días**. Defina el número de días.

> La tarea de eliminación pospuesta se ejecutará cada vez que no haya conexión con Kaspersky Security Center durante el período definido.

Al configurar la eliminación de datos pospuesta, tenga en cuenta que los empleados pueden tener diferentes horarios de trabajo. Tampoco olvide tener en cuenta el horario laboral de quienes trabajan sin conexión. Para más información sobre cómo trabajar con los equipos sin conexión y los usuarios que están fuera de la oficina, consulte la Ayuda de Kaspersky Security Center.

> Si el equipo está apagado y la conexión ha estado ausente durante más tiempo del configurado, después de encender el equipo, Kaspersky Endpoint Security no elimina los datos de inmediato. La aplicación espera la sincronización con Kaspersky Security Center durante una hora. Esto es necesario para evitar la eliminación no autorizada de datos en los equipos de los usuarios que apagaron sus equipos, por ejemplo, antes de irse de vacaciones.

Si esta casilla no está activada, la tarea se ejecutará después de que se realice la sincronización con Kaspersky Security Center.

10. Cree la lista de objetos que desee eliminar:

    - **Carpetas**. Kaspersky Endpoint Security eliminará todos los archivos y todas las subcarpetas de la carpeta. La ruta de acceso a la carpeta no puede contener máscaras ni variables de entorno.

    - **Archivos por extensión**. Kaspersky Endpoint Security buscará los archivos que tengan la extensión especificada en todas las unidades del equipo, incluidas las extraíbles. Para especificar más de una extensión, use los caracteres "`;`" o "`,`".

    - **Alcance predefinido**. Kaspersky Endpoint Security eliminará archivos de las siguientes áreas:

        - **Documentos**. Los archivos en la carpeta estándar *Documentos* del sistema operativo y sus subcarpetas.

        - **Cookies**. Los archivos en los que el navegador guarda datos de los sitios web visitados por el usuario (como los datos de autorización del usuario).

        - **Escritorio**. Los archivos en la carpeta estándar *Escritorio* del sistema operativo y sus subcarpetas.

        - **Archivos temporales de Internet Explorer**. Archivos temporales relacionados con el funcionamiento de Internet Explorer, como copias de páginas web, imágenes y archivos multimedia.

        - **Archivos temporales**. Archivos temporales relacionados con el funcionamiento de aplicaciones instaladas en el equipo. Por ejemplo, las aplicaciones de Microsoft Office crean archivos temporales que contienen copias de seguridad de documentos.

        - **Archivos de Outlook**. Archivos relacionados con el funcionamiento del cliente de correo Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de libretas de direcciones sin conexión (OAB) y archivos de libretas de direcciones personales (PAB).

        - **Perfil del usuario**. Conjunto de archivos y carpetas en los que el sistema operativo almacena la configuración asociada a la cuenta local del usuario.

    Puede crear una lista de objetos que desee eliminar en cada pestaña. Kaspersky Endpoint Security creará una lista consolidada y eliminará los archivos de esta lista cuando se complete una tarea.

    > Los archivos que Kaspersky Endpoint Security necesita para funcionar no pueden eliminarse.

11. Guarde los cambios.

12. Active la casilla ubicada junto a la tarea.

13. Haga clic en **Iniciar**.

    Como resultado, la información de los equipos se eliminará según el modo que se haya seleccionado, es decir, de inmediato o cuando no haya habido conexión. Si un archivo no pudiera eliminarse (por ejemplo, porque el usuario está trabajando con él), Kaspersky Endpoint Security no intentará eliminarlo una segunda vez. Para completar la eliminación de datos, deberá ejecutar la tarea nuevamente.

Control del equipo

Control Web

Control web permite regular el acceso de los usuarios a los recursos web. El componente ayuda a reducir tanto el volumen de tráfico como el tiempo que se malgasta en actividades no laborales. Cuando un usuario intenta abrir un sitio web que se ha restringido mediante Control web, Kaspersky Endpoint Security bloqueará el acceso o le mostrará una advertencia (vea la imagen más abajo).

Para utilizar Web Control, debe completar la configuración inicial de la aplicación:

- Para la supervisión del tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitado de forma predeterminada).
- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación supervisa todos los puertos).
- Seleccione las aplicaciones cuyo tráfico desea que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya están presentes en la lista de aplicaciones recomendadas por Kaspersky. Si su navegador no aparece en la lista, agréguelo manualmente.
- Recomendamos inyectar un script de interacción de página web en el tráfico web (de forma predeterminada, la inyección de script está desactivada). Este script permite el registro de eventos de Control web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Métodos para regular el acceso a los sitios web

Control web permite configurar el acceso a los sitios web a través de estos criterios:

- **Categorías de sitios web**. Para categorizar los sitios web, la aplicación utiliza el servicio en la nube Kaspersky Security Network, el análisis heurístico y la base de datos de sitios web conocidos, que está incluida con las demás bases de datos de la aplicación. Por ejemplo, puede restringir el acceso de los usuarios a la categoría *Redes sociales* o a otras categorías.
- **Tipo de datos**. Puede restringir el acceso de los usuarios a datos de un sitio web y, por ejemplo, ocultar las imágenes. Kaspersky Endpoint Security determina los tipos de datos basándose en el formato de los archivos, no en sus extensiones.

  > Kaspersky Endpoint Security no analiza el contenido de los archivos de almacenamiento. Por ello, si un grupo de imágenes está incluido en un archivo de almacenamiento, Kaspersky Endpoint Security considerará que el tipo de datos es *Archivos* en lugar de *Imágenes*.

- **Direcciones individuales**. Puede especificar una dirección web o usar máscaras.

Los criterios para regular el acceso a los sitios web pueden combinarse. Por ejemplo, puede restringir el acceso al tipo de datos *Archivos de aplicaciones de Office* solo para la categoría de sitios web *Correo electrónico basado en Web*.

Reglas de acceso a sitios web

Control web regula el acceso de los usuarios a los sitios web a través de *reglas de acceso*. Para cada una de estas reglas, puede configurar las siguientes opciones avanzadas:

- Usuarios alcanzados por la regla.

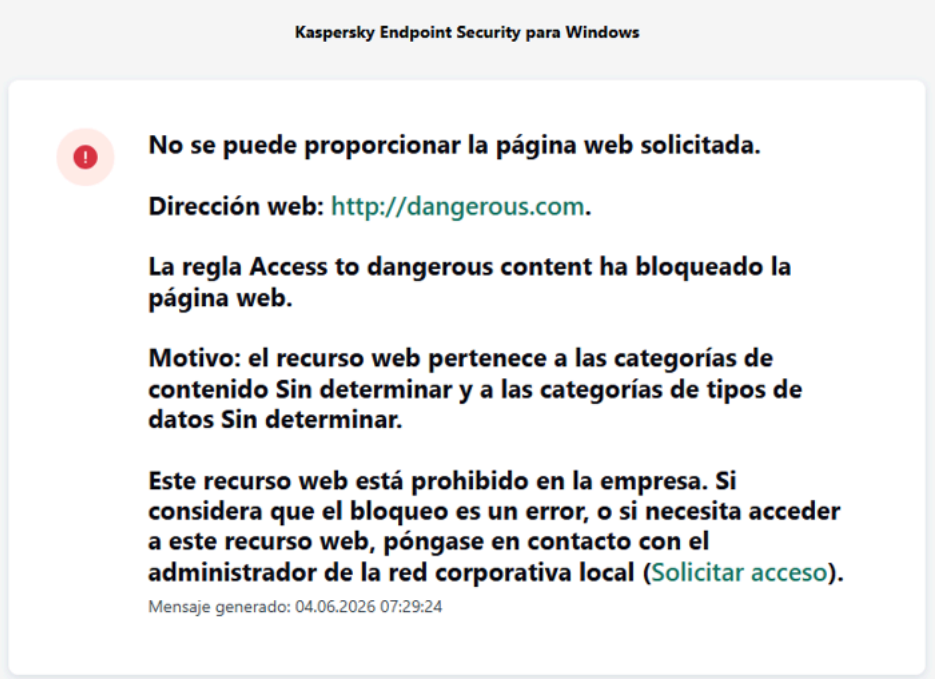
  Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.

- Planificación de reglas.

  Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

Prioridad de las reglas de acceso

Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web *Redes sociales* y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.





Mensajes de Control web

Adición de una regla de acceso a recursos web

Una *regla de acceso a recursos web* es un conjunto de filtros y acciones que Kaspersky Endpoint Security aplica cuando los usuarios visitan recursos web. Las reglas de acceso pueden incluir una planificación de reglas.

No se recomienda crear más de 1000 reglas de acceso a recursos web, ya que esto puede provocar inestabilidad en el sistema.

Una regla de acceso a recursos web es un conjunto de filtros y acciones que Kaspersky Endpoint Security realiza cuando el usuario visita recursos web que se describen en la regla durante el lapso de tiempo indicado en la planificación de reglas. Los filtros permiten especificar de forma precisa un conjunto de recursos web para los que el componente Control Web controla el acceso.

Están disponibles los siguientes filtros:

- **Filtrar por contenido**. Control Web categoriza los recursos web por contenido y tipo de datos. Puede controlar el acceso de los usuarios a los recursos web con tipos de datos y contenido que entran dentro de esas categorías. Cuando los usuarios visitan recursos web que pertenecen a la categoría de contenido o de tipo de dato seleccionada, Kaspersky Endpoint Security realiza la acción especificada en la regla.

- **Filtrar por direcciones de recursos web**. Puede controlar el acceso de los usuarios a todas las direcciones de recursos web, a direcciones de recursos web individuales o a grupos de direcciones de recursos web.

  Si se especifica el filtro por contenido y por direcciones de recursos web, y las direcciones de recursos web o los grupos de direcciones de recursos web especificados pertenecen a las categorías de contenido o de tipo de dato seleccionadas, Kaspersky Endpoint Security no controla el acceso a todos los recursos web en dichas categorías de contenido o de tipo de datos. En lugar de ello, la aplicación controla el acceso únicamente a las direcciones de recursos web o a los grupos de direcciones de recursos web.

- **Filtrar por nombres de usuarios y grupos de usuarios**. Puede especificar los nombres de los usuarios o grupos de usuarios para los que el acceso a los recursos web esté controlado de acuerdo con la regla.

- **Planificación de reglas**. Puede especificar la planificación de reglas. La planificación de reglas determina el intervalo de tiempo durante el que Kaspersky Endpoint Security supervisa el acceso a los recursos web cubiertos por la regla.

Tras instalar Kaspersky Endpoint Security, la lista de reglas del componente Control Web deja de estar vacío. La *Regla predeterminada* está preestablecida. Se utiliza para permitir o impedir a todos los usuarios el acceso a los recursos web para los que no existe otra regla.

Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web *Redes sociales* y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.

Cómo añadir una regla de acceso a recursos web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control Web**.
4. Seleccione la casilla **Control Web**.
5. En el bloque **Configuración de Control Web**, haga clic en el botón **Añadir**.

   Se abre la ventana **Regla de acceso a recursos web**.
6. Configure la regla de acceso a recursos web (consulte la tabla que aparece abajo).
7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Terminar la sesión de navegador activa tras aplicar la regla**.

   > Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

   Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.
8. Guarde los cambios.

Cómo añadir una regla de acceso a recursos web en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad → Control Web**.

5. Active la opción **Control Web ACTIVADO**.

6. En el bloque **Lista de reglas**, haga clic en el botón **Añadir**.

7. Configure la regla de acceso a recursos web (consulte la tabla que aparece abajo).

8. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Terminar la sesión de navegador activa tras aplicar la regla**.

   > Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

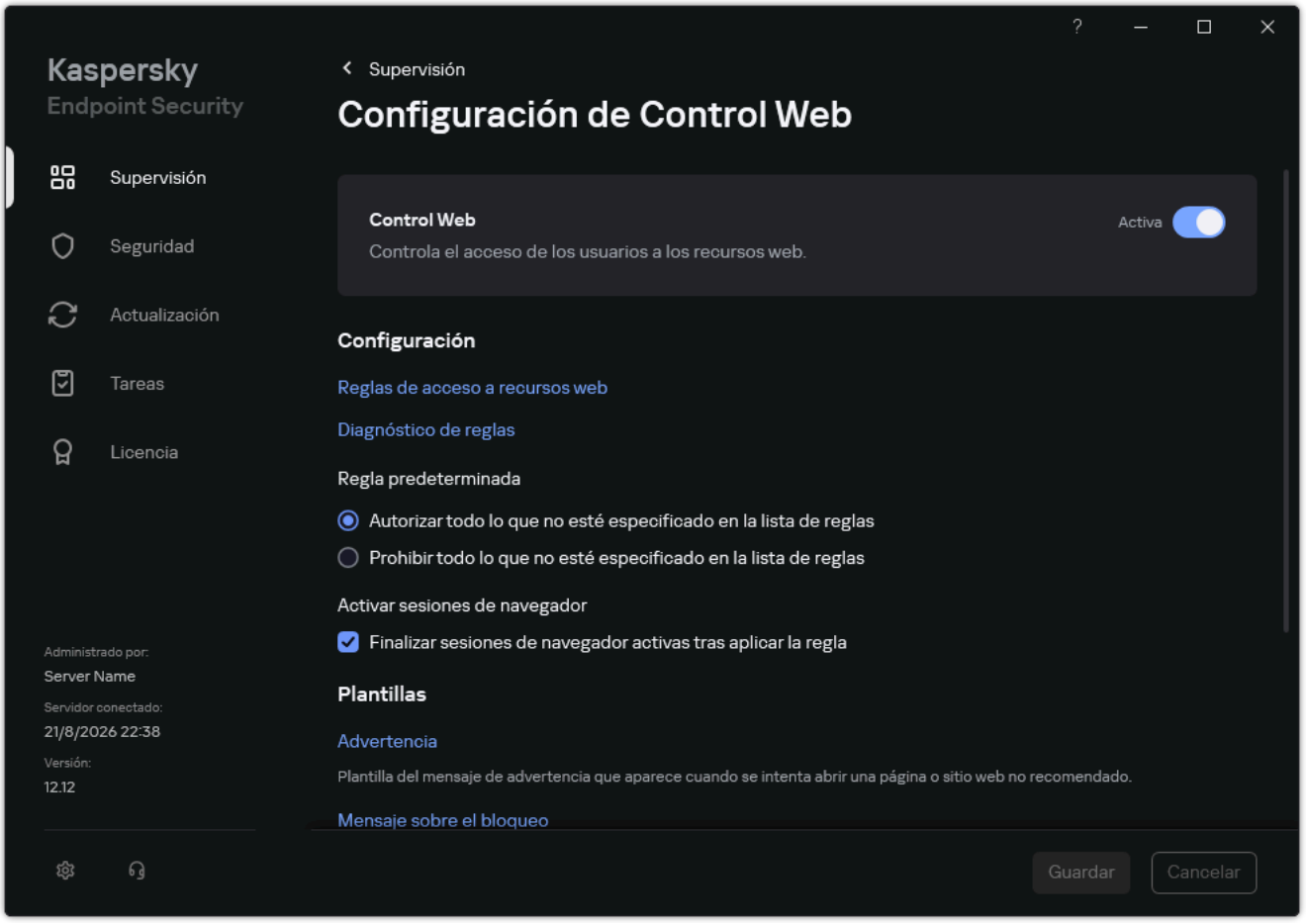
   Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

9. Guarde los cambios.

Cómo añadir una regla de acceso a recursos web en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control Web**.



Configuración de Control Web

3. Active la opción **Control Web**.

4. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.

5. En la ventana que se abre, haga clic en el botón **Añadir**.

   Se abre la ventana **Regla de acceso a recursos web**.

6. Configure la regla de acceso a recursos web (consulte la tabla que aparece abajo).

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Finalizar sesiones de navegador activas tras aplicar la regla**.

   Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

   Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

8. Guarde los cambios.

Como resultado, la nueva regla de Control Web se añade a la lista. Si es necesario, cambie la prioridad de la regla de Control Web. También puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

Parámetros de las regla de Control Web

Parámetro	Descripción
Nombre de la regla	Nombre de la regla de Control Web.
Condición	• **Activo**. • **Inactivo**. Puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento.
Acción	• **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla. • **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado. • **Advertir**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.
Contenido del filtro	• **Por categorías de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, la categoría *Redes sociales*). • **Por tipos de datos**. Puede controlar el acceso de los usuarios a los recursos web en función del tipo de datos específico de sus datos publicados (por ejemplo, *Imágenes*).
Direcciones	• **A todas las direcciones**. Control web no filtrará los recursos web por dirección. • **A direcciones individuales**. Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio. Si el Análisis de conexiones cifradas no está activado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.
Usuarios	• **A todos los usuarios**. Control web no filtrará recursos web para usuarios específicos. • **A usuarios individuales o grupos**. Control web filtrará los recursos web solo para usuarios específicos. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.
Planificación de reglas	La planificación de reglas determina el intervalo de tiempo durante el que Kaspersky Endpoint Security supervisa el acceso a los recursos web cubiertos por la regla. Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

Filtrar por direcciones de recursos web

Para controlar el acceso a recursos web individuales, debe crear una regla de Control Web, crear una lista de direcciones web y seleccionar una acción de Control Web. Al crear una lista de direcciones web, puede introducir direcciones URL o usar máscaras.

Las reglas pueden incluir una planificación de reglas y una lista de usuarios a los que se aplican las reglas. Por ejemplo, puede restringir el acceso a sitios web únicamente durante horas de trabajo, o permitir visitas a sitios web a usuarios de determinados grupos.

Cómo activar el filtro de direcciones de recursos web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control Web**.
4. Seleccione la casilla **Control Web**.
5. En el bloque **Configuración de Control Web**, haga clic en el botón **Añadir**.
   Se abre la ventana **Regla de acceso a recursos web**.
6. Configure la regla de acceso a recursos web:
   a. En el campo **Nombre**, introduzca el nombre de la regla.
   b. En la lista desplegable **Aplicar a direcciones**, seleccione **A direcciones individuales**.
   c. Crear una lista de direcciones de recursos web. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT.

      Si el Análisis de conexiones cifradas no está activado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

   d. En la lista desplegable **Aplicar a usuarios**, seleccione el filtro correspondiente para usuarios:
      - **A todos los usuarios**. Control web no filtrará los recursos web por dirección.
      - **A usuarios individuales o grupos**. Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

e. En la lista desplegable **Acción**, seleccione una opción.

- **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla.
- **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado.
- **Advertir**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

f. En la lista desplegable **Planificación de reglas**, seleccione una planificación o cree una nueva.

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Terminar la sesión de navegador activa tras aplicar la regla**.

   Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

   Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

8. Guarde los cambios.

Cómo activar el filtro de direcciones de recursos web en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control Web**.
5. Active la opción **Control Web ACTIVADO**.
6. En el bloque **Lista de reglas**, haga clic en el botón **Añadir**.
7. Configure la regla de acceso a recursos web:
   a. En el campo **Nombre de la regla**, introduzca el nombre de la regla.
   b. Seleccione el estado **Activado** para la regla de acceso a recursos web.
      Puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

c. En el bloque **Acción**, seleccione la opción correspondiente:

- **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla.
- **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado.
- **Informar**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

d. En **Alcance**, seleccione **Sitios web individuales**.

e. Configurar el filtro de contenido:

- **Dirección individual**. Crear una lista de direcciones de recursos web. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT.

  > Si el Análisis de conexiones cifradas no está activado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

- **Tipo de dato**. Puede controlar el acceso de los usuarios a los recursos web en función del tipo de datos específico de sus datos publicados (por ejemplo, *Imágenes*).

f. En **Usuario o grupo**, seleccione los usuarios a los que desea que Control web aplique la regla.

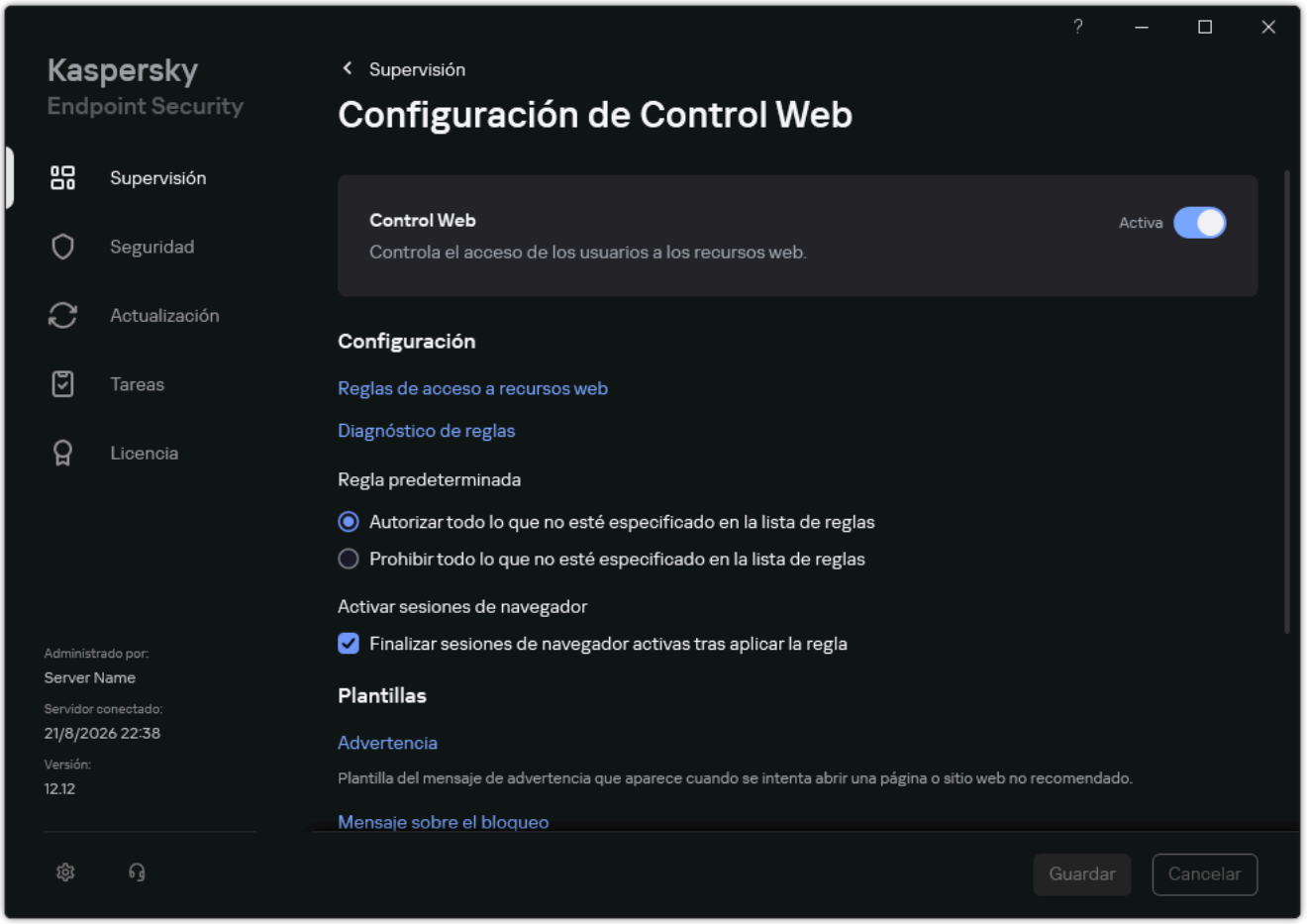
Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

g. En el bloque **Planificación del acceso**, seleccione una planificación o cree una nueva.

8. Guarde los cambios.

Cómo activar el filtro de direcciones de recursos web en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control Web**.



Configuración de Control Web

3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.

   Se abre la ventana **Regla de acceso a recursos web**.
5. En el campo **Nombre de la regla**, introduzca el nombre de la regla.
6. Seleccione el estado **Activo** para la regla de acceso a recursos web.

   Puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento.
7. En el bloque **Acción**, seleccione la opción correspondiente:

   - **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla.
   - **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado.
   - **Advertir**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.
8. En **Direcciones**, seleccione **A direcciones individuales**.

Crear una lista de direcciones de recursos web. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT.

Si el Análisis de conexiones cifradas no está activado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

9. En el bloque **Usuarios**, seleccione el filtro correspondiente para los usuarios:

   - **A todos los usuarios**. Control web no filtrará recursos web para usuarios específicos.
   - **A usuarios individuales o grupos**. Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

10. En la lista desplegable **Planificación de reglas**, seleccione una planificación o cree una nueva.

11. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Finalizar sesiones de navegador activas tras aplicar la regla**.

    Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

    Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

12. Guarde los cambios.

Como resultado, la nueva regla de Control Web se añade a la lista. Si es necesario, cambie la prioridad de la regla de Control Web. También puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

Filtrar por contenido de recursos web.

Para controlar el acceso por contenido de los recursos web, Control Web proporciona un filtro de categorías y un filtro de tipo de datos.

Para categorizar los sitios web, la aplicación utiliza el servicio en la nube Kaspersky Security Network, el análisis heurístico y la base de datos de sitios web conocidos, que está incluida con las demás bases de datos de la aplicación. Por ejemplo, puede restringir el acceso de los usuarios a la categoría *Redes sociales* o a otras categorías.

Puede restringir el acceso de los usuarios a un sitio web en función del tipo de datos; por ejemplo, para ocultar imágenes. Kaspersky Endpoint Security determina los tipos de datos basándose en el formato de los archivos, no en sus extensiones. Control Web distingue los siguientes tipos de datos:

- Vídeo
- Sonido

- Archivos de aplicaciones de Office
- Archivos ejecutables
- Archivos
- Imágenes
- Scripts

Kaspersky Endpoint Security no analiza el contenido de los archivos de almacenamiento. Por ello, si un grupo de imágenes está incluido en un archivo de almacenamiento, Kaspersky Endpoint Security considerará que el tipo de datos es *Archivos* en lugar de *Imágenes*.

Las reglas pueden incluir una planificación de reglas y una lista de usuarios a los que se aplican las reglas. Por ejemplo, puede restringir el acceso a sitios web únicamente durante horas de trabajo, o permitir visitas a sitios web a usuarios de determinados grupos.

Cómo activar el filtro de contenido de recursos web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control Web**.
4. Seleccione la casilla **Control Web**.
5. En el bloque **Configuración de Control Web**, haga clic en el botón **Añadir**.
   Se abre la ventana **Regla de acceso a recursos web**.
6. Configure la regla de acceso a recursos web:
   a. En el campo **Nombre**, introduzca el nombre de la regla.
   b. En la lista desplegable **Filtrar contenido**, seleccione el filtro de contenido relevante:
      - **Por categorías de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, la categoría *Redes sociales*).
      - **Por tipos de datos**. Puede controlar el acceso de los usuarios a los recursos web en función del tipo de datos específico de sus datos publicados (por ejemplo, *Imágenes*).
      - **Por categorías de contenido y tipos de datos**. Los filtros por categorías de contenido y tipos de datos están activados.

   Tras seleccionar los filtros, configure los parámetros de los filtros.

c. En la lista desplegable **Aplicar a usuarios**, seleccione el filtro correspondiente para usuarios:

- **A todos los usuarios**. Control web no filtrará los recursos web por dirección.
- **A usuarios individuales o grupos**. Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

d. En la lista desplegable **Acción**, seleccione una opción.

- **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla.
- **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado.
- **Advertir**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

e. En la lista desplegable **Planificación de reglas**, seleccione una planificación o cree una nueva.

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Terminar la sesión de navegador activa tras aplicar la regla**.

   Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

   Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

8. Guarde los cambios.

Cómo activar el filtro de contenido de recursos web en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control Web**.
5. Active la opción **Control Web ACTIVADO**.
6. En el bloque **Lista de reglas**, haga clic en el botón **Añadir**.

7. Configure la regla de acceso a recursos web:

   a. En el campo **Nombre de la regla**, introduzca el nombre de la regla.

   b. Seleccione el estado **Activado** para la regla de acceso a recursos web.

      Puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento.

   c. En el bloque **Acción**, seleccione la opción correspondiente:

      - **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla.
      - **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado.
      - **Informar**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

   d. En **Alcance**, seleccione **Categoría de contenido**.

   e. Configurar el filtro de contenido:

      - **Categoría de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, la categoría *Redes sociales*).
      - **Tipo de dato**. Puede controlar el acceso de los usuarios a los recursos web en función del tipo de datos específico de sus datos publicados (por ejemplo, *Imágenes*).

   f. En **Usuario o grupo**, seleccione los usuarios a los que desea que Control web aplique la regla.

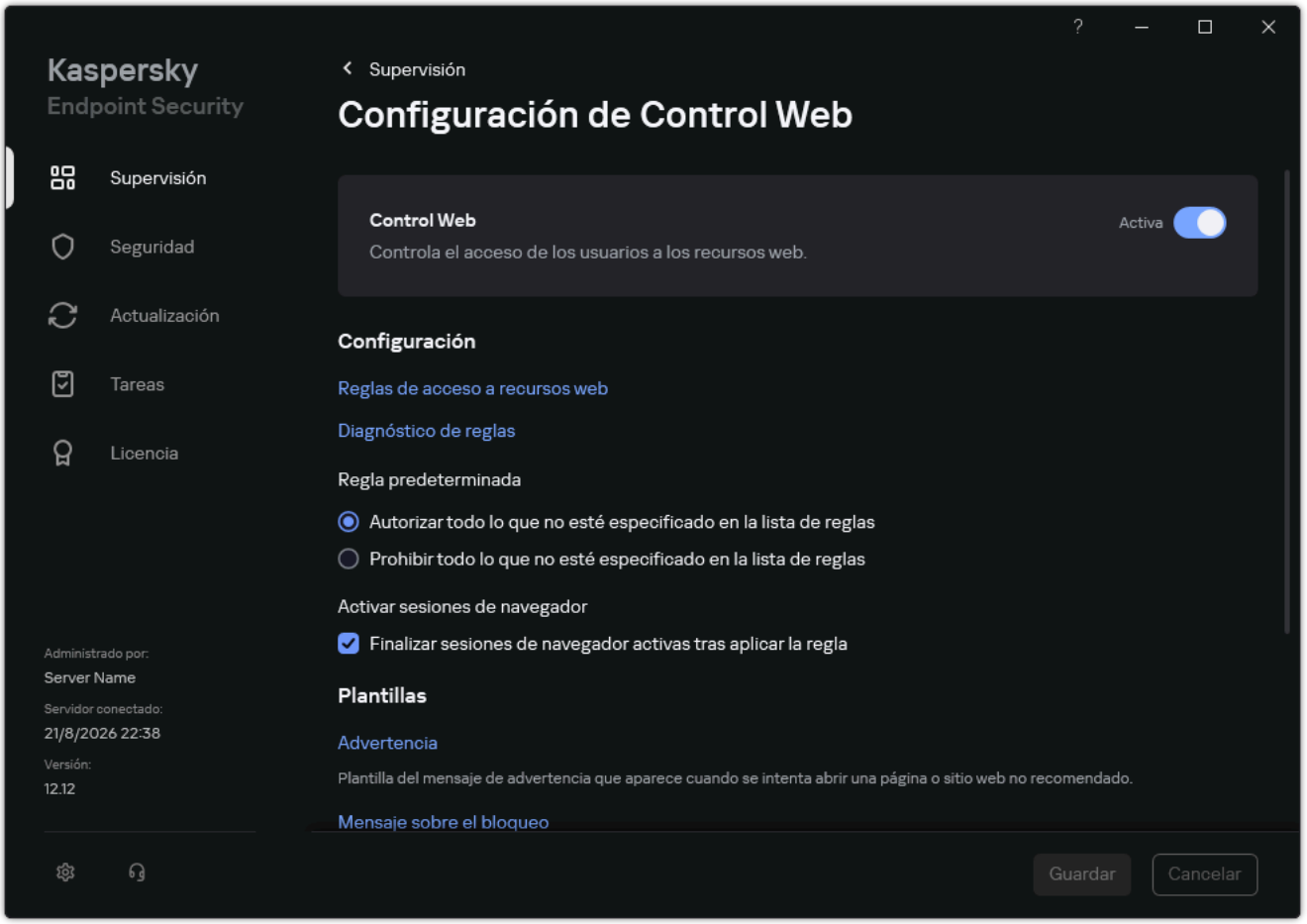
      Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   g. En el bloque **Planificación del acceso**, seleccione una planificación o cree una nueva.

8. Guarde los cambios.

Cómo activar el filtro de contenido de recursos web en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.



Configuración de Control Web

3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.

   Se abre la ventana **Regla de acceso a recursos web**.
5. En el campo **Nombre de la regla**, introduzca el nombre de la regla.
6. Seleccione el estado **Activo** para la regla de acceso a recursos web.

   Puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento.
7. En el bloque **Acción**, seleccione la opción correspondiente:

   - **Permitir**. Control Web permite acceder a recursos web que coinciden con los parámetros de la regla.
   - **Bloquear**. Control Web bloquea el acceso a recursos web que coinciden con los parámetros de la regla y muestra un mensaje de acceso a sitio web denegado.
   - **Advertir**. Cuando un usuario intenta acceder a un recurso web que coincide con la regla, Control Web muestra una advertencia de que no es recomendable visitar el recurso web. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

8. En el bloque **Contenido del filtro**, seleccione el filtro de contenido relevante:

   - **Por categorías de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, la categoría *Redes sociales*).
   - **Por tipos de datos**. Puede controlar el acceso de los usuarios a los recursos web en función del tipo de datos específico de sus datos publicados (por ejemplo, *Imágenes*).

   Para configurar el filtro de contenido:

   a. Haga clic en el enlace **Configuración**.

   b. Seleccione las casillas de verificación junto a los nombres de las categorías de contenido y de tipos de datos requeridas.

   Al seleccionar la casilla de verificación junto al nombre de una categoría de contenido o de tipos de datos, Kaspersky Endpoint Security aplica la regla para controlar el acceso a los recursos web que pertenecen a las categorías de contenido o a las categorías de tipos de datos seleccionadas.

   c. Regrese a la ventana para configurar la regla de acceso a recursos web.

9. En el bloque **Usuarios**, seleccione el filtro correspondiente para los usuarios:

   - **A todos los usuarios**. Control web no filtrará los recursos web por dirección.
   - **A usuarios individuales o grupos**. Control web filtrará solo las direcciones de recursos web de la lista. Puede especificar una dirección web o usar máscaras. También puede exportar una lista de direcciones de recursos web desde un archivo TXT. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio. Para crear una lista de usuarios a los que desea aplicar la regla:

     a. Haga clic en **Añadir**.

     b. En la ventana que se abre, seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de acceso a recursos web.

     c. Regrese a la ventana para configurar la regla de acceso a recursos web.

10. En la lista desplegable **Planificación de reglas**, seleccione el nombre de la planificación necesaria o genere una nueva planificación basada en la planificación de la regla seleccionada. Para ello:

    a. Haga clic en **Editar o añadir nuevo**.

    b. En la ventana que se abre, haga clic en el botón **Añadir**.

    c. En la ventana que se abre, introduzca el nombre de la planificación de reglas.

    d. Configure la planificación de acceso a los recursos web para los usuarios.

    e. Regrese a la ventana para configurar la regla de acceso a recursos web.

11. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de aplicar la directiva, seleccione la casilla de verificación **Finalizar sesiones de navegador activas tras aplicar la regla**.

Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones.

Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

12. Guarde los cambios.

Como resultado, la nueva regla de Control Web se añade a la lista. Si es necesario, cambie la prioridad de la regla de Control Web. También puede usar el interruptor para desactivar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

Comprobación de las reglas de acceso a recursos web

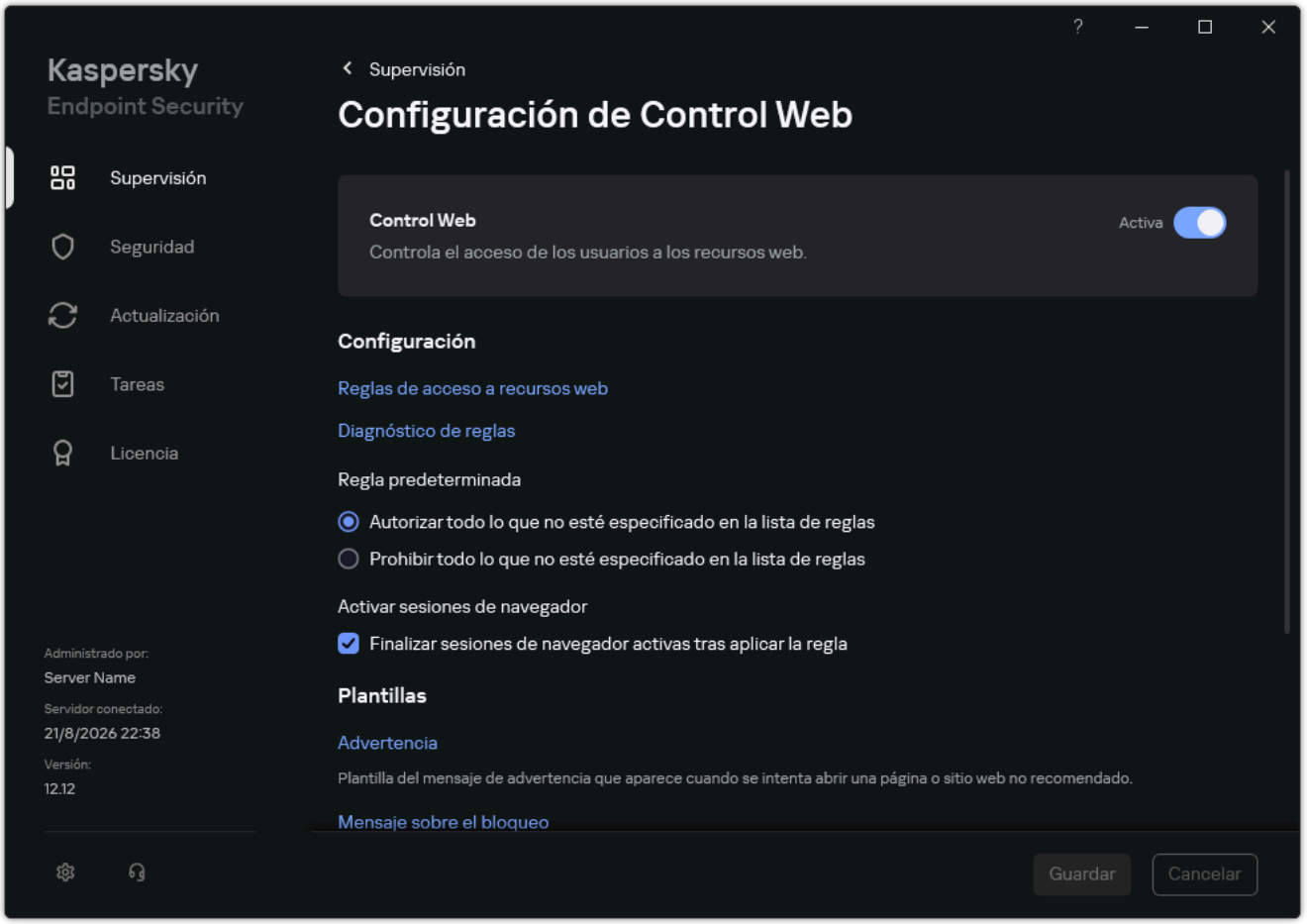
Al configurar Control Web, quizá bloquee involuntariamente el acceso a los recursos web que los usuarios necesitan para su trabajo. Para saber qué regla de Control Web bloquea el acceso a los recursos web, puede usar la herramienta *diagnóstico de reglas de Control Web*. El diagnóstico de reglas de Control Web solo está disponible en la interfaz de Kaspersky Endpoint Security. En la consola de Kaspersky Security Center no puede averiguar qué regla de Control Web incluye un recurso concreto.

Si el usuario cree que el recurso web está bloqueado por error, este puede hacer clic en el enlace del mensaje que informa del bloqueo del recurso web para enviar un mensaje generado previamente y enviárselo al administrador de la red de área local.

Para probar las reglas de acceso a recursos web:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.



Configuración de Control Web

3. En el bloque **Configuración**, haga clic en el enlace **Diagnóstico de reglas**.

   Se abre la ventana **Diagnóstico de reglas**.

4. Si quiere probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a un recurso web específico, seleccione la casilla de verificación **Especificar dirección**. Introduzca la dirección del recurso web en el campo que aparece abajo.

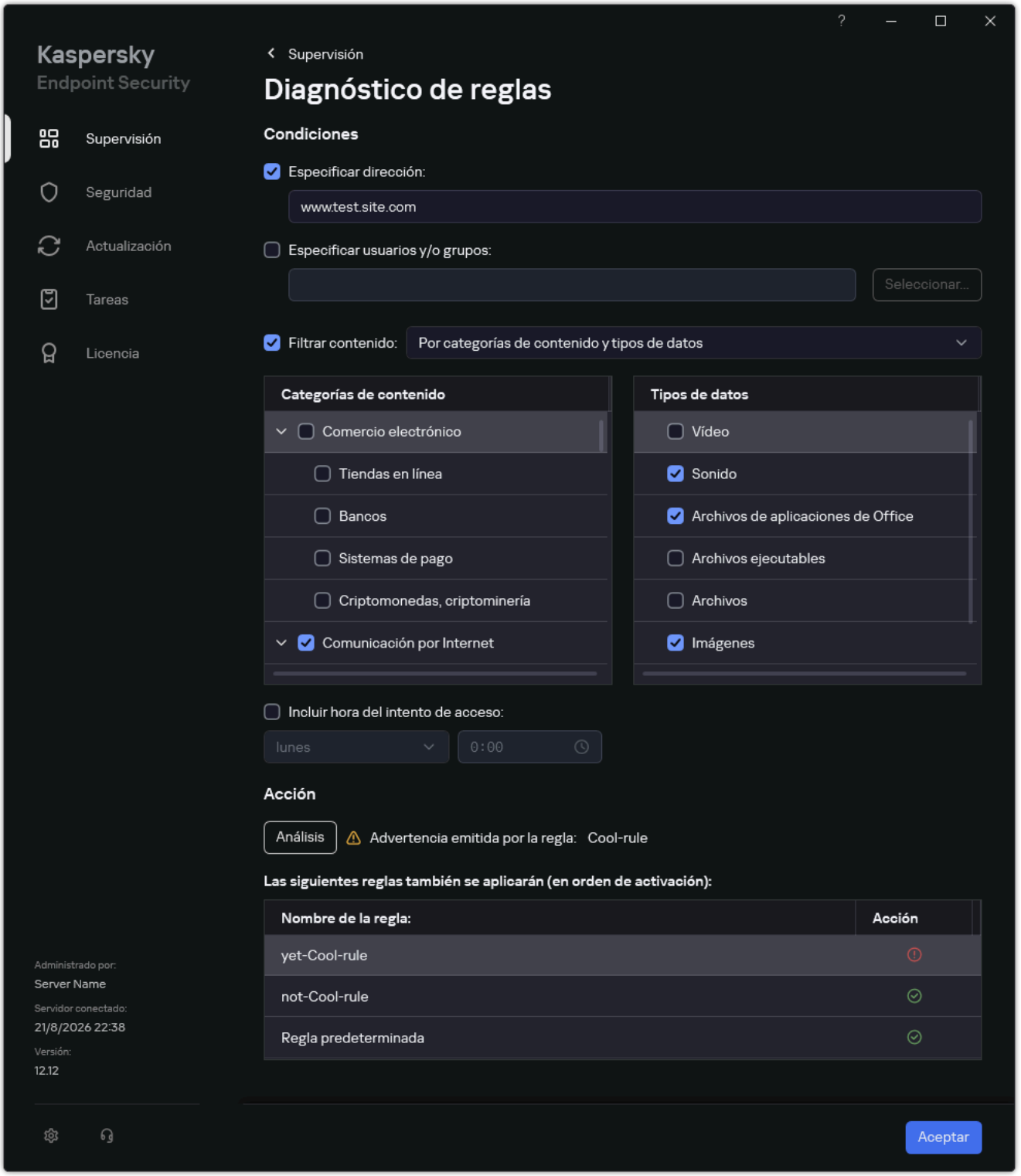
5. Si quiere probar las reglas que Kaspersky Endpoint Security utiliza para controlar el acceso a recursos web para usuarios y grupos de usuarios especificados, especifique una lista de usuarios o grupos de usuarios.

6. Si quiere probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a recursos web de ciertas categorías de contenido o categorías de tipos de datos, seleccione la casilla de verificación **Filtrar contenido** y elija la opción correspondiente de la lista desplegable (**Por categorías de contenido**, **Por tipos de datos** o **Por categorías de contenido y tipos de datos**).

7. Si quiere probar las reglas que tienen en cuenta la hora y el día de la semana cuando se realiza un intento de acceder a los recursos web especificados en las condiciones del diagnóstico de reglas, seleccione la casilla de verificación **Incluir hora del intento de acceso**. A continuación, especifique el día de la semana y la hora.

8. Haga clic en **Análisis**.

Después de que se complete la prueba, aparece un mensaje con información sobre la acción que realiza Kaspersky Endpoint Security, de acuerdo con la primera regla activada ente un intento de acceso al recurso web especificado (autorizar, bloquear o advertencia). La primera regla que se activa es la primera con un rango en la lista de reglas de Control Web superior al de otras reglas que cumplen las condiciones de diagnóstico. El mensaje se muestra a la derecha del botón **Análisis**. La siguiente tabla incluye las reglas restantes activadas, en las que se especifica la acción que ha llevado a cabo Kaspersky Endpoint Security. Las reglas se incluyen en orden de prioridad decreciente.



Exportación e importación de reglas de Control Web

Puede exportar la lista de reglas de Control Web a un archivo XML o JSON. Luego puede modificar el archivo para, por ejemplo, añadir una gran cantidad de direcciones del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de Control Web o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de reglas de Control Web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control Web**.
4. Para exportar la lista de reglas de Control Web, haga lo siguiente:
   a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
   b. Haga clic en el enlace **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
   d. Guarde el archivo.
      Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.
5. Para importar la lista de reglas de Control Web, haga lo siguiente:
   a. Haga clic en el enlace **Importar**.
      En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
   b. Abra el archivo.
      Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
6. Guarde los cambios.

Cómo exportar e importar una lista de reglas de Control Web en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control Web**.

5. Para exportar la lista de reglas, en el bloque **Lista de reglas**:

   a. Seleccione las reglas que quiera exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de reglas a un archivo JSON en la carpeta de descargas predeterminada.

6. Para importar la lista de reglas, en el bloque **Lista de reglas**:

   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que desea importar la lista de reglas.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

7. Guarde los cambios.

Exportar e importar direcciones de recursos web de la regla de Control Web

Si ha creado una lista de direcciones de recursos web en una regla de acceso a recursos web, puede exportarla a un archivo:

- en formato TXT a la Consola de administración (MMC);
- En formato JSON en Web Console
- en formato CSV a la interfaz de la aplicación.

Puede importar en veces sucesivas la lista desde este archivo para evitar la creación de una nueva lista de direcciones de recursos web manualmente al configurar una regla de acceso. La opción de exportación e importación de la lista de direcciones de recursos web puede ser útil si, por ejemplo, crea reglas de acceso son parámetros similares.

También puede exportar/importar todas las reglas de Control Web, y no únicamente las direcciones de recursos web de una regla individual.

Cómo exportar e importar direcciones de recursos web de la regla de Control Web en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control Web**.

5. En el bloque **Configuración de Control Web**, seleccione la regla cuya lista de direcciones de recursos web desee exportar o importar.

   Aparecen las propiedades de la regla de Control Web.

6. Para importar la lista de recursos web, haga lo siguiente en la lista de direcciones:

   a. Seleccione las direcciones que desea exportar.

      Si no seleccionó ninguna dirección, Kaspersky Endpoint Security exportará todas las direcciones.

   b. Haga clic en el botón .

   c. En la ventana que se abre, introduzca el nombre del archivo TXT al que desea exportar la lista de direcciones de recursos web y seleccione la carpeta en la que desea guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de direcciones de recursos web a un archivo TXT.

7. Para importar la lista de recursos web, haga lo siguiente en la lista de direcciones:

   a. Haga clic en el botón .

      En la ventana que se abre, seleccione el archivo TXT del que importar la lista de recursos web.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de direcciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo TXT.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo exportar e importar direcciones de recursos web de la regla de Control web en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control Web**.

5. En el bloque **Lista de reglas**, seleccione la regla cuya lista de direcciones de recursos web desee exportar o importar.

   Aparecen las propiedades de la regla de Control Web.

6. En el bloque **Alcance** → **Sitios web individuales**, haga clic en el botón **Modificar**.

7. Para importar la lista de recursos web, haga lo siguiente en la lista de direcciones:

   a. Seleccione las direcciones que desea exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de direcciones de recursos web a un archivo JSON en la carpeta de descargas predeterminada.

8. Para importar la lista de recursos web, haga lo siguiente en la lista de direcciones:

   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que desea importar la lista de direcciones de recursos web.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de direcciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

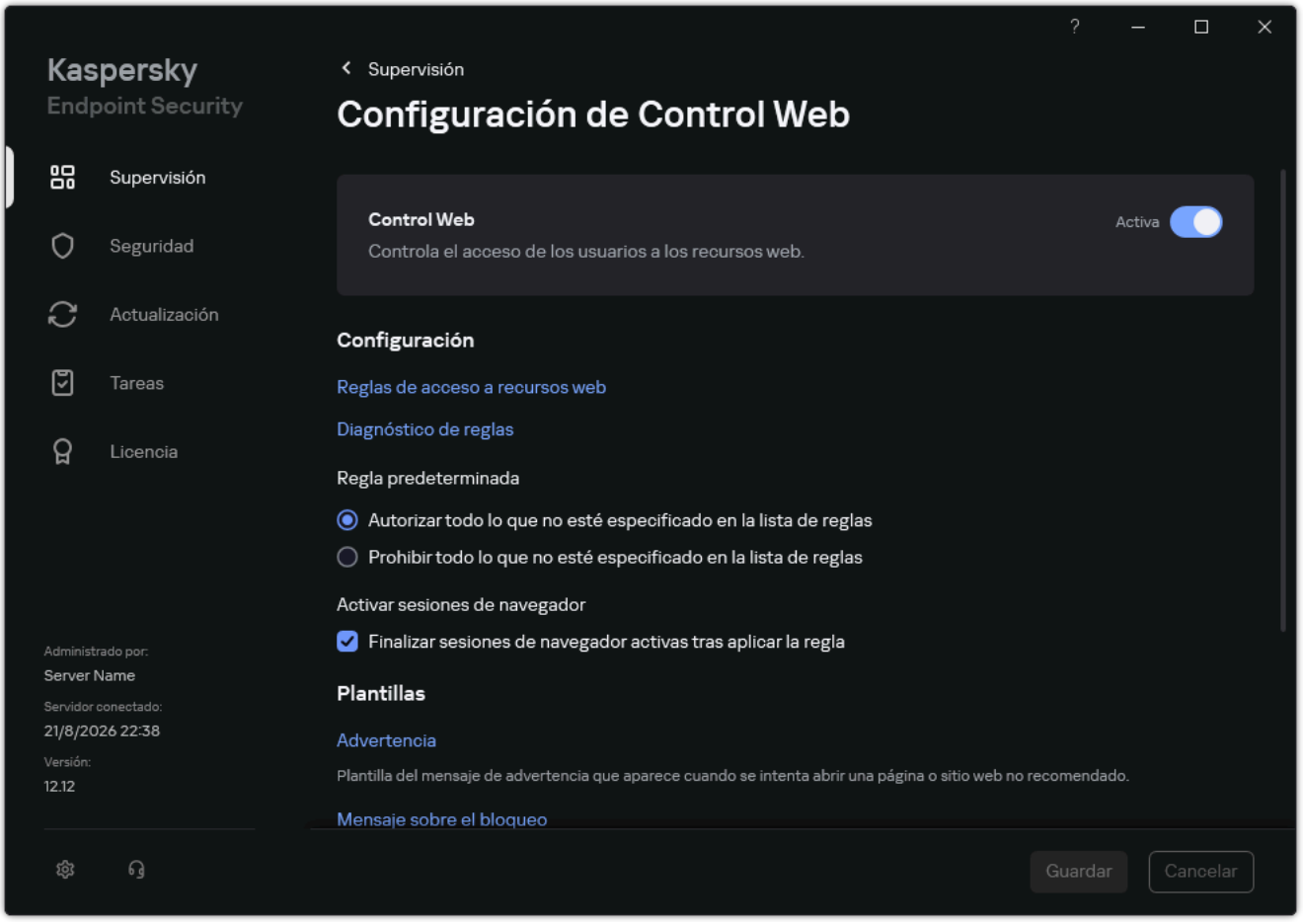
   Puede exportar e importar grupos de sitios web de la misma manera.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo exportar e importar direcciones de recursos web de la regla de Control Web en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.



Configuración de Control Web

3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.

4. Seleccione la regla cuya lista de direcciones de recursos web desee exportar o importar.

5. Para exportar la lista de direcciones web de confianza, haga lo siguiente en el bloque **Direcciones**:

   a. Seleccione las direcciones que desea exportar.

      Si no seleccionó ninguna dirección, Kaspersky Endpoint Security exportará todas las direcciones.

   b. Haga clic en **Exportar**.

   c. En la ventana que se abre, introduzca el nombre del archivo CSV al que desea exportar la lista de direcciones de recursos web y seleccione la carpeta en la que desea guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de direcciones de recursos web a un archivo CSV.

6. Para importar la lista de recursos web, haga lo siguiente en el bloque **Direcciones**:

   a. Haga clic en **Importar**.

      En la ventana que se abre, seleccione el archivo CSV del que importar la lista de recursos web.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de direcciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo CSV.

7. Guarde los cambios.

Supervisión de las actividades de los usuarios en Internet

Kaspersky Endpoint Security puede registrar información sobre todos los sitios web que visitan los usuarios, incluso cuando se trata de sitios web permitidos. Esto hace posible obtener un historial de navegación completo. Kaspersky Endpoint Security envía los eventos sobre las actividades de los usuarios a Kaspersky Security Center, al registro local de Kaspersky Endpoint Security y al registro de eventos de Windows. Para recibir estos eventos en Kaspersky Security Center, deberá configurar los ajustes de los eventos en una directiva, ya sea a través de Web Console o con la Consola de administración. Dependiendo de la configuración, los eventos de Control web también pueden transmitirse por correo electrónico o mostrarse en el equipo del usuario a través de notificaciones en pantalla.

Navegadores que admiten la función de supervisión: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. La supervisión de las actividades de los usuarios no funciona en otros navegadores.

Cuando un usuario utiliza Internet, Kaspersky Endpoint Security crea los siguientes eventos:

- Bloqueo del sitio web (estado *Crítico*).
- Visita a un sitio web no recomendado (estado *Advertencia*).
- Visita a un sitio web permitido (estado *Información*).

Antes de activar la supervisión de la actividad de Internet del usuario, debe hacer lo siguiente:

- Inyecte un script de interacción de la página web en el tráfico web (consulte las instrucciones a continuación). El script permite el registro de eventos de Control web.
- Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario activar el análisis de conexiones cifradas.

Inyección de un script de interacción de una página web

Cómo inyectar un script de interacción de una página web en el tráfico web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
4. En el bloque **Análisis de conexiones cifradas**, seleccione la casilla de verificación **Insertar scripts en el tráfico web para interactuar con las páginas web**.
5. Guarde los cambios.

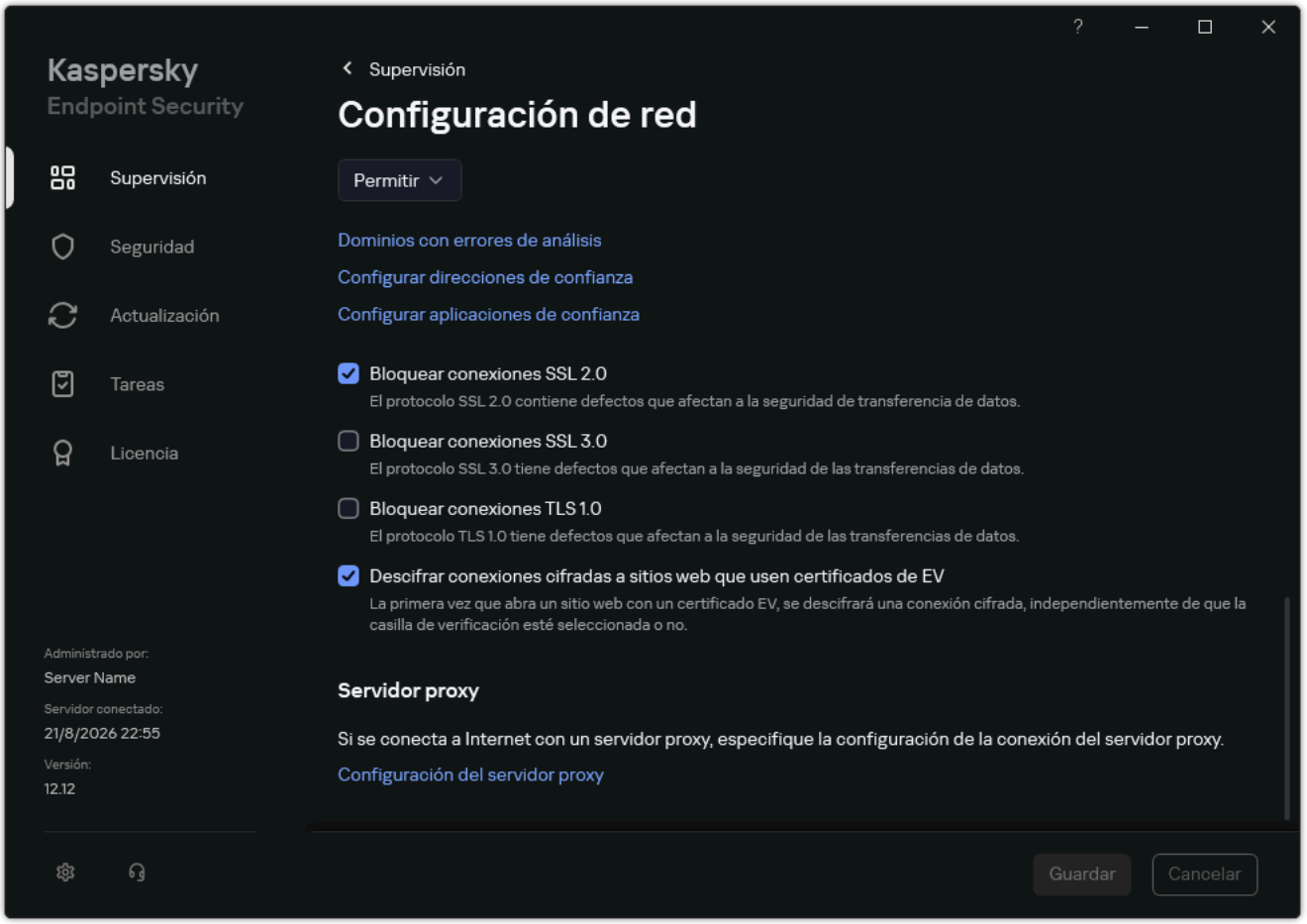
Cómo inyectar un script de interacción de una página web en el tráfico web en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
5. En **Supervisión de conexiones a Internet**, active el interruptor **Supervisión de conexiones a Internet ACTIVADA**.
6. Guarde los cambios.

Cómo inyectar un script de interacción de una página web en el tráfico web en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.



Configuración de red de aplicaciones

3. En el bloque **Procesamiento de tráfico**, seleccione la casilla de verificación **Insertar scripts en el tráfico web para interactuar con las páginas web**.
4. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security inyectará un script de interacción de la página web en el tráfico web. Este script permite el registro de eventos de Control web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Configuración del registro de eventos de Control web

Para que los eventos de Control web se registren en el equipo del usuario:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En el bloque **Notificaciones**, haga clic en el botón **Configurar notificaciones**.

4. En la ventana que se abre, seleccione la sección **Control Web**.

   Se abrirá una tabla con los eventos de Control web y los distintos métodos de notificación.

5. Configure el método de notificación para cada evento: **Guardar en informe local** o **Guardar en Registro de eventos de Windows**.

   Para que se registren las visitas a sitios web permitidos, también deberá hacer cambios en la configuración de Control web (consulte las instrucciones más abajo).

   A través de la tabla de eventos también podrá activar las notificaciones en pantalla y las notificaciones por correo electrónico. Para que la aplicación envíe notificaciones por correo electrónico, deberá configurar los ajustes del servidor SMTP. Para obtener más información sobre el envío de notificaciones por correo electrónico, consulte la Ayuda de Kaspersky Security Center.

6. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security comenzará a registrar los eventos relacionados con las actividades en Internet del usuario.

Control web envía los eventos sobre las actividades de los usuarios a Kaspersky Security Center de la siguiente manera:

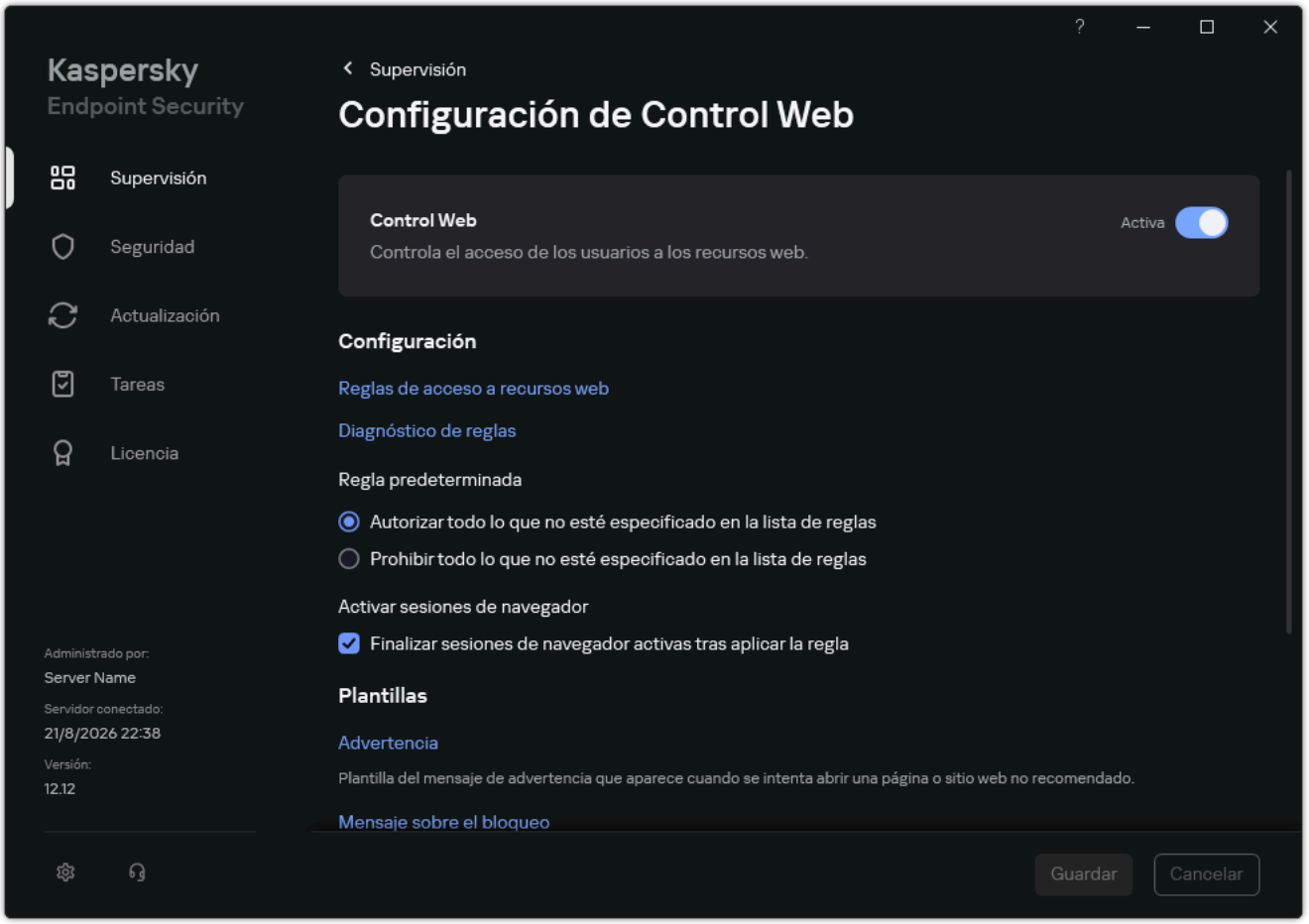
- Si utiliza Kaspersky Security Center, Control web envía los eventos para todos los objetos que componen la página web. Por este motivo, cada página web bloqueada podría dar lugar a más de un evento. Por ejemplo, si se bloquea la página web http://www.example.com, Kaspersky Endpoint Security podría transmitir eventos sobre los objetos http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js, etc.

- Si utiliza Kaspersky Security Center Cloud Console, Control web agrupa los eventos y solo envía el protocolo y el dominio del sitio web. Por ejemplo, si un usuario abre las páginas web no recomendadas http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, Kaspersky Endpoint Security enviará solo un evento con el objeto http://www.example.com.

Registro de eventos al visitar sitios web permitidos

Para que se registren los eventos al visitar sitios web permitidos:

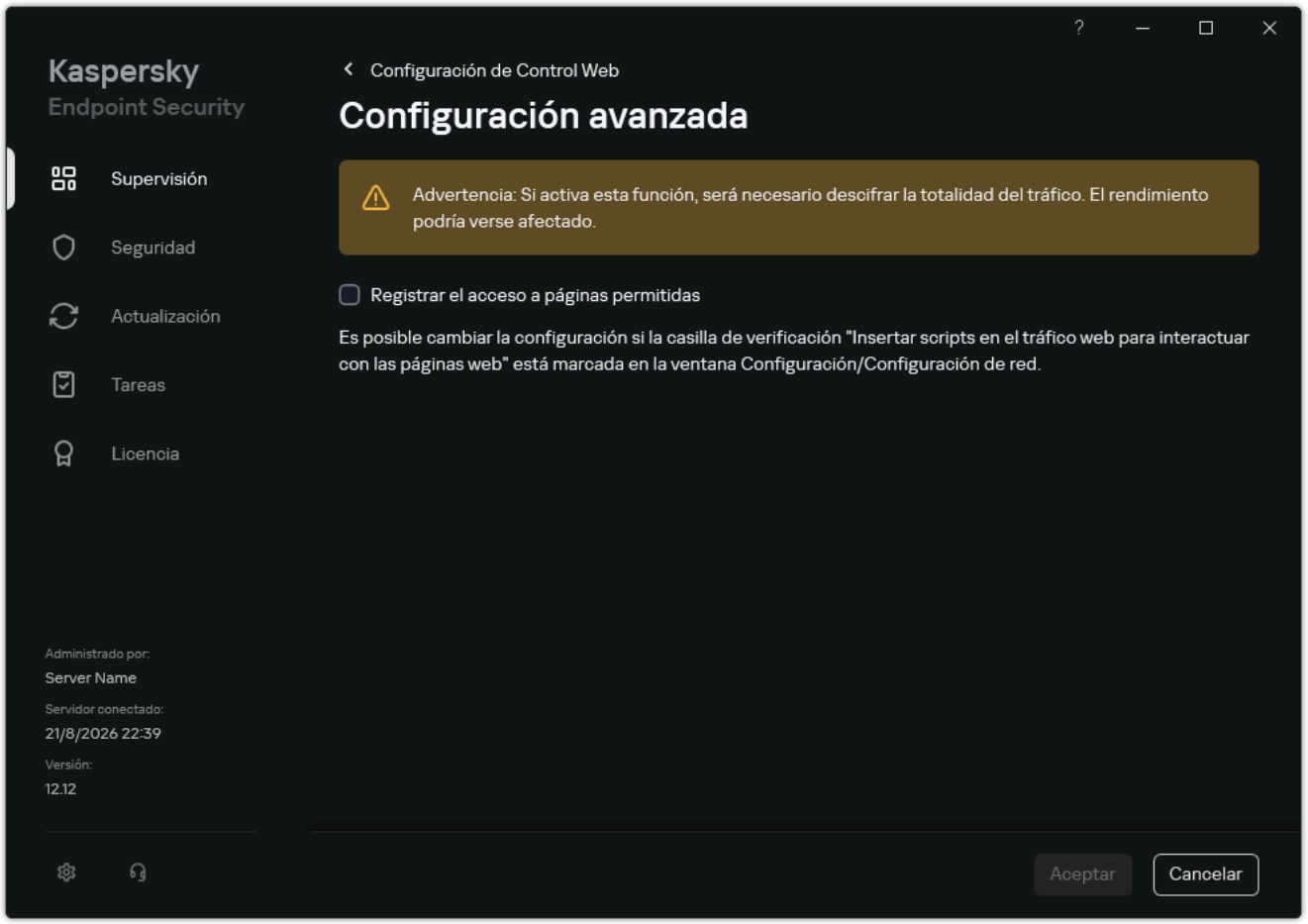
1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.



Configuración de Control Web

3. En el bloque **Adicional**, haga clic en el botón **Configuración avanzada**.

4. En la ventana que se abre, active la casilla **Registrar el acceso a páginas permitidas**.



Configuración avanzada de Control Web

5. Guarde los cambios.

Como resultado, podrá ver el historial de navegación completo.

Edición de plantillas de mensajes de Control Web

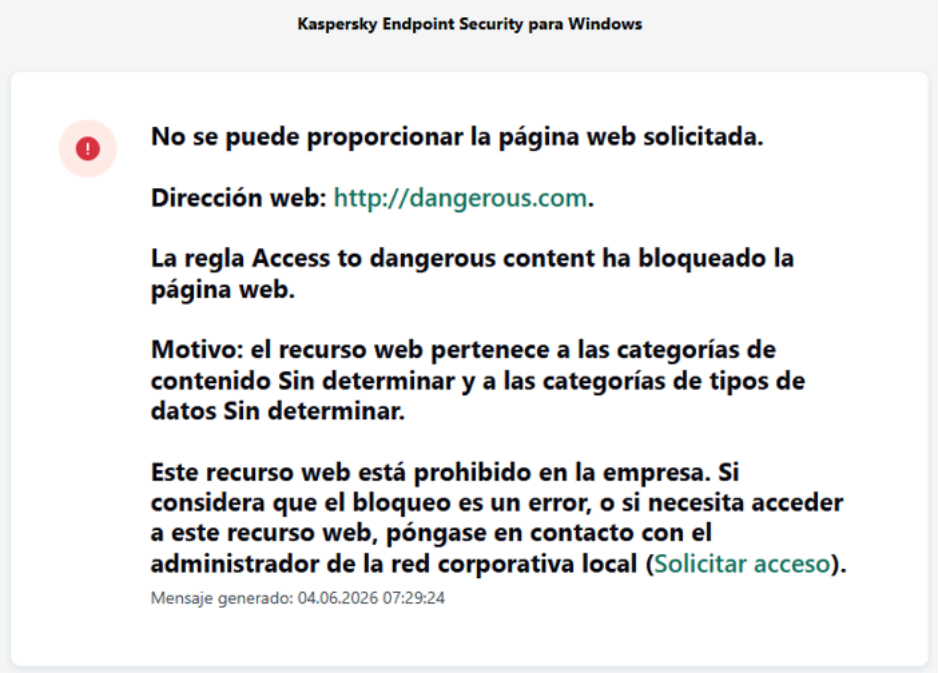
Dependiendo del tipo de acción seleccionado en las propiedades de las reglas de Control Web, Kaspersky Endpoint Security muestra un mensaje de uno de los siguientes tipos cuando los usuarios intentan acceder a recursos de Internet (la aplicación sustituye una página HTML por un mensaje para la respuesta para el servidor HTTP):

- Mensaje de advertencia. Este mensaje advierte al usuario de que no se recomienda visitar el recurso web o de que este infringe la directiva corporativa de seguridad. Kaspersky Endpoint Security muestra un mensaje de advertencia si se selecciona la opción **Advertir** en la configuración de la regla que describe este recurso web.

  Si el usuario cree que la advertencia es un error, este puede hacer clic en el enlace de la advertencia para enviar un mensaje generado previamente al administrador de la red de área local.

- Mensaje que informe del bloqueo de un recurso web. Kaspersky Endpoint Security muestra un mensaje que informa de que se ha bloqueado un recurso web (consulte la figura que aparece más adelante) si se selecciona la opción **Bloquear** en la configuración de la regla que describe este recurso web.

Si el usuario cree que el recurso web está bloqueado por error, este puede hacer clic en el enlace del mensaje que informa del bloqueo del recurso web para enviar un mensaje generado previamente y enviárselo al administrador de la red de área local.



Mensaje sobre bloqueo de recursos web

Se proporcionan plantillas especiales para un mensaje de advertencia, el mensaje que informe de que se ha bloqueado un recurso web y el mensaje que se envía al administrador de la LAN. Se proporcionan variables especiales para administrar la plantilla de mensaje (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensaje para diferentes ordenadores. Al generar un mensaje, Kaspersky Endpoint Security recupera el valor de la variable de la configuración del sistema operativo y lo inserta en el mensaje correspondiente al equipo, usuario y evento específicos.

Cómo cambiar la plantilla de mensaje de Control web en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control Web**.
4. En el bloque **Configuración de la plantilla de mensajes**, haga clic en el botón **Plantillas**.
5. Configure las plantillas de mensajes de Control web:
   - **Advertencia**. El campo de entrada consta de una plantilla del mensaje que se muestra si se activa una regla de advertencia sobre intentos de acceso a un recurso web no deseado.
   - **Mensaje sobre el bloqueo**. El campo de entrada contiene la plantilla del mensaje que aparece si se activa una regla que bloquee el acceso a un recurso web.
   - **Mensaje al administrador**. La plantilla del mensaje que se enviará al administrador de la LAN si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso a la página web**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y elija la variable requerida de la lista de opciones disponibles.

También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Predeterminado**.

6. Guarde los cambios.

Cómo cambiar la plantilla del mensaje en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control Web**.
5. En el bloque **Plantillas de mensajes**, haga clic en el vínculo **Mensaje sobre bloqueo de sitios web** y configure plantillas para mensajes de Control web:

   - **Advertencia**. El campo de entrada consta de una plantilla del mensaje que se muestra si se activa una regla de advertencia sobre intentos de acceso a un recurso web no deseado.
   - **Mensaje sobre el bloqueo**. El campo de entrada contiene la plantilla del mensaje que aparece si se activa una regla que bloquee el acceso a un recurso web.
   - **Mensaje al administrador**. La plantilla del mensaje que se enviará al administrador de la LAN si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso a la página web**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

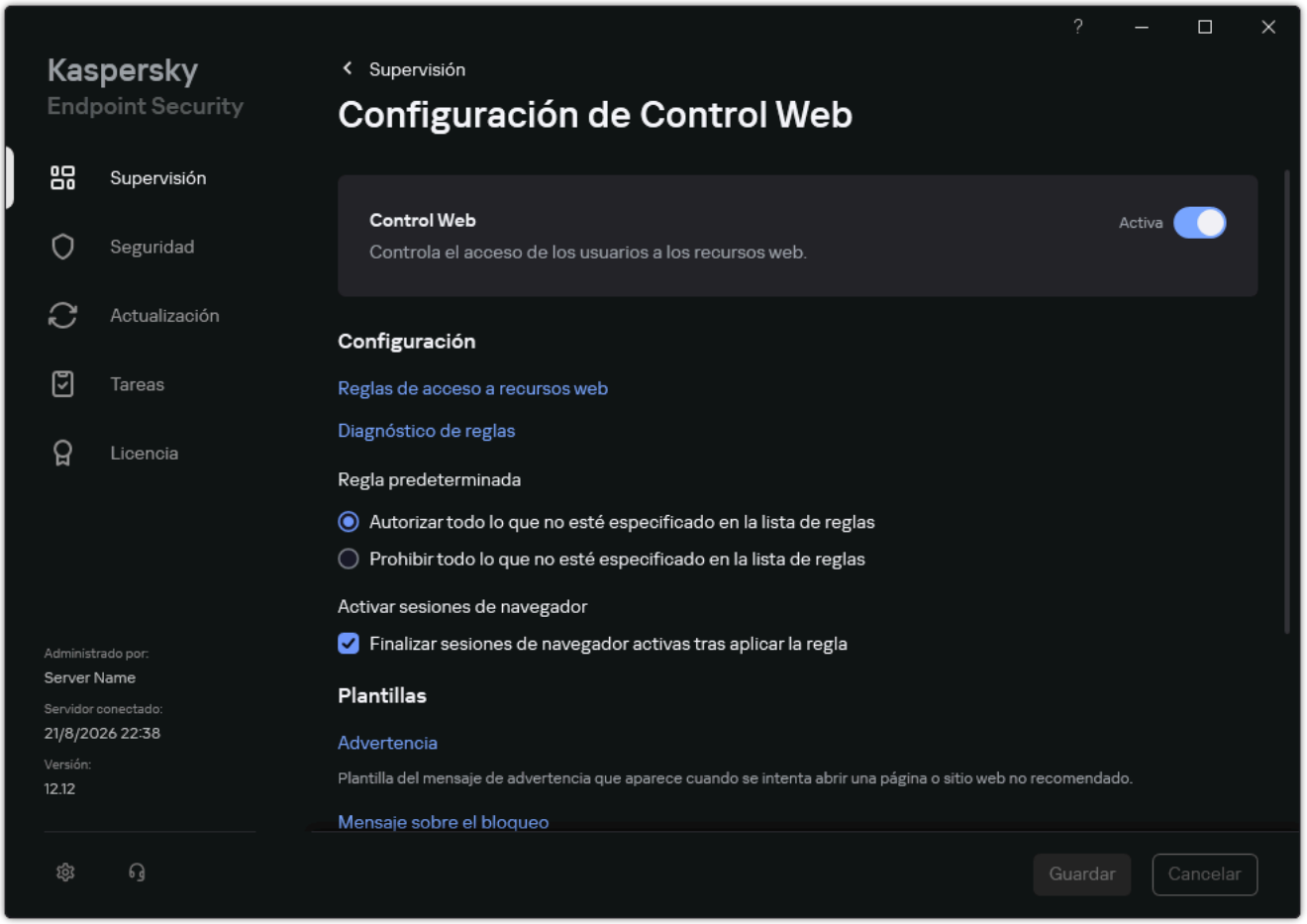
   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Restablecer valores predeterminados**.
6. Guarde los cambios.

Cómo cambiar la plantilla del mensaje de Control web en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.



Configuración de Control Web

3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control web:

   - **Advertencia**. El campo de entrada consta de una plantilla del mensaje que se muestra si se activa una regla de advertencia sobre intentos de acceso a un recurso web no deseado.

   - **Mensaje sobre el bloqueo**. El campo de entrada contiene la plantilla del mensaje que aparece si se activa una regla que bloquee el acceso a un recurso web.

   - **Mensaje para el administrador**. La plantilla del mensaje que se enviará al administrador de la LAN si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso a la página web**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Restablecer**.

4. Guarde los cambios.

Edición de máscaras para direcciones de recursos web

El uso de una *máscara para direcciones de recursos web* (también denominada "máscara de dirección") puede resultar útil si tiene que introducir varias direcciones de recursos web similares al crear una regla de acceso a recursos web. Si se elabora correctamente, una máscara de dirección puede sustituir un gran número de direcciones de recursos web.

Siga estas reglas si va a crear una máscara de dirección:

1. El carácter `*` sustituye cualquier secuencia que contenga cero caracteres o más.

   Por ejemplo, si introduce la máscara de dirección `*abc*`, la regla de acceso se aplica a todos los recursos web que contengan la secuencia `abc`. Ejemplo: `http://www.example.com/page_0-9abcdef.html`.

2. Una secuencia de caracteres `*.` (conocida como *máscara de dominio*) le permite seleccionar todos los dominios de una dirección. La máscara de dominio `*.` representa cualquier nombre de dominio, nombre de subdominio o una línea en blanco.

   Ejemplo: la máscara `*.example.com` representa las siguientes direcciones:

   - `http://pictures.example.com`. La máscara de dominio `*.` representa `pictures.`.
   - `http://user.pictures.example.com`. La máscara de dominio `*.` representa `pictures.` y `user.`.
   - `http://example.com`. La máscara de dominio `*.` se interpreta como una línea en blanco.

3. La secuencia de caracteres `www.` que se encuentra al comienzo de cualquier máscara de dirección se interpreta como `*.`.

   Ejemplo: la máscara de dirección `www.example.com` se interpreta como `*.example.com`. Esta máscara cubre las direcciones `www2.example.com` y `www.pictures.example.com`.

4. Si una máscara de dirección no comienza con el carácter `*`, su contenido será equivalente al mismo contenido con el prefijo `*.`.

5. Si una máscara de dirección termina con un carácter distinto de `/` o `*`, su contenido será equivalente al mismo contenido que con el sufijo `/*`.

   Ejemplo: la máscara de dirección `http://www.example.com` incluye direcciones como `http://www.example.com/abc` donde `a`, `b` y `c` son cualesquiera caracteres.

6. Si una máscara de dirección termina con el carácter `/`, su contenido será equivalente al mismo contenido que con el sufijo `/*`.

7. La secuencia de caracteres `/*` al final de una máscara de dirección se considera como `/*` o como una cadena vacía.

8. Las direcciones de recursos web se contrastan con una máscara de dirección y se tiene en cuenta el protocolo (http o https):

   - Si la máscara de dirección no contiene ningún protocolo de red, dicha máscara de dirección abarca direcciones con cualquier protocolo de red.

     Ejemplo: la máscara de dirección `example.com` abarca las direcciones `http://example.com` y `https://example.com`.

- Si la máscara de dirección contiene un protocolo de red, dicha máscara de dirección abarca únicamente direcciones con el mismo protocolo de red que el de la máscara de dirección.

  Ejemplo: la máscara de dirección `http://*.example.com` incluye la dirección `http://www.example.com`, pero no incluye `https://www.example.com`.

9. Una máscara de dirección entre comillas dobles se trata sin tener en cuenta ninguna sustitución adicional, excepto el carácter `*` si se ha incluido inicialmente en la máscara de dirección. Las reglas 5 y 7 no se aplican a las máscaras de dirección que aparezcan dentro de dobles comillas (ver ejemplos 14-18 en la siguiente tabla).

10. Durante la comparación con la máscara de dirección de un recurso web no se tienen en cuenta el nombre de usuario, la contraseña, el puerto de conexión ni la diferencia entre mayúsculas y minúsculas de los caracteres.

Ejemplos de cómo utilizar reglas para crear máscaras de dirección

No.	Máscara de dirección	Dirección de un recurso web para verificar	Es la dirección que abarca la máscara de dirección	Comentario
1	*.ejemplo.com	http://www.123example.com	No	Consulte la regla 1.
2	*.ejemplo.com	http://www.123.example.com	Sí	Consulte la regla 2.
3	*ejemplo.com	http://www.123example.com	Sí	Consulte la regla 1.
4	*ejemplo.com	http://www.123.example.com	Sí	Consulte la regla 1.
5	http://www.*.ejemplo.com	http://www.123example.com	No	Consulte la regla 1.
6	www.ejemplo.com	http://www.example.com	Sí	Consulte las reglas 3, 2 y 1.
7	www.ejemplo.com	https://www.example.com	Sí	Consulte las reglas 3, 2 y 1.
8	http://www.*.ejemplo.com	http://123.example.com	Sí	Consulte las reglas 3, 4 y 1.
9	www.ejemplo.com	http://www.example.com/abc	Sí	Consulte las reglas 3, 5 y 1.
10	ejemplo.com	http://www.example.com	Sí	Consulte las reglas 3 y 1.
11	http://ejemplo.com/	http://example.com/abc	Sí	Consulte la regla 6.
12	http://ejemplo.com/*	http://ejemplo.com	Sí	Consulte la regla 7.
13	http://ejemplo.com	https://example.com	No	Consulte la regla 8.
14	"ejemplo.com"	http://www.example.com	No	Consulte la regla 9.
15	"http://www.ejemplo.com"	http://www.example.com/abc	No	Consulte la regla 9.
16	"*.ejemplo.com"	http://www.example.com	Sí	Consulte las reglas 1 y 9.
17	"http://www.ejemplo.com/*"	http://www.example.com/abc	Sí	Consulte las reglas 1 y 9.
18	"www.ejemplo.com"	http://www.example.com; https://www.example.com	Sí	Consulte las reglas 9 y 8.
19	www.ejemplo.com/abc/123	http://www.example.com/abc	No	Una máscara de dirección contiene más información aparte de la dirección de un recurso web.

Control web para máquinas virtuales

Control web controla el tráfico en el equipo, así como en una máquina virtual que se implementa localmente en el equipo. Esto funciona sin necesidad de instalar la aplicación Kaspersky Endpoint Security en la máquina virtual local. Esto significa que si el usuario intenta abrir un sitio web que está bloqueado por una regla de Control web en un navegador en la *maquina virtual*, la aplicación instalada en el sistema operativo host del *equipo* niega el acceso a ese sitio web.

Control web funciona de manera diferente en diferentes máquinas virtuales.

Oracle VM VirtualBox

Kaspersky Endpoint Security admite reglas de Control web en máquinas virtuales Oracle VM VirtualBox sin limitaciones. La aplicación puede controlar todo el tráfico de la máquina virtual. Si se configura un filtro por usuario en las reglas de Control web, la aplicación funciona correctamente porque el usuario local inicia todos los procesos de las máquinas virtuales.

VMware Workstation

Kaspersky Endpoint Security admite reglas de Control web en máquinas virtuales Vmware Workstation con limitaciones. La aplicación no admite reglas con filtro por usuario configurado. Los procesos de la máquina virtual se ejecutan bajo el usuario del sistema (SYSTEM). Esto hace que sea imposible identificar al usuario que está intentando abrir el sitio web en la máquina virtual.

Microsoft Hyper-V

Kaspersky Endpoint Security no admite reglas de Control web en máquinas virtuales Microsoft Hyper-V.

Variables en las plantillas de mensajes de Control web:

Puede utilizar las siguientes variables en las plantillas de mensajes de usuario o las plantillas de mensajes de administrador:

- **Nombre de usuario** - `%USER_NAME%`.

  Nombre de la cuenta de usuario actual en el equipo en el que se generó el mensaje, en formato `<device name>\<user alias>` (por ejemplo, `DESKTOP-123\John.Smith`).

- **Dirección de recurso web** - `%CANONIC_REQUEST_URL%`.

  Dirección del recurso web bloqueado.

- **Nombre de la regla** - `%RULE%`.

  Nombre de la regla que bloqueó el recurso web.

- **Correo electrónico para el envío de mensajes** - `%COMPLAIN_EMAIL%`.

  Dirección de correo electrónico para recibir comentarios sobre los bloques de recursos web. Al hacer clic en la dirección de correo electrónico, se abre una ventana en la que el usuario puede escribir un mensaje al administrador.

- **Nombre de la categoría de contenido** - `%CONTENT_CATEGORY_LIST%`.

  Categoría de sitio web a la que pertenece el recurso bloqueado (por ejemplo, *Sistemas de pago*).

- **Nombre de la categoría del tipo de datos** - `%TYPE_CATEGORY_LIST%`.

  Categoría de tipo de datos en el recurso web bloqueado (por ejemplo, *Imágenes*).

- **Vínculo al recurso web solicitado** - `%CONTINUE_PAGE%`.

  Enlace a la página web solicitada (por ejemplo, `http://www.example.com/pagename.html`).

- **Vínculo al sitio web** - `%CONTINUE_SITE%`.

  Enlace al sitio web que contiene la página web solicitada (por ejemplo, `http://www.example.com/`).

- **Vínculo para acceder a dominios** - `%CONTINUE_DOMAIN%`.

  Enlace en el que se puede hacer clic para obtener acceso a todas las páginas web existentes del nombre de dominio. Por ejemplo, si la dirección de la página web bloqueada es `http://www.example.com`, la variable `%CONTINUE_DOMAIN%` se reemplaza con el vínculo `http://*.example.com`. Al hacer clic en este enlace se permite el acceso a todas las direcciones web del nombre de dominio base `http://www.example.com/` incluidos los subdominios, por ejemplo, `http://start.example.com/*` o `http://domain.domain.example.com/*`, donde el carácter `*` representa cualquier secuencia de caracteres (incluida una cadena vacía).

Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi). Esto le permite proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos.

Si el Control de dispositivos está activado, la aplicación transmite información sobre los dispositivos conectados a Kaspersky Security Center. Puede ver la lista de dispositivos conectados en Kaspersky Security Center en la carpeta **Avanzado** → **Repositorios** → **Hardware**.

Niveles de acceso a dispositivos

Control de dispositivos controla el acceso a los siguientes niveles:

- **Tipo de dispositivo**. Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

  Puede configurar el acceso a los dispositivos del siguiente modo:

  - Permitir – .
  - Bloquear – .
  - Por las reglas (solo impresoras y dispositivos portátiles) – .
  - Depende del bus de conexión (excepto wifi): .
  - Bloquear con excepciones (solo wifi): .

- **Bus de conexión**. Un *bus de conexión* es una interfaz usada para conectar dispositivos al equipo (por ejemplo, USB o FireWire). Si se selecciona el modo **Depende del bus de conexión** para el tipo de dispositivo, la aplicación permite o deniega el acceso al dispositivo según la interfaz de conexión (por ejemplo, USB).

Puede configurar el acceso a los dispositivos del siguiente modo:

- Permitir – ✓.
- Bloquear – ⊘.

- **Dispositivos de confianza**. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

  Puede añadir dispositivos de confianza según los siguientes datos:

  - **Dispositivos por ID**. Cada dispositivo tiene un identificador exclusivo (Hardware ID o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. Ejemplo de ID de dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.
  - **Dispositivos por modelo**. Cada dispositivo tiene un Vendor ID (VID) y un Product ID (PID). Puede ver los ID en las propiedades del dispositivo usando herramientas del sistema operativo. Plantilla para introducir el VID y el PID: `VID_1234&PID_5678`. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.
  - **Dispositivos por máscara de ID**. Si utiliza varios dispositivos con ID similares, puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `WDC_C*`.
  - **Dispositivos por máscara de modelo**. Si utiliza varios dispositivos con VID y PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `VID_05AC&PID_*`.

Control de dispositivos regula el acceso de los usuarios a dispositivos usando *reglas de acceso*. Control de dispositivos también le permite guardar eventos de conexión/desconexión de dispositivos. Para guardar eventos, tiene que configurar el registro de eventos en una directiva.

Cuando el acceso a un dispositivo dependa del bus de conexión (estado ◔), Kaspersky Endpoint Security no guardará ningún evento relacionado con la conexión o desconexión del dispositivo. Para que Kaspersky Endpoint Security guarde eventos de conexión/desconexión, debe autorizar el acceso al tipo de dispositivo correspondiente (estado ✓) o añadir el dispositivo a la lista de dispositivos de confianza.

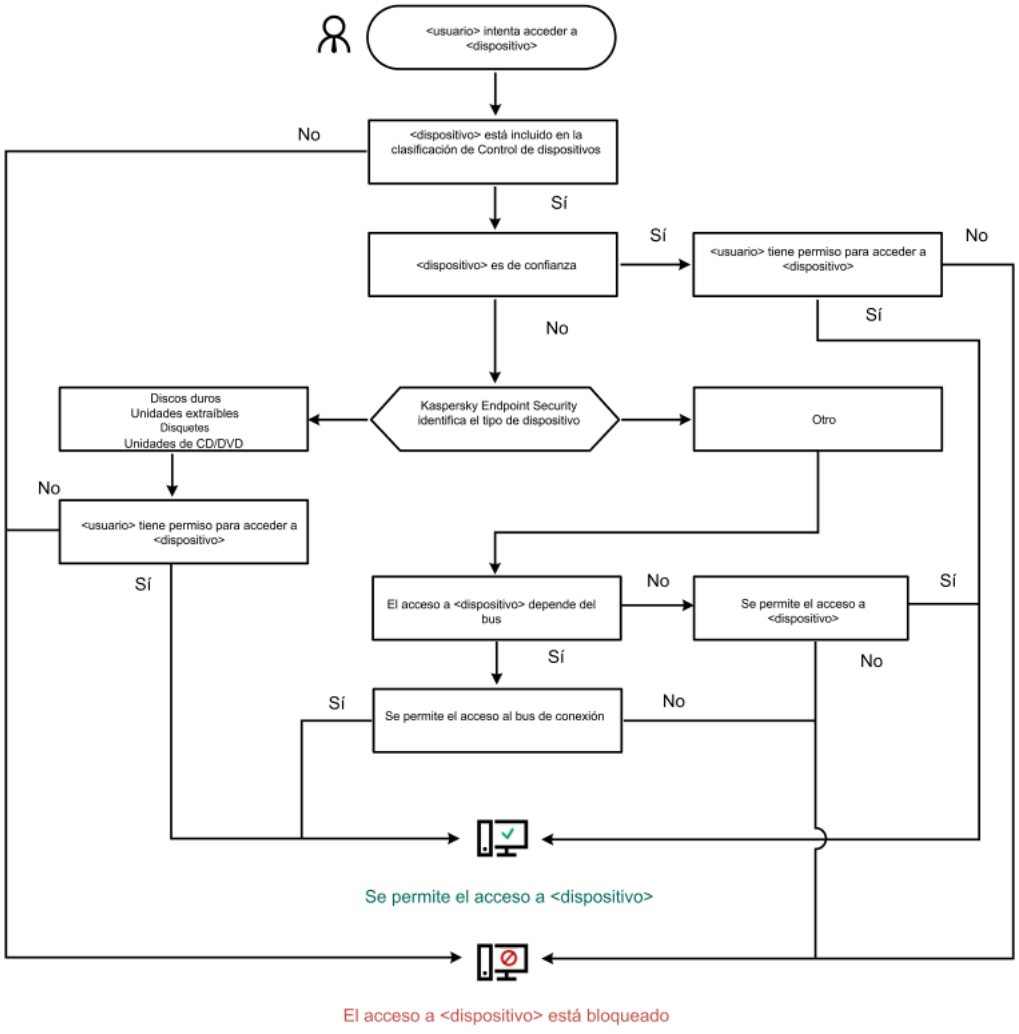
Cuando un dispositivo que está bloqueado por Control de dispositivos se conecte al equipo, Kaspersky Endpoint Security bloqueará el acceso y mostrará una notificación (véase la figura siguiente).



Notificación de Control de dispositivos

Algoritmo de funcionamiento de Control de dispositivos

Kaspersky Endpoint Security toma una decisión sobre si permitir el acceso a un dispositivo después de que el usuario conecte un dispositivo al equipo de la siguiente imagen.



Algoritmo de funcionamiento de Control de dispositivos

Si conecta un dispositivo y se le permite acceder a él, puede editar la regla de acceso y bloquear la posibilidad de utilizarlo. Cuando alguien intente acceder al dispositivo nuevamente (por ejemplo, para ver la estructura de carpetas o para realizar una operación de lectura o escritura), Kaspersky Endpoint Security bloqueará el acceso. Un dispositivo sin sistema de archivos solo se bloquea la próxima vez que se conecta el dispositivo.

Si un usuario del equipo donde se ha instalado Kaspersky Endpoint Security debe solicitar el acceso a un dispositivo que el usuario cree que se bloqueó por equivocación, envíe al usuario las instrucciones para solicitar acceso.

Sobre las reglas de acceso

Una *regla de acceso al dispositivo* es un grupo de ajustes de configuración que determina cómo los usuarios pueden acceder a dispositivos instalados en un equipo o conectados a él. Esta configuración incluye acceso a un dispositivo específico, un horario de acceso y permisos de lectura o escritura. No puede añadir un dispositivo que no pertenezca a la clasificación de Control de dispositivos. El acceso a tales dispositivos está permitido para todos los usuarios.

Reglas de acceso a dispositivos

El grupo de ajustes de configuración para una regla del acceso depende del tipo de dispositivo (consulte la tabla a continuación).

Ajustes de reglas de acceso

Dispositivos	Control de acceso	Planificar el acceso a un dispositivo	Asignación de usuarios y/o un grupo de usuarios	Prioridad	Permiso de lectura/escritura
Discos duros	✓	✓	✓	✓	✓
Unidades extraíbles (incluidas las unidades flash USB)	✓	✓	✓	✓	✓
Disquetes	✓	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓	✓
Dispositivos portátiles (MTP)	✓	✓	✓	✓	✓
Impresoras locales	✓	–	✓	✓	–
Impresoras de red	✓	–	✓	✓	–
Módems	✓	–	–	–	–
Unidades de cinta	✓	–	–	–	–
Dispositivos multifuncionales	✓	–	–	–	–
Lectores de tarjetas inteligentes	✓	–	–	–	–
Dispositivos Windows CE USB ActiveSync	✓	–	–	–	–
Adaptadores de red externos	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Cámaras y escáneres	✓	–	–	–	–

Reglas de acceso para redes wifi

Una regla del acceso de red wifi determina si el uso de redes wifi se permite (estado ✓) o se prohíbe (estado ⊘). Puede añadir una *red wifi de confianza* (estado ⊡) a una regla. El uso de una red wifi de confianza se permite sin limitaciones. De forma predeterminada, una regla del acceso a red wifi permite acceder a cualquier red wifi.

Reglas de acceso a los buses de conexión

Si se selecciona el valor **Depende del bus de conexión** para la regla de acceso por tipo de dispositivo, la aplicación permite o deniega el acceso al dispositivo según la interfaz de conexión. Las reglas que permiten el acceso a los buses se crean de forma predeterminada para todos los buses de conexión presentes en la clasificación del componente Control de dispositivos.

Las reglas del acceso de bus de conexión determinan si la conexión de dispositivos se permite (estado ✓) o se prohíbe (estado ⊘). La prioridad de las reglas de acceso del tipo de dispositivo es mayor que la prioridad de las reglas de acceso al bus de conexión.

El teclado y el ratón no se pueden bloquear mediante el Control de dispositivos. Si prohíbe el acceso al bus de conexión USB, el usuario seguirá trabajando con un teclado y un ratón conectados por USB. El componente Prevención de ataques BadUSB está diseñado para impedir que dispositivos USB infectados que imitan teclados se conecten al equipo.

Obtención de información sobre los dispositivos instalados

Kaspersky Security Center recibe información sobre los dispositivos instalados de los siguientes proveedores: el Agente de red y Kaspersky Endpoint Security. La información sobre los dispositivos instalados es necesaria para administrar el acceso y crear una lista de dispositivos de confianza.

Información sobre el hardware del equipo

Si el Agente de red está instalado en un dispositivo Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:

- RAM
- dispositivos de almacenamiento (incluidos los discos duros)
- placa base
- CPU
- adaptador de red
- monitores
- GPU
- tarjeta de sonido

El Agente de red proporciona esta información cada vez que se sincroniza con Kaspersky Security Center. Puede consultar el hardware de un equipo en las propiedades de este (**Registro de hardware**).

Información sobre el hardware

Kaspersky Endpoint Security proporciona información sobre el hardware instalado: impresoras, unidades extraíbles, dispositivos portátiles (MTP), etc. Para recibir información sobre el hardware, debe aplicar una directiva activa que permita transmitir información sobre los dispositivos instalados (esta transmisión está habilitada de forma predeterminada).

Cómo habilitar la transmisión de datos sobre los dispositivos instalados en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general → Informes y Almacenamiento**.
5. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.
6. Seleccione la casilla **Dispositivos instalados**.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo habilitar la transmisión de datos sobre los dispositivos instalados en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Integración con KSC**.
5. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración avanzada**.
6. Seleccione la casilla **Acerca de dispositivos instalados**.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Como resultado, puede consultar la lista de dispositivos instalados en la consola de Kaspersky Security Center (**Repositorios → Hardware**).

Administrar el acceso a dispositivos por tipo

Control de dispositivos permite administrar el acceso a los dispositivos por tipo. El tipo de dispositivo lo determina el sistema operativo cuando el dispositivo está conectado. Puede buscar el tipo de dispositivo con la herramienta Administrador de dispositivos integrada en el sistema operativo. Para administrar el acceso a los dispositivos, debe configurar reglas. Una *regla de acceso al dispositivo* es un grupo de ajustes de configuración que determina cómo los usuarios pueden acceder a dispositivos instalados en un equipo o conectados a él. Esta configuración incluye acceso a un dispositivo específico, un horario de acceso y permisos de lectura o escritura. No puede añadir un dispositivo que no pertenezca a la clasificación de Control de dispositivos. El acceso a tales dispositivos está permitido para todos los usuarios.

De forma predeterminada, Control de dispositivos permite el acceso a todos los dispositivos para todos los usuarios.

Puede configurar el acceso a los dispositivos de la siguiente manera:

- **Permitir**.

  Kaspersky Endpoint Security otorga a todos los usuarios acceso total a los dispositivos.

- **Bloquear**.

  Kaspersky Endpoint Security bloquea las conexiones de dispositivos. La aplicación permite únicamente la conexión de dispositivos de confianza.

- **Depende del bus de conexión**.

  Kaspersky Endpoint Security determina la interfaz de conexión de los dispositivos y restringe el acceso a los dispositivos de acuerdo con su estado de conexión de bus. La aplicación también permite conectar dispositivos de confianza.

- **Por las reglas**.

  Para algunos tipos de dispositivos, puede designar usuarios individuales o un grupo de usuarios que pueden usar dispositivos, establecer una programación para el acceso a los dispositivos y configurar permisos de lectura y escritura. La aplicación también permite conectar dispositivos de confianza.

Tenga cuidado al configurar el acceso a dispositivos del tipo **Discos duros**. Si bloquea el acceso al disco del sistema, la aplicación puede provocar un fallo (BSOD) al iniciar el sistema operativo.

Si un dispositivo no encaja en el esquema de clasificación de Control de dispositivos, el acceso a dicho dispositivo no se puede restringir.

Cómo administrar el acceso a dispositivos por tipo en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.

5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   La pestaña **Tipos de dispositivos** muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de Control de dispositivos.

6. Configure las reglas de acceso para los dispositivos:

   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión**, **Por las reglas**.

      Para seleccionar el modo de acceso **Por las reglas**, debe hacer doble clic para abrir las propiedades de la regla de acceso.

   b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

   c. En el caso de los dispositivos de almacenamiento (por ejemplo, medios extraíbles), puede configurar los permisos de acceso para usuarios individuales. También puede configurar una programación para el acceso a los dispositivos y configurar los permisos de lectura y escritura.

      Puede añadir dispositivos a la lista de confianza. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

   d. Si es necesario, configure las reglas de impresión.

   e. Si es necesario, configure las reglas de acceso a dispositivos Bluetooth.

   f. Si es necesario, configure las reglas de conexión Wi-Fi del equipo.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo administrar el acceso a dispositivos por tipo en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En **Reglas de acceso a dispositivos**, seleccione la pestaña **Dispositivos y redes wifi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.

6. Configure las reglas de acceso para los dispositivos:

   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Dependiente del bus**, **Personalizado**.

      Si el modo de acceso no aparece en el menú desplegable, abra las propiedades de la regla de acceso haciendo doble clic en el tipo de dispositivo.

   b. Si selecciona el modo de acceso **Dependiente del bus**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

c. En el caso de los dispositivos de almacenamiento (por ejemplo, medios extraíbles), puede configurar los permisos de acceso para usuarios individuales. También puede configurar una programación para el acceso a los dispositivos y configurar los permisos de lectura y escritura.

Puede añadir dispositivos a la lista de confianza. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

d. Si es necesario, configure las reglas de impresión.

e. Si es necesario, configure las reglas de acceso a dispositivos Bluetooth.

f. Si es necesario, configure las reglas de conexión Wi-Fi del equipo.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo administrar el acceso a los dispositivos en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el enlace **Dispositivos y redes wifi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
4. Configure las reglas de acceso para los dispositivos:

   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión**, **Por las reglas**.

   Si el modo de acceso no aparece en el menú desplegable, abra las propiedades de la regla de acceso haciendo doble clic en el tipo de dispositivo.

   b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

   c. En el caso de los dispositivos de almacenamiento (por ejemplo, medios extraíbles), puede configurar los permisos de acceso para usuarios individuales. También puede configurar una programación para el acceso a los dispositivos y configurar los permisos de lectura y escritura.

   Puede añadir dispositivos a la lista de confianza. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

   d. Si es necesario, configure las reglas de impresión.

   e. Si es necesario, configure las reglas de acceso a dispositivos Bluetooth.

   f. Si es necesario, configure las reglas de conexión Wi-Fi del equipo.

5. Guarde los cambios.

Como resultado, cuando un usuario intenta obtener acceso a un dispositivo, la aplicación bloquea el acceso de acuerdo con las reglas. Kaspersky Endpoint Security también registra un evento correspondiente. Si desea otorgar acceso a dispositivos individuales, puede añadir estos dispositivos a la lista de dispositivos de confianza.

Gestionar el acceso a dispositivos por bus de conexión

Para editar una regla de acceso a bus de conexión:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Buses de conexión**.

   La ventana abierta muestra las reglas de acceso para todos los buses de conexión que se incluyen en la clasificación del componente Control de dispositivos.
4. Seleccione la regla de acceso que quiera editar.
5. En la columna **Acceso**, elija si desea permitir el acceso al bus de conexión: **Permitir** o **Bloquear**.

   Si ha cambiado el acceso al bus de conexión **Puerto serie** (COM) o **Puerto paralelo** (LPT), debe reiniciar el equipo para activar la regla de acceso.
6. Guarde los cambios.

Diferenciación de los derechos de acceso de los usuarios a los dispositivos

Puede configurar los derechos de acceso de los usuarios por tipo de dispositivo o para dispositivos de confianza.

Diferenciación de los derechos de acceso de los usuarios por tipo de dispositivo

Control de dispositivos permite configurar los derechos de acceso del usuario a los datos en *dispositivos de almacenamiento*. Para tales dispositivos, puede configurar permisos de escritura y lectura. Control de dispositivos admite los siguientes tipos de *dispositivos de almacenamiento*:

- Discos duros
- Unidades extraíbles (incluidas las unidades flash USB)
- Disquetes
- Unidades de CD/DVD
- Dispositivos portátiles (MTP) Los dispositivos portátiles (MTP) incluyen, por ejemplo, dispositivos móviles, cámaras de fotos, reproductores de medios, etc.

De esta forma se puede, por ejemplo, permitir el uso de medios extraíbles solo al grupo de administradores. Para otros tipos de dispositivos, puede denegar o permitir el acceso a todos los usuarios. También puede configurar los derechos de acceso de los usuarios para utilizar las impresoras.

Cómo configurar los derechos de acceso de los usuarios a los datos en los dispositivos de almacenamiento en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.
5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   La pestaña **Tipos de dispositivos** muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de Control de dispositivos.
6. Para configurar reglas de acceso a dispositivos de almacenamiento, haga doble clic para abrir la lista de reglas.
7. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Reglas de acceso**, haga clic en el botón **Añadir**.

   Esto abre una ventana para agregar una nueva regla de acceso al dispositivo de almacenamiento.

   b. En el campo **Prioridad de regla**, configure la prioridad de *escritura de la regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

   Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

   Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

   La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

   c. En **Regla para usuarios y grupos**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   d. Haga clic en **Aceptar**.
8. En **Programación para la regla de acceso seleccionada**, configure una planificación del acceso a dispositivos de almacenamiento para usuarios.

   Por ejemplo, puede permitir que los usuarios utilicen dispositivos de almacenamiento solo durante el horario de trabajo.

9. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Leer** / **Escribir**).

10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar los derechos de acceso de los usuarios a los datos en los dispositivos de almacenamiento en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En la tabla de reglas de acceso del bloque **Reglas de acceso a dispositivos**, abra las propiedades de las reglas de acceso para dispositivos de almacenamiento.

6. En el bloque **Reglas de acceso a dispositivos**, seleccione **Personalizado**.

7. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Usuarios y sus derechos**, haga clic en el botón **Añadir**.

      Esto abre una ventana para agregar una nueva regla de acceso al dispositivo de almacenamiento.

   b. En el campo **Prioridad**, configure la prioridad de *escritura de la regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

      Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

      Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

      La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

   c. En **Usuario o grupo**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   d. En **Planificación del acceso**, configure una planificación del acceso a dispositivos de almacenamiento para usuarios.

      Por ejemplo, puede permitir que los usuarios utilicen dispositivos de almacenamiento solo durante el horario de trabajo.

e. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Lectura** / **Escritura**).

f. Haga clic en **Guardar**.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar los derechos de acceso de los usuarios a los datos en los dispositivos de almacenamiento en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el enlace **Dispositivos y redes wifi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
4. Para configurar reglas de acceso a dispositivos de almacenamiento, haga clic con el botón derecho para abrir la lista de reglas.
5. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Derechos de los usuarios**, haga clic en el botón **Añadir**.

   Esto abre una ventana para agregar una nueva regla de acceso al dispositivo de almacenamiento.

   b. En el campo **Prioridad**, configure la prioridad de *escritura de la regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

   Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

   Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

   La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

   c. En **Usuarios**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory o introducir un nombre de usuario local manualmente. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   d. Haga clic en **Aceptar**.

6. En **Planificar acceso a los dispositivos**, configure una planificación del acceso a dispositivos de almacenamiento para usuarios.

   Por ejemplo, puede permitir que los usuarios utilicen dispositivos de almacenamiento solo durante el horario de trabajo.
7. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Leer** / **Escribir**).
8. Guarde los cambios.

Diferenciación de los derechos de acceso de los usuarios a los dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento. Para trabajar con dispositivos de confianza, puede otorgar acceso a un usuario individual, a un grupo de usuarios o a todos los usuarios de la organización. Puede configurar derechos de acceso de los usuarios usuario en las propiedades del dispositivo de confianza.

Administrar el acceso a dispositivos móviles

Kaspersky Endpoint Security le permite controlar el acceso a los datos en dispositivos móviles que ejecutan Android e iOS. Los dispositivos móviles pertenecen a la categoría de dispositivos portátiles (MTP). Por tanto, para configurar el acceso a los datos en dispositivos móviles, debe editar la configuración de acceso para dispositivos portátiles (MTP).

Cuando un dispositivo móvil se conecta a un equipo, el sistema operativo determina de qué tipo de dispositivo se trata. Si en el equipo están instalados Android Debug Bridge (ADB), iTunes o aplicaciones equivalentes, el sistema operativo identifica los dispositivos móviles como dispositivos ADB o iTunes. En los demás casos, se lo reconoce como dispositivo portátil (MTP) capaz de transferir archivos, como dispositivo PTP (o cámara) capaz de transferir imágenes o como otra clase de dispositivo. El tipo de dispositivo depende del modelo del dispositivo móvil y del modo de conexión USB seleccionado. Kaspersky Endpoint Security le permite configurar permisos de acceso individuales para datos en dispositivos móviles en aplicaciones ADB, iTunes o el administrador de archivos. En todos los demás casos, el Control de dispositivos permite el acceso a dispositivos móviles de acuerdo con las reglas de acceso de dispositivos portátiles (MTP).

Acceso a dispositivos móviles

Los dispositivos móviles pertenecen a la categoría de dispositivos portátiles (MTP); por tanto, la configuración para ellos es la misma. Puede seleccionar uno de los siguientes modos de acceso a dispositivos móviles:

- **Permitir**. Kaspersky Endpoint Security permite el acceso total a los dispositivos móviles. Puede abrir, crear, modificar, copiar o eliminar archivos en dispositivos móviles utilizando el administrador de archivos o las aplicaciones ADB e iTunes. También puede cargar la batería del dispositivo conectando el dispositivo móvil a un puerto USB del equipo.

- **Bloquear**. Kaspersky Endpoint Security restringe el acceso a dispositivos móviles en el administrador de archivos y las aplicaciones ADB e iTunes. La aplicación permite el acceso únicamente a dispositivos móviles de confianza. También puede cargar la batería del dispositivo conectando el dispositivo móvil a un puerto USB del equipo.

- **Depende del bus de conexión**. Kaspersky Endpoint Security permite conectarse a dispositivos móviles de acuerdo con el estado de la conexión USB (**Permitir** o **Bloquear**).

- **Por las reglas**. Kaspersky Endpoint Security restringe el acceso a dispositivos móviles de acuerdo con las reglas. En las reglas, puede configurar derechos de acceso (lectura/escritura), seleccionar usuarios o un grupo de usuarios que pueden tener acceso a dispositivos móviles y configurar una planificación del acceso para dispositivos móviles. También puede restringir el acceso a los dispositivos mediante las aplicaciones ADB e iTunes.

Configuración de las reglas de acceso a dispositivos móviles

Las reglas de acceso para dispositivos portátiles (MTP), dispositivos ADB y dispositivos iTunes se configuran de manera diferente. Para dispositivos portátiles (MTP) y dispositivos ADB, puede configurar reglas para usuarios individuales o grupos de usuarios y crear una planificación para el momento en que se deban aplicar las reglas. Esto no se puede hacer con dispositivos iTunes. Solo puede permitir o denegar el acceso a los datos a través de la aplicación iTunes para todos los usuarios.

Cómo configurar reglas de acceso a dispositivos móviles en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.
4. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
5. En el menú contextual del tipo de dispositivo **Dispositivos portátiles (MTP)**, configure el modo de acceso del dispositivo móvil: **Permitir**, **Bloquear** o **Depende del bus de conexión**.
6. Para configurar reglas de acceso a dispositivos móviles, haga doble clic para abrir la lista de reglas.
7. Configure la regla de acceso a dispositivos móviles:

   a. En el bloque **Reglas de acceso**, haga clic en el botón **Añadir**.

      Esto abre una ventana para agregar una nueva regla de acceso al dispositivo móvil.

   b. En el campo **Prioridad**, configure la prioridad de escritura de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (acceso de lectura/escritura/ADB) y prioridad.

      Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

      Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

      La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

   c. En **Regla para usuarios y grupos**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   d. Haga clic en **Aceptar**.

8. En **Programación para la regla de acceso seleccionada**, configure una planificación del acceso a dispositivos móviles para usuarios.

   No es posible configurar una planificación del acceso independiente para dispositivos ADB. Puede configurar una planificación del acceso común para dispositivos ADB y dispositivos portátiles (MTP).

9. Configure los permisos de acceso de los usuarios a los dispositivos móviles en el administrador de archivos (**Leer** / **Escribir**).

10. Configure el acceso a los datos en un dispositivo móvil a través de la aplicación ADB usando la casilla de verificación **Acceder mediante ADB**.

    Si la casilla de verificación está desactivada, cuando el dispositivo móvil se conecte, la aplicación ADB no puede detectar el dispositivo.

11. En **Acceder mediante iTunes**, configure el acceso a los datos en el dispositivo móvil a través de la aplicación iTunes.

    Kaspersky Endpoint Security aplica la configuración para el acceso de dispositivos móviles a través de la aplicación iTunes para todos los usuarios. No es posible configurar una planificación del acceso independiente para dispositivos iTunes.

12. Guarde los cambios.

Cómo configurar reglas de acceso a dispositivos móviles en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En el bloque **Reglas de acceso a dispositivos**, haga clic en el enlace **Dispositivos y redes wifi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.

6. Seleccione el tipo de dispositivo **Dispositivos portátiles (MTP)**.

   Esto abre los derechos de acceso de dispositivos portátiles (MTP).

7. Configure el modo de acceso a dispositivos móviles: **Permitir**, **Bloquear**, **Dependiente del bus** o **Personalizado**.

8. Use el interruptor **Acceder mediante iTunes para todos los usuarios ACTIVADO** para configurar el acceso a los datos en el dispositivo móvil a través de la aplicación iTunes.

   Kaspersky Endpoint Security aplica la configuración para el acceso de dispositivos móviles a través de la aplicación iTunes para todos los usuarios. No es posible configurar una planificación del acceso independiente para dispositivos iTunes.

9. Si selecciona el modo **Personalizado**, debe agregar reglas de acceso para dispositivos. Para ello, en **Usuarios y sus derechos**, haga clic en el botón **Añadir** y configure la regla de acceso a dispositivos móviles:

   a. En el campo **Prioridad**, configure la prioridad de escritura de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (acceso de lectura/escritura/ADB) y prioridad.

   Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

   Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

   La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

   b. En **Usuario o grupo**, seleccione usuarios o grupos de usuarios para acceder a dispositivos móviles. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   c. En **Planificación del acceso**, configure una planificación del acceso a dispositivos móviles para usuarios.

   > No es posible configurar una planificación del acceso independiente para dispositivos ADB. Puede configurar una planificación del acceso común para dispositivos ADB y dispositivos portátiles (MTP).

   d. Configure los permisos de acceso de los usuarios a los dispositivos móviles en el administrador de archivos (**Lectura** / **Escritura**).

   e. Configure el acceso a los datos en un dispositivo móvil a través de la aplicación ADB usando la casilla de verificación **Acceder mediante ADB**.

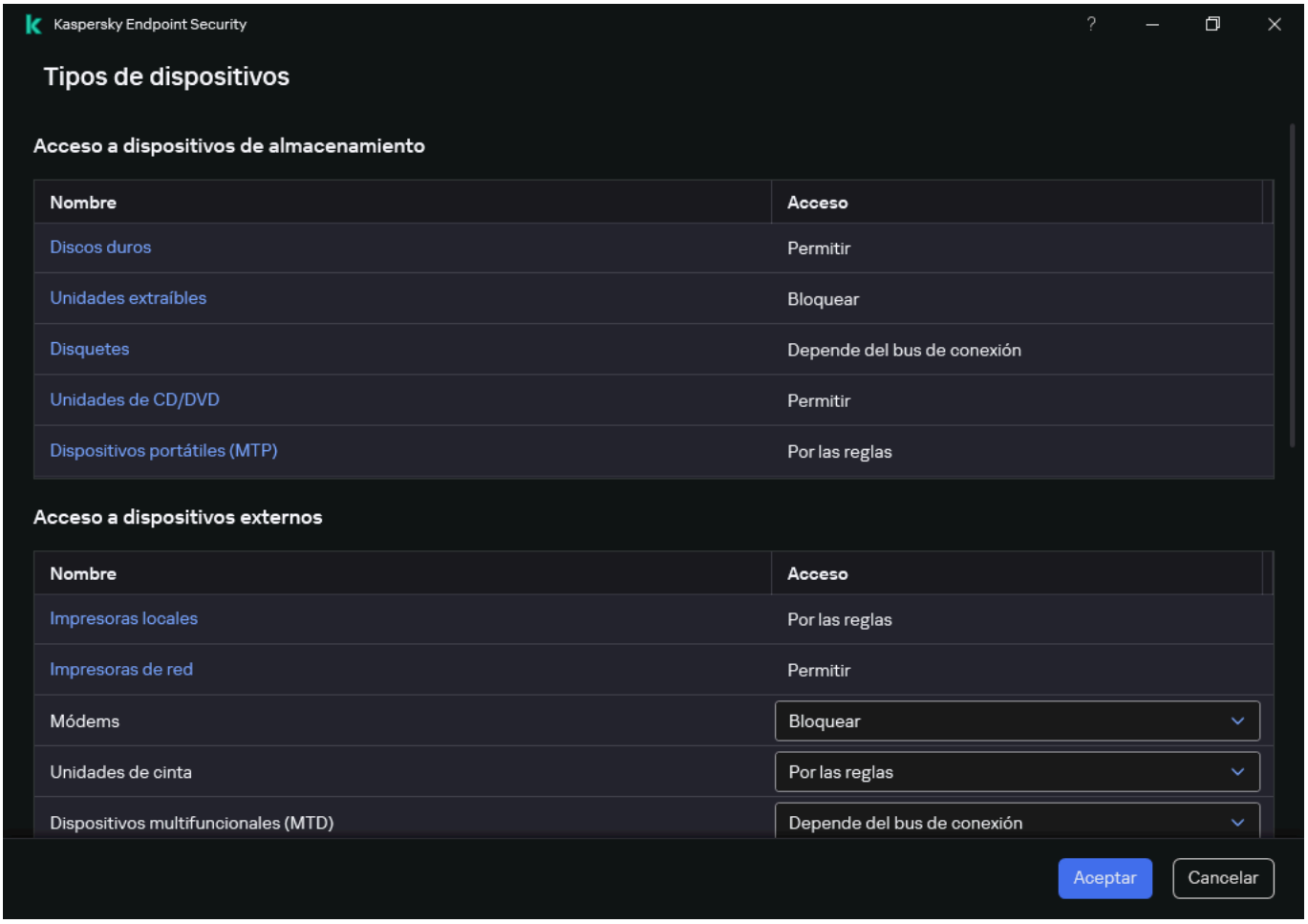
   Si la casilla de verificación está desactivada, cuando el dispositivo móvil se conecte, la aplicación ADB no puede detectar el dispositivo.

10. Guarde los cambios.

Cómo configurar reglas de acceso a dispositivos móviles en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.



Tipos de dispositivos en el componente Control de dispositivos

4. En el bloque **Acceso a dispositivos de almacenamiento**, haga clic en el enlace **Dispositivos portátiles (MTP)**.

   Se abre una ventana que contiene las reglas de acceso de dispositivos portátiles (MTP).

5. En **Acceso**, configure el modo de acceso a dispositivos móviles: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por las reglas**.

6. Si selecciona el modo **Por las reglas**, debe agregar reglas de acceso para dispositivos:

   a. En el bloque **Derechos de los usuarios**, haga clic en el botón **Añadir**.

      Esto abre una ventana para agregar una nueva regla de acceso al dispositivo móvil.

   b. En el campo **Prioridad**, configure la prioridad de escritura de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (acceso de lectura/escritura/ADB) y prioridad.

      Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

      Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

      La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

c. En **Condición**, active la regla de acceso al dispositivo móvil.

d. En **Reglas de acceso**, configure los permisos de acceso a dispositivos móviles para usuarios.

- Configure los permisos de acceso de los usuarios a los dispositivos móviles en el administrador de archivos (**Leer** / **Escribir**).
- Configure el acceso a los datos en un dispositivo móvil a través de la aplicación ADB usando la casilla de verificación **Acceder mediante ADB**.

  Si la casilla de verificación está desactivada, cuando el dispositivo móvil se conecte, la aplicación ADB no puede detectar el dispositivo.

e. En **Usuarios**, seleccione usuarios o grupos de usuarios para acceder a dispositivos móviles. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

f. En **Planificar acceso a los dispositivos**, configure una planificación del acceso a dispositivos para usuarios.

> No es posible configurar una planificación del acceso independiente para dispositivos ADB. Puede configurar una planificación del acceso común para dispositivos ADB y dispositivos portátiles (MTP).

g. En **Acceder mediante iTunes**, configure el acceso a los datos en el dispositivo móvil a través de la aplicación iTunes.

> Kaspersky Endpoint Security aplica la configuración para el acceso de dispositivos móviles a través de la aplicación iTunes para todos los usuarios. No es posible configurar una planificación del acceso independiente para dispositivos iTunes.

7. Guarde los cambios.

Como resultado, el acceso de los usuarios a los dispositivos móviles ser restringe de acuerdo con las reglas. Si ha prohibido el acceso a dispositivos móviles en las aplicaciones ADB e iTunes, cuando conecte un dispositivo móvil, las aplicaciones ADB e iTunes no podrán detectar el dispositivo móvil.

Dispositivos móviles de confianza

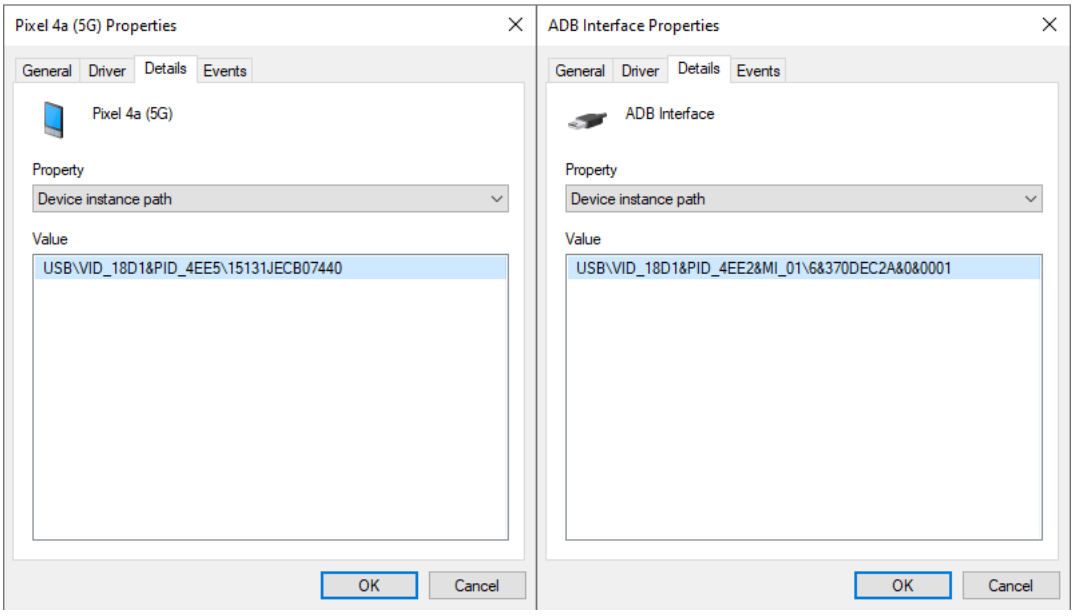
Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

El procedimiento para añadir un dispositivo móvil de confianza es exactamente igual que para otros tipos de dispositivos de confianza. Puede agregar un dispositivo móvil por ID o modelo de dispositivo.

Para añadir un dispositivo móvil de confianza por ID, necesitará un ID único (Hardware ID – HWID). Puede encontrar el ID en las propiedades del dispositivo utilizando las herramientas del sistema operativo (consulte la figura a continuación). La herramienta Administrador de dispositivos le permite hacer esto. Los ID de los dispositivos portátiles (MTP) y los dispositivos ADB e iTunes son diferentes incluso para el mismo dispositivo móvil. El ID de un dispositivo portátil (MTP) puede ser parecido a este: `15131JECB07440`. El ID de un dispositivo ADB puede ser parecido a este: `6&370DEC2A&0&0001`. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos. También puedes usar mascarillas.

Si ha instalado las aplicaciones ADB o iTunes después de conectar un dispositivo al equipo, el ID único del dispositivo se podría restablecer. Esto significa que Kaspersky Endpoint Security detectará este dispositivo como dispositivo nuevo. Si un dispositivo es de confianza, vuelva a añadir el dispositivo a la lista de confianza.

Para añadir un dispositivo móvil de confianza por modelo de dispositivo, necesitará su Vendor ID (VID) and Product ID (PID). Puede encontrar los ID en las propiedades del dispositivo utilizando las herramientas del sistema operativo (consulte la figura a continuación). Plantilla para introducir el VID y el PID: `VID_18D1&PID_4EE5`. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.



ID de dispositivo en el Administrador de dispositivos

Administrar el acceso a dispositivos con Bluetooth

Kaspersky Endpoint Security permite administrar el acceso a dispositivos con Bluetooth. Los dispositivos con Bluetooth incluyen teclados, ratones, auriculares, impresoras, etc. inalámbricos. También puede utilizar Bluetooth para comunicarse, por ejemplo, con un dispositivo móvil.

Cuando se conectan o desconectan dispositivos Bluetooth, la aplicación puede crear múltiples eventos sobre el dispositivo. La razón es que el sistema operativo puede detectar un dispositivo Bluetooth como varios dispositivos de diferentes tipos. Kaspersky Endpoint Security también administra el adaptador Bluetooth a través del cual el dispositivo se conecta como un dispositivo independiente. Por este motivo, la aplicación crea un evento para cada uno de los dispositivos detectados.

Puede seleccionar uno de los siguientes modos de acceso a dispositivos con Bluetooth:

- **Permitir y no registrar**. Kaspersky Endpoint Security permite conectar cualquier dispositivo con Bluetooth y no guarda información sobre la conexión en el registro de eventos. Puede conectar dispositivos de entrada con Bluetooth (teclados, ratones, etc.), enviar datos a través de Bluetooth o administrar otros dispositivos con Bluetooth (auriculares, cascos, etc.).

- **Permitir**. Kaspersky Endpoint Security permite conectar cualquier dispositivo con Bluetooth. Puede conectar dispositivos de entrada con Bluetooth (teclados, ratones, etc.), enviar datos a través de Bluetooth o administrar otros dispositivos con Bluetooth (auriculares, cascos, etc.).

- **Bloquear**. Kaspersky Endpoint Security restringe el acceso a dispositivos Bluetooth. Puede permitir la conexión solo de dispositivos de entrada Bluetooth (de la clase Human Interface Devices). La lista de estos dispositivos incluye teclados, ratones, joysticks, etc.

No es posible crear una lista dispositivos con Bluetooth de confianza. Si tiene acceso restringido a dispositivos con Bluetooth, solo puede conectar dispositivos con Bluetooth de entrada.

Cómo configurar reglas de acceso a dispositivos con Bluetooth en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione **Directivas**.

3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.

5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.

6. En el menú contextual del tipo de dispositivo **Bluetooth**, configure el modo de acceso del dispositivo con Bluetooth: **Permitir**, **Bloquear** o **Permitir y no registrar**.

7. Si selecciona el modo **Bloquear**, puede permitir únicamente la conexión de dispositivos de entrada con Bluetooth (teclados, ratones, etc.). Para ello, en **Exclusiones**, seleccione la casilla **Dispositivos de entrada (ratones y teclados)**.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar reglas de acceso a dispositivos con Bluetooth en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En el bloque **Reglas de acceso a dispositivos**, haga clic en el enlace **Dispositivos y redes wifi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.

6. Seleccione el tipo de dispositivo **Dispositivos Bluetooth**.

   Esto abre la configuración de acceso al dispositivo con Bluetooth.

7. Configure el modo de acceso al dispositivo con Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**.

8. Si selecciona el modo **Bloquear**, puede permitir únicamente la conexión de dispositivos de entrada con Bluetooth (teclados, ratones, etc.). Para ello, en **Exclusiones**, seleccione la casilla **Dispositivos de entrada (ratones y teclados)**.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

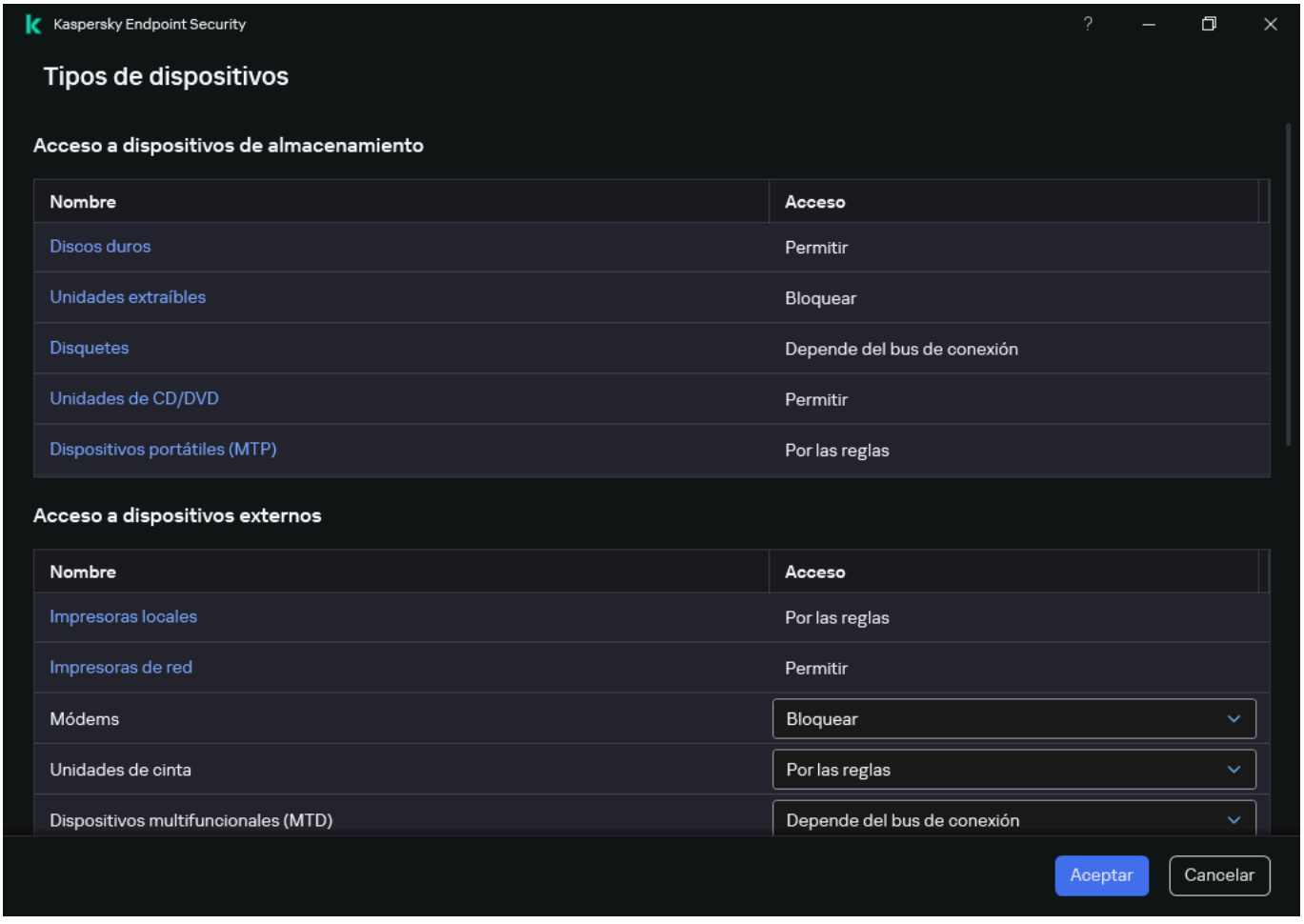
Cómo configurar reglas de acceso a dispositivos Bluetooth en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de dispositivos**.

3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

   La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.



Tipos de dispositivos en el componente Control de dispositivos

4. En el bloque **Acceso a dispositivos externos**, haga clic en el enlace **Bluetooth**.

   Esto abre la configuración de acceso al dispositivo con Bluetooth.

5. En **Acceso**, configure el modo de acceso a dispositivos con Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**

6. Si selecciona el modo **Bloquear**, puede permitir únicamente la conexión de dispositivos de entrada con Bluetooth (teclados, ratones, etc.). Para ello, en **Exclusiones**, seleccione la casilla **Dispositivos de entrada (ratones y teclados)**.

7. Guarde los cambios.

Control de impresión

Control de impresión no es compatible con equipos basados en Arm.

Puede utilizar Control de impresión para configurar el acceso de los usuarios a las impresoras locales y de red.

Control de las impresoras locales

Kaspersky Endpoint Security permite configurar el acceso a las impresoras locales en dos niveles: *conexión* e *impresión*.

Kaspersky Endpoint Security controla la conexión de impresoras locales a través de los siguientes buses: USB, Puerto serial (COM), Puerto paralelo (LPT).

Kaspersky Endpoint Security controla la conexión de impresoras locales a los puertos COM y LPT solo en el nivel del bus. Por lo tanto, para evitar conexiones de impresora a través de puertos COM y LPT, debe seleccionar el modo de acceso Depende del bus de conexión acceso para impresoras locales y prohibir conexiones a buses COM y LPT.

Para impresoras conectadas a USB, la aplicación ejerce el control en dos niveles: tipo de dispositivo (impresoras locales) y bus de conexión (USB).

Puede seleccionar uno de los siguientes modos de acceso a las impresoras locales a través de USB:

- **Permitir** ✓. Kaspersky Endpoint Security otorga acceso total a las impresoras locales a todos los usuarios. Los usuarios pueden conectar impresoras e imprimir documentos utilizando los medios que proporciona el sistema operativo.

- **Bloquear** ⊘. Kaspersky Endpoint Security bloquea la conexión de impresoras locales. La aplicación solo permite conectarse a impresoras de confianza.

- **Depende del bus de conexión**. Kaspersky Endpoint Security permite conectarse a impresoras locales de acuerdo con el estado de conexión del bus USB (**Permitir** o **Bloquear**).
- **Por las reglas**. Para controlar la impresión, debe agregar *reglas de impresión*. En las reglas, puede seleccionar usuarios o un grupo de usuarios para los que desea autorizar o bloquear el acceso a la impresión de documentos en impresoras locales.

Control de impresoras de red

Kaspersky Endpoint Security permite configurar el acceso a la impresión en impresoras de red. Puede seleccionar uno de los siguientes modos de acceso a impresoras de red:

- **Permitir y no registrar**. Kaspersky Endpoint Security no controla la impresión en impresoras de red. La aplicación otorga acceso a la impresión a todos los usuarios y no guarda información sobre la impresión en el registro de eventos.
- **Permitir**. Kaspersky Endpoint Security otorga acceso a la impresión en impresoras de red a todos los usuarios.
- **Bloquear**. Kaspersky Endpoint Security restringe el acceso a las impresoras de red para todos los usuarios. La aplicación autoriza el acceso únicamente a impresoras de confianza.
- **Por las reglas**. Kaspersky Endpoint Security otorga acceso a la impresión de acuerdo con reglas de impresión. En las reglas, puede seleccionar usuarios o un grupo de usuarios a los que se les autorizará o impedirá imprimir documentos en una impresora de red.

Agregar reglas de impresión para impresoras

Cómo añadir reglas de impresión en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.
4. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
5. En el menú contextual de los tipos de dispositivo **Impresoras locales** y **Impresoras de red**, configure el modo de acceso a las impresoras correspondientes: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), o **Depende del bus de conexión** (solo para impresoras locales).
6. Para configurar reglas de impresión en impresoras locales y de red, haga doble clic en las listas de reglas para abrirlas.
7. Seleccione **Por las reglas** como modo de acceso a la impresora.

8. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de impresión.

    a. Haga clic en **Añadir**.

    Esto abre una ventana para agregar una nueva regla impresión.

    b. Asigne una prioridad a la entrada de la regla. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (autorizar/bloquear) y prioridad.

    Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

    Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

    La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

    c. En **Acción**, configure el acceso del usuario para imprimir en la impresora.

    d. Haz clic en **Usuarios y grupos**, seleccione usuarios o grupos de usuarios para acceder a la impresión. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

    e. Haga clic en **Aceptar**.

9. Guarde los cambios.

Cómo agregar reglas de impresión en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

    Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En el bloque **Reglas de acceso a dispositivos**, haga clic en el enlace **Dispositivos y redes wifi**.

    En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.

6. Selecciona el tipo de dispositivo **Impresoras locales** o **Impresoras de red**.

    Se abren las reglas de acceso a las impresoras.

7. Configure el modo de acceso de las impresoras correspondientes: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Dependiente del bus** (solo para impresoras locales), o **Personalizado**.

8. Si selecciona el modo **Personalizado**, debe agregar reglas de impresión para impresoras locales o de red. Para ello, haga clic en el botón **Añadir** en la tabla de reglas de impresión.

    Esto abre la configuración de la nueva regla de impresión.

9. Asigne una prioridad a la entrada de la regla. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (autorizar/bloquear) y prioridad.

   Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

   Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

   La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

10. En **Acción**, configure el acceso del usuario para imprimir en la impresora.

11. En **Usuario o grupo**, seleccione usuarios o grupos de usuarios para acceder a la impresión. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

12. Guarde los cambios.

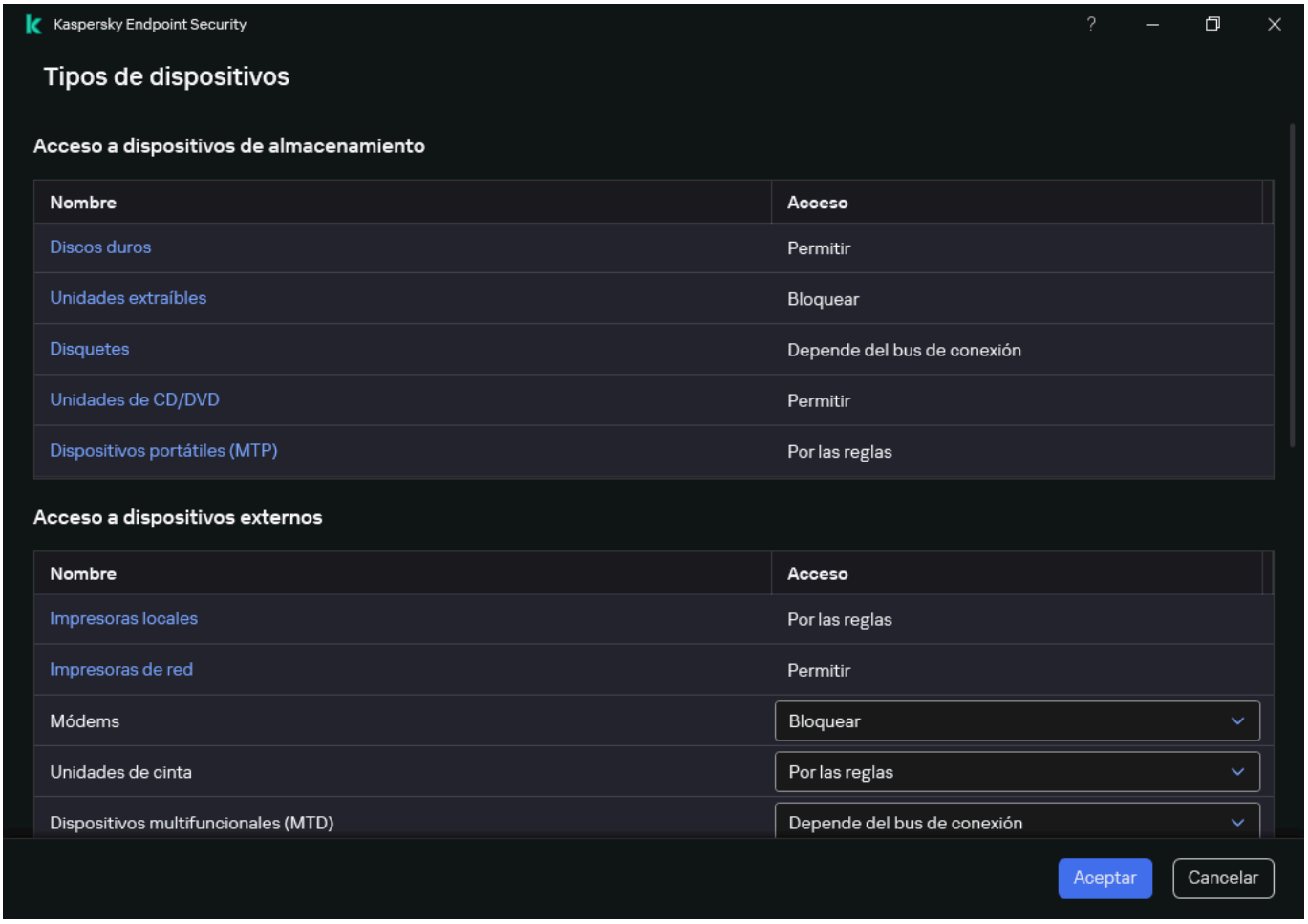
Cómo añadir reglas de impresión en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.



Tipos de dispositivos en el componente Control de dispositivos

4. En **Acceso a dispositivos externos**, haga clic en **Impresoras locales** o en **Impresoras de red**.

   Esto abre una ventana con reglas de acceso a las impresoras.

5. En **Acceso a impresoras locales** o **Acceso a impresoras en red**, configure el modo de acceso para impresoras: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Depende del bus de conexión** (solo para impresoras locales) o **Por las reglas**.

6. Si selecciona el modo **Por las reglas**, debe agregar reglas de impresión para las impresoras. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de impresión.

   a. Haga clic en **Añadir**.

      Esto abre una ventana para agregar una nueva regla impresión.

   b. Asigne una prioridad a la entrada de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, permisos (permitir/bloquear) y prioridad.

      Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.

      Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

c. En **Acción**, configure los permisos de usuario para acceder a la impresión.

d. En **Usuarios y grupos**, seleccione usuarios o grupos de usuarios para acceder a la impresión. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

7. Guarde los cambios.

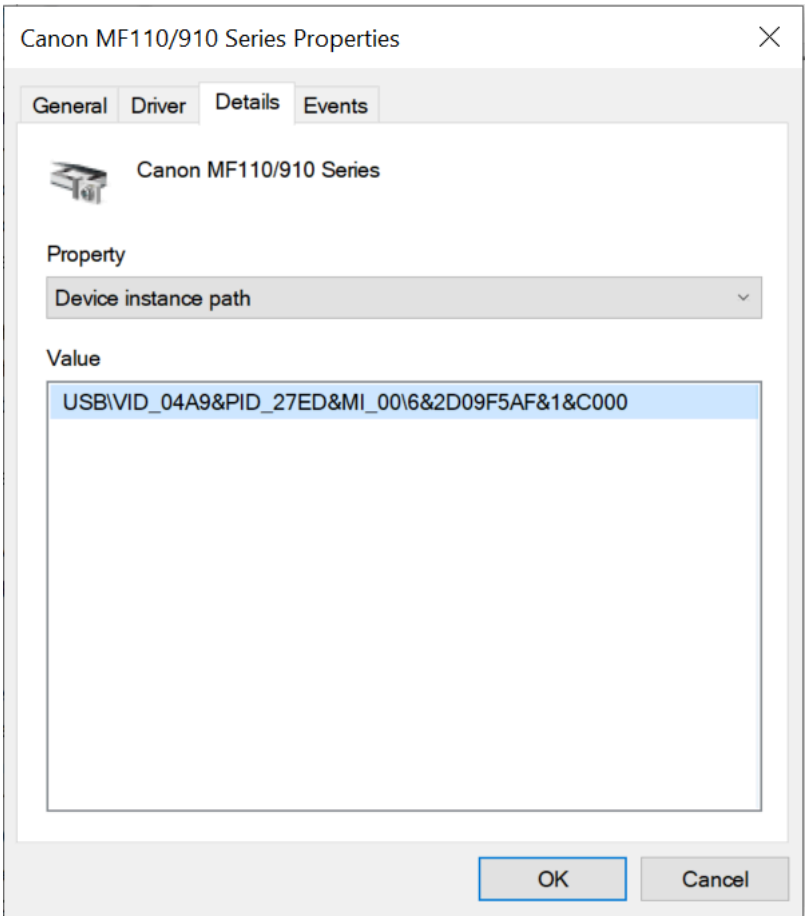
Impresoras de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

El procedimiento para añadir impresoras de confianza es exactamente igual que para otros tipos de dispositivos de confianza. Puede agregar impresoras locales por ID o modelo de dispositivo. Solo puede agregar impresoras de red por ID de dispositivo.

Para añadir una impresora local de confianza por ID, necesitará una ID única (Hardware ID – HWID). Puede encontrar el ID en las propiedades del dispositivo utilizando las herramientas del sistema operativo (consulte la figura a continuación). La herramienta Device Manager le permite realizar esta acción. El ID de una impresora local puede ser similar a este: `6&2D09F5AF&1&C000`. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos. También puedes usar mascarillas.

Para añadir una impresora local de confianza por modelo de dispositivo, necesitará su Vendor ID (VID) y Product ID (PID). Puede encontrar los ID en las propiedades del dispositivo utilizando las herramientas del sistema operativo (consulte la figura a continuación). Plantilla para introducir el VID y el PID: `VID_04A9&PID_27FD`. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.



ID de dispositivo en el Administrador de dispositivos

Para agregar una impresora de red de confianza, necesitará su ID de dispositivo. Para impresoras de red, el ID del dispositivo puede ser el nombre de red de la impresora (nombre de la impresora compartida), la dirección IP de la impresora o la URL de la impresora.

Control de conexiones wifi

Control de dispositivos permite administrar la conexión wifi del equipo (portátil). Las redes wifi públicas pueden no ser seguras, y el uso de dichas redes puede provocar la pérdida de datos. Control de dispositivos le permite bloquear a un usuario para que no se conecte a redes wifi, o permitir que se conecte solo a redes de confianza. Por ejemplo, puede autorizar únicamente la conexión a la red wifi corporativa sea lo suficientemente segura. Control de dispositivos bloqueará el acceso a todas las redes wifi excepto las especificadas en la lista de confianza.

En equipos que ejecutan Windows 11, debe activar los servicios de ubicación para controlar las conexiones Wi-Fi. Para hacer esto, debe habilitar el interruptor **Servicios de ubicación** en la configuración del sistema operativo (**Configuración** → **Privacidad & seguridad** → **Ubicación**). Si los servicios de ubicación están desactivados, Kaspersky Endpoint Security no controla las conexiones a las redes Wi-Fi.

Cómo restringir las conexiones wifi en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.
4. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
5. En el menú contextual del tipo de dispositivo **wifi**, seleccione la acción de Control de dispositivos que se realiza al conectarse a wifi: **Permitir** (), **Bloquear** () o **Bloquear con excepciones** ().
6. Si seleccionó la opción **Bloquear con excepciones**, cree una lista de redes wifi de confianza:

   a. Haga doble clic para abrir la lista de redes wifi de confianza.

   b. En el bloque **Redes wifi de confianza**, haga clic en el botón **Añadir**.

   c. Esto abre una ventana; en ella, configure la red wifi de confianza (vea la figura a continuación):

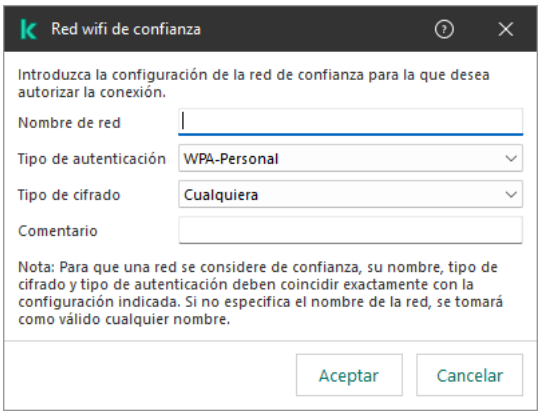
   - **Nombre de red**. Nombre o SSID (Service Set Identifier) de la red wifi.
   - **Tipo de autenticación**. Tipo de autenticación utilizado al conectarse a la red wifi.

     A partir de la versión 12.0 de Kaspersky Endpoint Security para Windows, se ha agregado la compatibilidad con el protocolo WPA3 a la aplicación. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en un equipo, el protocolo WPA2 se selecciona en equipos con Kaspersky Endpoint Security versión 11.11.0 y anteriores; WPA2/WPA3 se selecciona con las versiones 12.0 a 12.1; WPA3 se selecciona con las versiones 12.2 y posteriores.
   - **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico wifi.
   - **Comentario**. Más información sobre la red wifi añadida.

   Puede ver la configuración de la red wifi de confianza en la configuración del enrutador.

   Una red wifi se considera de confianza si sus ajustes coinciden con todos los que se especifican en la regla.

7. Guarde los cambios.



Configuración de la red wifi de confianza

Cómo restringir las conexiones wifi en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control de dispositivos**.
5. En **Reglas de acceso a dispositivos**, seleccione la pestaña **Dispositivos y redes wifi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
6. En el bloque **Redes wifi**, haga clic en el enlace **Wifi**.
7. En la ventana que se abre, seleccione qué acción de Control de dispositivos se realiza al conectarse a la red wifi: **Permitir**, **Bloquear** o **Bloquear con exclusiones**.
8. Si seleccionó la opción **Bloquear con exclusiones**, cree una lista de redes wifi de confianza:

   a. Haga doble clic para abrir la lista de redes wifi de confianza.

   b. En el bloque **Redes wifi de confianza**, haga clic en el botón **Añadir**.

   c. Esto abre una ventana; en ella, configure la red wifi de confianza (vea la figura a continuación):

   - **Nombre**. Nombre o SSID (Service Set Identifier) de la red wifi.
   - **Tipo de autenticación**. Tipo de autenticación utilizado al conectarse a la red wifi.

     A partir de la versión 12.0 de Kaspersky Endpoint Security para Windows, se ha agregado la compatibilidad con el protocolo WPA3 a la aplicación. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en un equipo, el protocolo WPA2 se selecciona en equipos con Kaspersky Endpoint Security versión 11.11.0 y anteriores; WPA2/WPA3 se selecciona con las versiones 12.0 a 12.1; WPA3 se selecciona con las versiones 12.2 y posteriores.

- **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico wifi.
- **Comentario**. Más información sobre la red wifi añadida.

Puede ver la configuración de la red wifi de confianza en la configuración del enrutador.

> Una red wifi se considera de confianza si sus ajustes coinciden con todos los que se especifican en la regla.

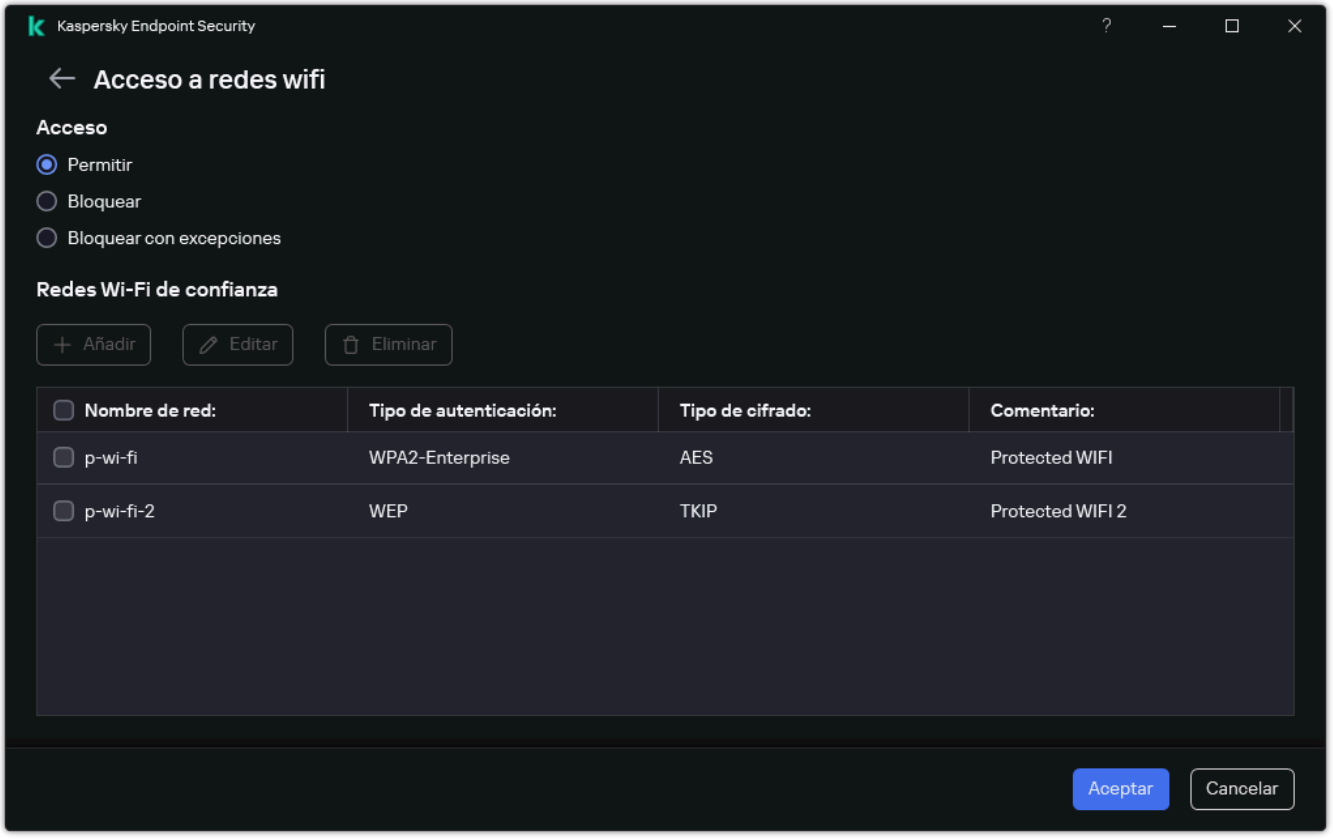
9. Guarde los cambios.

Cómo restringir las conexiones wifi en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

   La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
4. En el bloque **Acceso a redes wifi**, haga clic en el enlace **Wifi**.

   La ventana abierta muestra las reglas de acceso a la red wifi.



Configuración de acceso wifi

5. En **Acceso**, seleccione la acción de Control de dispositivos realizada al conectarse a la red wifi: **Permitir**, **Bloquear** o **Bloquear con excepciones**.

6. Si seleccionó la opción **Bloquear con excepciones**, cree una lista de redes wifi de confianza:

   a. En el bloque **Redes Wi-Fi de confianza**, haga clic en el botón **Añadir**.

   b. Esto abre una ventana; en ella, configure la red wifi de confianza (vea la figura a continuación):

   - **Nombre de red**. Nombre o SSID (Service Set Identifier) de la red wifi.
   - **Tipo de autenticación**. Tipo de autenticación utilizado al conectarse a la red wifi.

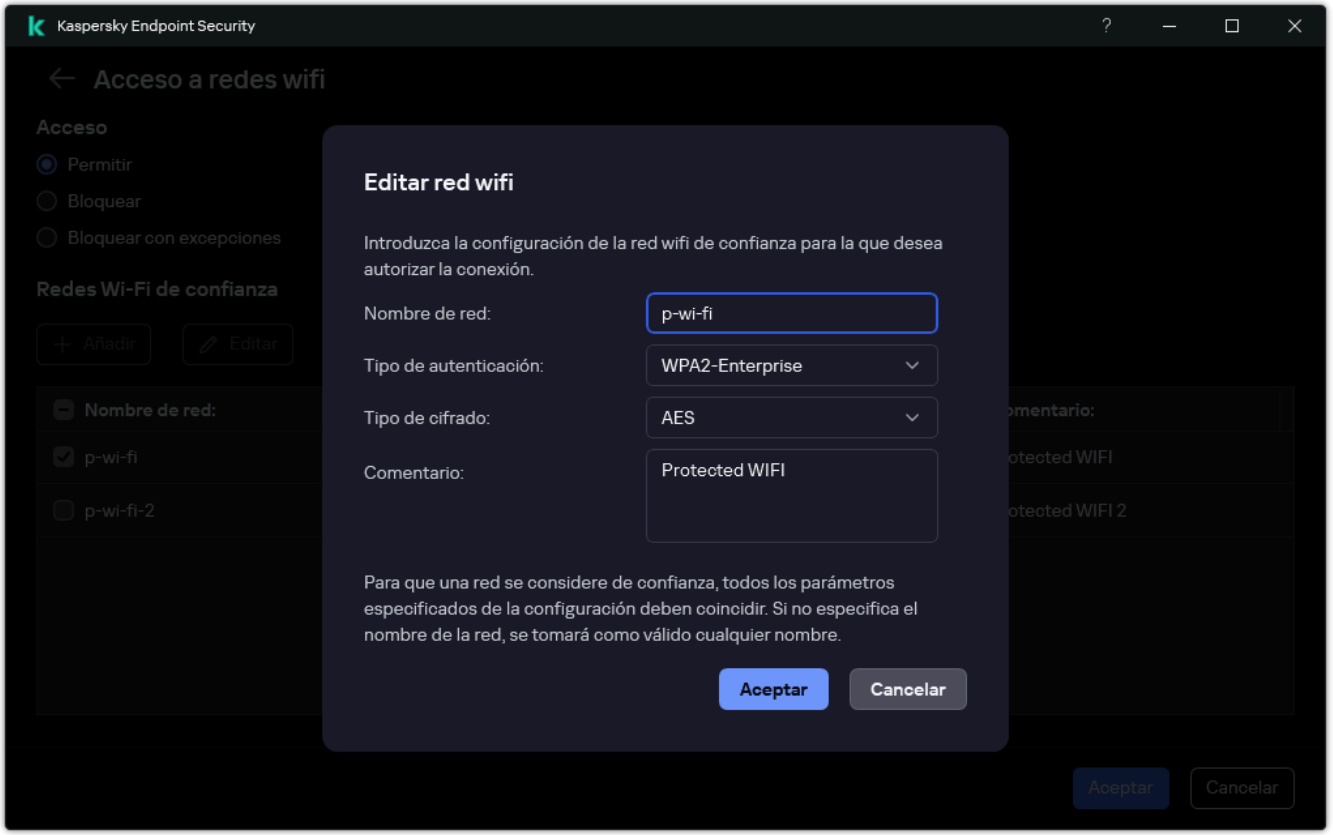
     A partir de la versión 12.0 de Kaspersky Endpoint Security para Windows, se ha agregado la compatibilidad con el protocolo WPA3 a la aplicación. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en un equipo, el protocolo WPA2 se selecciona en equipos con Kaspersky Endpoint Security versión 11.11.0 y anteriores; WPA2/WPA3 se selecciona con las versiones 12.0 a 12.1; WPA3 se selecciona con las versiones 12.2 y posteriores.

   - **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico wifi.
   - **Comentario**. Más información sobre la red wifi añadida.

   Puede ver la configuración de la red wifi de confianza en la configuración del enrutador.

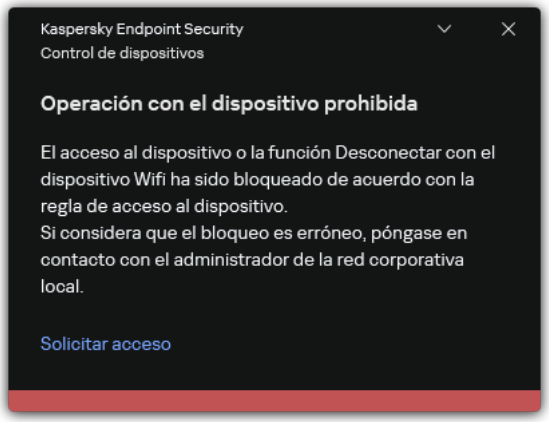
   Una red wifi se considera de confianza si sus ajustes coinciden con todos los que se especifican en la regla.

7. Guarde los cambios.



Configuración de la red wifi de confianza

Como resultado, cuando un usuario intenta conectarse a una red wifi que no figura como de confianza, la aplicación bloquea la conexión y muestra una notificación (consulte la figura a continuación).



Notificación de Control de dispositivos

Seguimiento del uso de unidades extraíbles

La supervisión del uso de unidades extraíbles incluye lo siguiente:

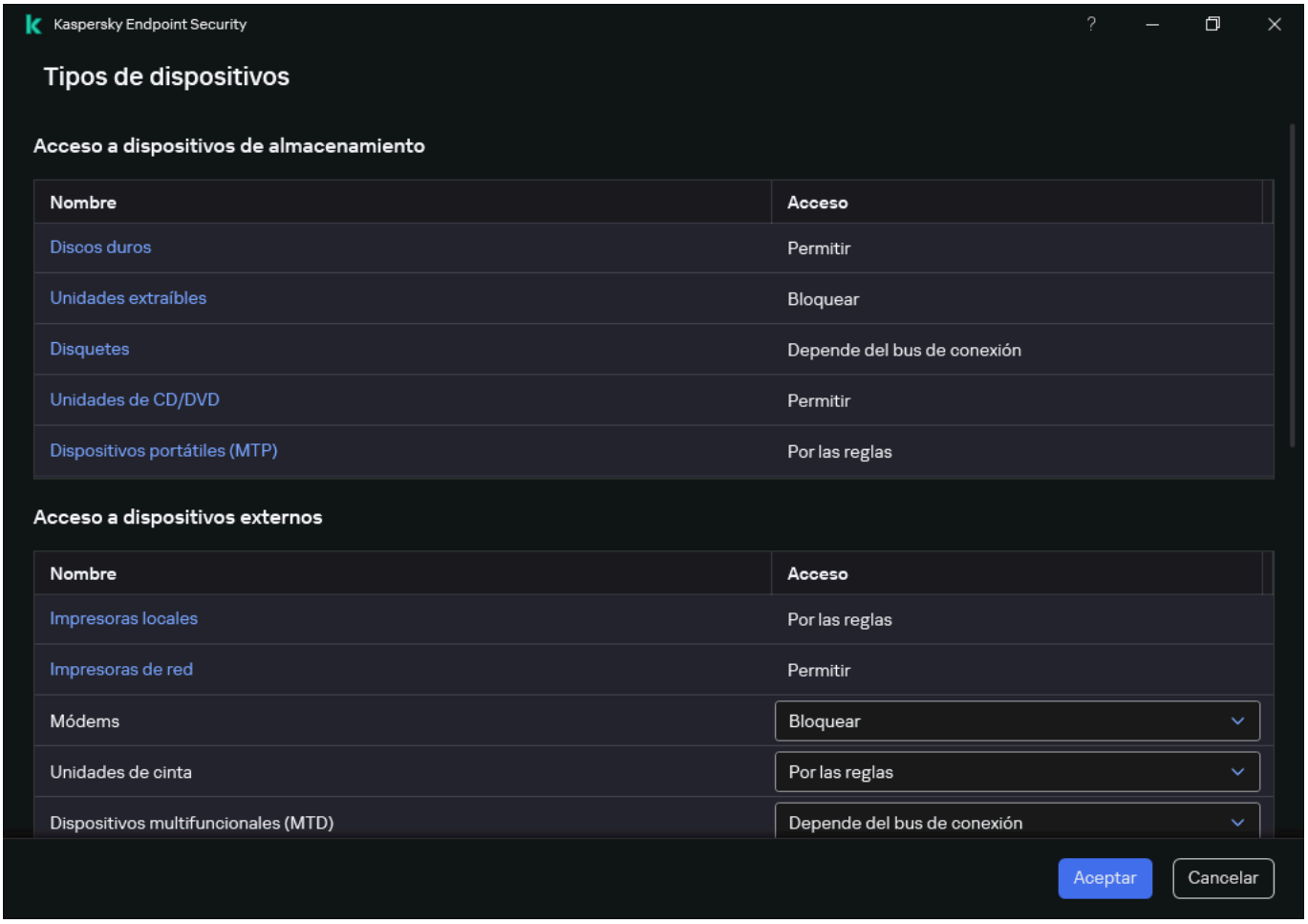
- Supervisión de operaciones en archivos en unidades extraíbles.
- Supervisión de la conexión y desconexión de unidades extraíbles de confianza.

  Kaspersky Endpoint Security permite supervisar la conexión y desconexión de todos los dispositivos de confianza y no solo las unidades extraíbles. Puede activar el registro de eventos en la configuración de notificaciones para el componente de Control de dispositivos. Los eventos tienen el nivel de severidad *Mensaje de información*.

Para activar el seguimiento del uso de unidades extraíbles:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

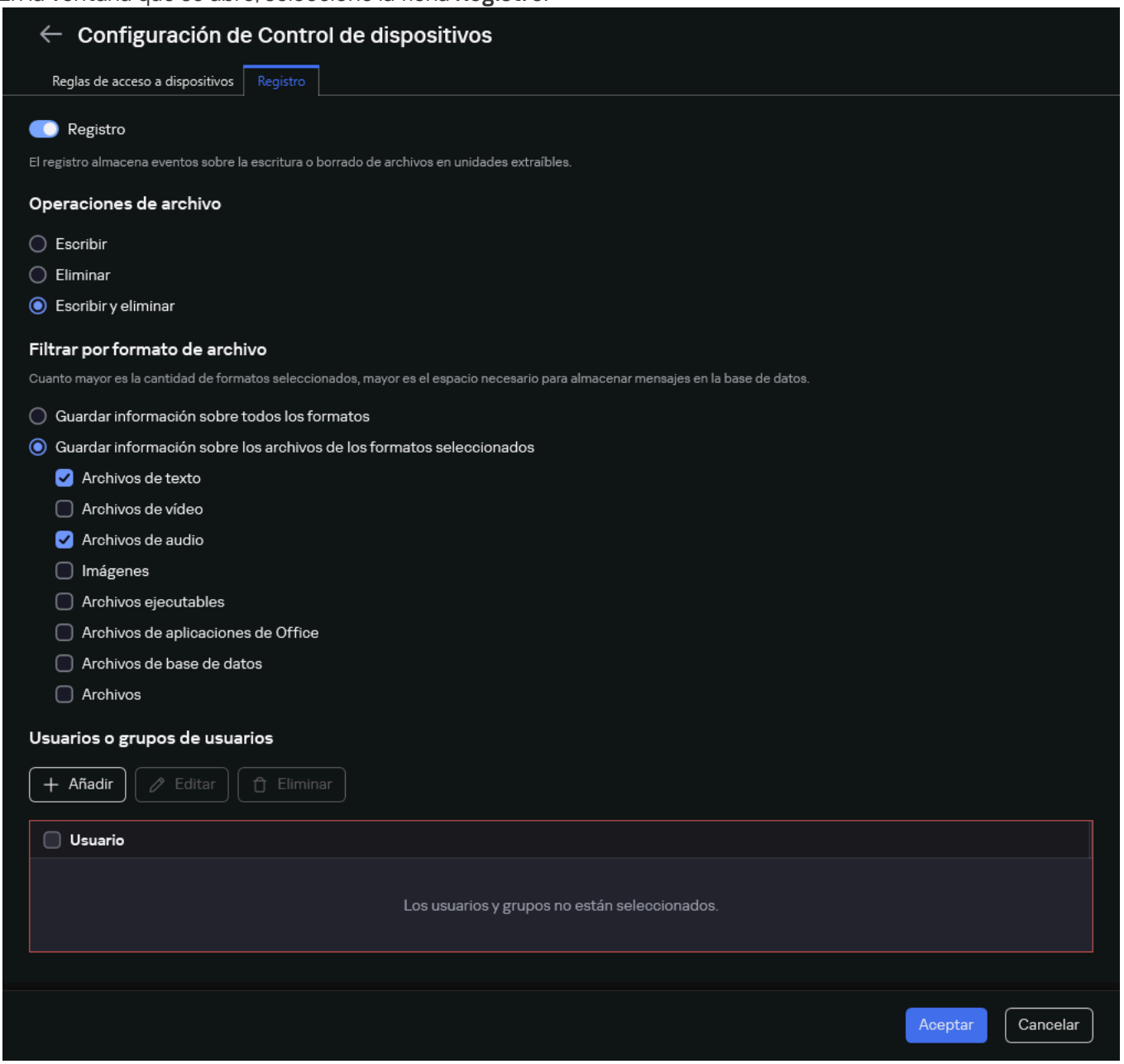
La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.



Tipos de dispositivos en el componente Control de dispositivos

4. En el bloque **Acceso a dispositivos de almacenamiento**, seleccione **Unidades extraíbles**.

5. En la ventana que se abre, seleccione la ficha **Registro**.



La configuración de la supervisión del uso de unidades extraíbles

6. Active la opción **Registro**.

7. En el bloque **Operaciones de archivo**, seleccione las operaciones que desea supervisar: **Escribir**, **Eliminar**.

8. En el bloque **Filtrar por formato de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas deben ser registradas por Control de dispositivos.

9. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.

10. Guarde los cambios.

Como resultado, cuando los usuarios escriben en archivos ubicados en unidades extraíbles o eliminan archivos de unidades extraíbles, Kaspersky Endpoint Security guarda la información sobre esas operaciones en el registro de eventos y envía eventos a Kaspersky Security Center. Puede ver eventos asociados con archivos en unidades extraíbles en la Consola de administración de Kaspersky Security Center, en el espacio de trabajo del nodo **Servidor de administración** en la pestaña **Eventos**. Para que los eventos se muestren en el registro de eventos local de Kaspersky Endpoint Security, debe seleccionar la casilla **Operación de archivo realizada** en la configuración de notificación para el componente Control de dispositivos.

Cambiar la duración del almacenamiento en caché

El componente Control de dispositivos registra eventos relacionados con los dispositivos supervisados, como la conexión y desconexión de un dispositivo, la lectura de un archivo de un dispositivo, la escritura de un archivo en un dispositivo y otros eventos. Luego, Control de dispositivos permite o bloquea la acción de acuerdo con la configuración de Kaspersky Endpoint Security.

Control de dispositivos guarda información sobre eventos durante un período específico llamado *período de almacenamiento en caché*. Si la información sobre un evento se almacena en caché y este evento se repite, no es necesario notificarlo a Kaspersky Endpoint Security ni mostrar otro mensaje para otorgar acceso a la acción correspondiente, como conectar un dispositivo. Esto hace que sea más conveniente trabajar con un dispositivo.

Un evento se considera un evento duplicado si toda la configuración de los eventos siguientes coincide con el registro en el caché:

- ID de dispositivo
- SID de la cuenta de usuario que intenta acceder
- Categoría de dispositivo
- Acción realizada con el dispositivo
- Permiso de la aplicación para esta acción: permitido o denegado
- Ruta del proceso utilizado para realizar la acción
- Archivo al que se accede

Antes de cambiar el período de almacenamiento en caché, desactive Autoprotección de Kaspersky Endpoint Security. Después de cambiar el período de almacenamiento en caché, active Autoprotección.

Para cambiar el período de almacenamiento en caché:

1. Abra el editor de registro en el equipo.
2. En el editor de registro, vaya a la siguiente sección:
   - Para sistemas operativos de 64 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - Para sistemas operativos de 32 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Abra `DeviceControlEventsCachePeriod` para editarlo.
4. Defina la cantidad de minutos en los que Control de dispositivos debe guardar información sobre un evento antes de que se elimine esta información.

Acciones con dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

Para trabajar con dispositivos de confianza, puede otorgar acceso a un usuario individual, a un grupo de usuarios o a todos los usuarios de la organización.

Por ejemplo, si su organización no permite el uso de unidades extraíbles, pero los administradores usan unidades extraíbles en su trabajo, puede permitir unidades extraíbles solo para un grupo de administradores. Para hacerlo, añada unidades extraíbles a la lista de confianza y configure los permisos de acceso de usuario.

No se recomienda añadir más de 5000 dispositivos de confianza, ya que esto puede provocar inestabilidad en el sistema.

Kaspersky Endpoint Security le permite añadir un dispositivo a la lista de confianza de las siguientes maneras:

- Si Kaspersky Security Center no está implementado en su organización, puede conectar el dispositivo al equipo y añadirlo a la lista de confianza en la configuración de la aplicación. Para distribuir la lista de dispositivos de confianza a todos los equipos de su organización, puede activar la combinación de listas de dispositivos de confianza en una directiva o usar el procedimiento de exportación/importación.

- Si utiliza Kaspersky Security Center en su organización, puede detectar todos los dispositivos conectados remotamente y crear una lista de dispositivos de confianza en la directiva. La lista de dispositivos de confianza estará disponible en todos los equipos a los que se aplica la directiva.

Kaspersky Endpoint Security permite controlar el uso de dispositivos de confianza (conexión y desconexión). Puede activar el registro de eventos en la configuración de notificaciones para el componente de Control de dispositivos. Los eventos tienen el nivel de severidad *Mensajes de información*.

Adición de un dispositivo a la lista de confianza

Kaspersky Security Center recibe información sobre los dispositivos si Kaspersky Endpoint Security está instalado en los equipos, el Control de dispositivos está activado y la transmisión de datos del dispositivo está activada. No se puede añadir un dispositivo a la lista de confianza a menos que la información sobre ese dispositivo esté disponible en Kaspersky Security Center.

De forma predeterminada, al añadir un dispositivo a la lista de dispositivos de confianza, a todos los usuarios (el grupo de usuarios Todos) se les concede acceso a este dispositivo.

Puede añadir un dispositivo a la lista de confianza según los datos siguientes:

- **Dispositivos por ID**. Cada dispositivo tiene un identificador exclusivo (Hardware ID o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. Ejemplo de ID de dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.

- **Dispositivos por modelo**. Cada dispositivo tiene un Vendor ID (VID) y un Product ID (PID). Puede ver los ID en las propiedades del dispositivo usando herramientas del sistema operativo. Plantilla para introducir el VID y el PID: `VID_1234&PID_5678`. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.

- **Dispositivos por máscara de ID**. Si utiliza varios dispositivos con ID similares, puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `WDC_C*`.

- **Dispositivos por máscara de modelo**. Si utiliza varios dispositivos con VID y PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `VID_05AC&PID_*`.

Cómo añadir un dispositivo a la lista de confianza en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione **Directivas**.

3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Controles de seguridad → Control de dispositivos**.

5. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.

6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de dispositivos de confianza para todos los equipos de la empresa.

   Se fusionarán las listas de dispositivos de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Los dispositivos de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar dispositivos de confianza de la directiva principal.

7. Haga clic en el botón **Añadir** y seleccione un método para añadir un dispositivo a la lista de confianza.

8. Para filtrar dispositivos, seleccione un tipo de dispositivo de la lista desplegable **Tipo de dispositivo** (por ejemplo, **Unidades extraíbles**).

   Kaspersky Endpoint Security no admite la adición de dispositivos del tipo **Disquetes** en la lista de confianza.

9. En el campo **Nombre o modelo**, introduzca el ID de dispositivo, modelo (VID y PID) o máscara, según el método para añadir seleccionado.

   Añadir dispositivos por máscara de modelo (VID y PID) funciona de la siguiente manera: si introduce una máscara de modelo que no coincida con ningún modelo, Kaspersky Endpoint Security verifica si el ID de dispositivo (HWID) coincide con la máscara. Kaspersky Endpoint Security solo verifica la parte del ID de dispositivo que determina el fabricante y el tipo de dispositivo (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Si la máscara de modelo coincide con esta parte del ID de dispositivo, los dispositivos que coinciden con la máscara se añadirán a la lista de dispositivos de confianza en el equipo. Al mismo tiempo, la lista de dispositivos de Kaspersky Security Center permanece vacía al hacer clic en el botón **Mejorar**. Para mostrar la lista de dispositivos correctamente, puede añadir dispositivos por la máscara de ID de dispositivo.

10. Para filtrar dispositivos, en el campo **Equipo**, introduzca el nombre del equipo o una máscara para el nombre del equipo al que está conectado el dispositivo.

    El carácter `*` sustituye cualquier conjunto de caracteres. El carácter `?` sustituye cualquier carácter único.

11. Haga clic en **Mejorar**.

    La tabla muestra una lista de dispositivos que satisfacen los criterios de filtrado definidos.

12. Seleccione las casillas de verificación junto a los nombres de los dispositivos que quiera añadir a la lista de confianza.

13. En el campo **Comentario**, introduzca una descripción del motivo para añadir dispositivos a la lista de confianza.

14. Haga clic en el botón **Seleccionar**, situado a la derecha del campo **Permitir a usuarios y/o grupos de usuarios**.

    Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

    De forma predeterminada, el acceso a los dispositivos de confianza está permitido para el grupo "Todos".

15. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir un dispositivo a la lista de confianza en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Zona de confianza**.

5. En la ventana que se abre, haga clic en el vínculo **Dispositivos**.

   Esto abre una ventana que contiene una lista de dispositivos de confianza.

6. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.

7. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de dispositivos de confianza para todos los equipos de la empresa.

   Se fusionarán las listas de dispositivos de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Los dispositivos de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar dispositivos de confianza de la directiva principal.

8. Haga clic en **Añadir**.

   Esto abre el formulario para añadir un dispositivo de confianza.

9. En **Usuario o grupo**, seleccione los usuarios a los que desea permitir el acceso a los dispositivos de confianza.

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   De forma predeterminada, el acceso a los dispositivos de confianza está permitido para el grupo "Todos".

10. Para filtrar dispositivos, seleccione un tipo de dispositivo de la lista desplegable **Tipo de dispositivo** (por ejemplo, **Unidades extraíbles**).

    Kaspersky Endpoint Security no admite la adición de dispositivos del tipo **Disquetes** en la lista de confianza.

11. Si no conoce el ID exacto ni el modelo del dispositivo, seleccione la casilla **Usar máscara**.

12. Seleccione cómo desea añadir el dispositivo: por ID o por modelo del dispositivo (VID y PID).

    Añadir dispositivos por máscara de modelo (VID y PID) funciona de la siguiente manera: si introduce una máscara de modelo que no coincida con ningún modelo, Kaspersky Endpoint Security verifica si el ID de dispositivo (HWID) coincide con la máscara. Kaspersky Endpoint Security solo verifica la parte del ID de dispositivo que determina el fabricante y el tipo de dispositivo (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Si la máscara de modelo coincide con esta parte del ID de dispositivo, los dispositivos que coinciden con la máscara se añadirán a la lista de dispositivos de confianza en el equipo. Al mismo tiempo, se mostrará una lista vacía de dispositivos en Kaspersky Security Center. Para mostrar la lista de dispositivos correctamente, puede añadir dispositivos por la máscara de ID de dispositivo.

13. Para filtrar dispositivos, en el campo **Buscar dispositivos de confianza**, introduzca el nombre del equipo o una máscara para el nombre del equipo al que está conectado el dispositivo.

    El carácter `*` sustituye cualquier conjunto de caracteres. El carácter `?` sustituye cualquier carácter único.

    La tabla muestra una lista de dispositivos que satisfacen los criterios de filtrado definidos.

14. Seleccione las casillas de verificación junto a los nombres de los dispositivos que quiera añadir a la lista de confianza.

15. En el campo **Comentario**, introduzca una descripción del motivo para añadir dispositivos a la lista de confianza.

16. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir un dispositivo a la lista de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.
4. Haga clic en **Seleccionar**.

   Esto abre la lista de dispositivos conectados. La lista de dispositivos depende del valor que se seleccione en la lista desplegable **Mostrar dispositivos conectados**.
5. En la lista de dispositivos, seleccione el dispositivo que desea añadir a la lista de confianza.

   Kaspersky Endpoint Security no admite la adición de dispositivos del tipo **Disquetes** en la lista de confianza.
6. En el campo **Comentario**, puede proporcionar cualquier información relevante sobre el dispositivo de confianza.
7. Seleccione los usuarios o grupos de usuarios a los que desea permitir el acceso a los dispositivos de confianza.

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.
8. Guarde los cambios.

Cuando se conecta un dispositivo, Kaspersky Endpoint Security comprueba la lista de dispositivos de confianza para un usuario autorizado. Si el dispositivo es de confianza, Kaspersky Endpoint Security permite el acceso al dispositivo con todos los permisos, incluso si se deniega el acceso al tipo de dispositivo o al bus de conexión. Si el dispositivo no es de confianza y se le deniega el acceso, puede solicitar acceso al dispositivo bloqueado.

Exportación e importación de la lista de dispositivos de confianza

Para distribuir la lista de dispositivos de confianza a todos los equipos de su organización, puede usar el procedimiento de exportación/importación.

Por ejemplo, si necesita distribuir una lista de unidades extraíbles de confianza, tiene que hacer lo siguiente:

1. Conecte las unidades extraíbles a su equipo secuencialmente.
2. En la configuración de Kaspersky Endpoint Security, añada las unidades extraíbles a la lista de confianza. De ser necesario, configure los permisos de acceso de usuario. Por ejemplo, permita que solo los administradores accedan a las unidades extraíbles.
3. Exporte la lista de dispositivos de confianza en la configuración de Kaspersky Endpoint Security (consulte las instrucciones más abajo).

4. Distribuya el archivo de la lista de dispositivos de confianza a otros equipos de su organización. Por ejemplo, coloque el archivo en una carpeta compartida.

5. Importe la lista de dispositivos de confianza en la configuración de Kaspersky Endpoint Security en otros equipos de la organización (consulte las instrucciones más abajo).

Para importar o exportar la lista de dispositivos de confianza:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.

4. Para exportar la lista de dispositivos de confianza:

   a. Seleccione los dispositivos de confianza que desee exportar.

   b. Haga clic en **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de dispositivos de confianza y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista completa de dispositivos de confianza al archivo XML.

5. Para importar la lista de dispositivos de confianza:

   a. En la lista desplegable **Importar**, seleccione la acción correspondiente: **Importar y añadir al existente** o **Importar y sustituir el existente**.

   b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de dispositivos de confianza.

   c. Abra el archivo.

6. Guarde los cambios.

Cuando se conecta un dispositivo, Kaspersky Endpoint Security comprueba la lista de dispositivos de confianza para un usuario autorizado. Si el dispositivo es de confianza, Kaspersky Endpoint Security permite el acceso al dispositivo con todos los permisos, incluso si se deniega el acceso al tipo de dispositivo o al bus de conexión.

Obtención de acceso a un dispositivo bloqueado

Al configurar el componente Control de dispositivos, existe el riesgo de bloquear inadvertidamente el acceso a un dispositivo que se necesita para trabajar.

Si no utiliza Kaspersky Security Center en su organización, puede brindar acceso a un dispositivo a través de los ajustes de Kaspersky Endpoint Security. Por ejemplo, puede añadir el dispositivo a la lista de dispositivos de confianza o desactivar el componente Control de dispositivos en forma temporal.

Si en su organización sí utilizan Kaspersky Security Center y los equipos tienen una directiva aplicada, puede otorgar acceso al dispositivo a través de la Consola de administración.

Modo con conexión para otorgar acceso

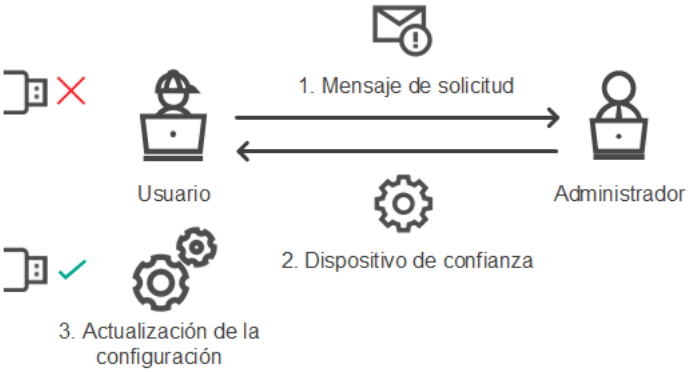
Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo con conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. También es necesario que el equipo pueda comunicarse con el Servidor de administración.

Estos son los pasos para otorgar acceso a un dispositivo en el modo con conexión:

1. El usuario envía un mensaje con una solicitud de acceso al administrador.
2. El administrador recibe un mensaje con la solicitud en la consola de Kaspersky Security Center.

   La consola de Kaspersky Security Center tiene una selección de eventos preestablecida *Solicitudes de los usuarios* para facilitar el seguimiento de los mensajes de los usuarios.
3. El administrador añade el dispositivo a la lista de dispositivos de confianza.

   Para añadir un dispositivo de confianza, existen dos alternativas: modificar una directiva aplicada al grupo de administración o modificar la configuración local de la aplicación instalada en un equipo específico.
4. El administrador actualiza la configuración de Kaspersky Endpoint Security en el equipo del usuario.



Esquema para otorgar acceso a un dispositivo en el modo con conexión

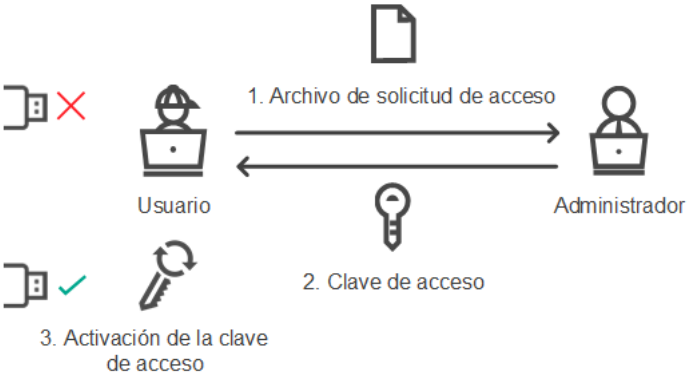
Modo sin conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo sin conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. En la configuración de la directiva, dentro de la sección **Control de dispositivos**, la casilla **Permitir solicitudes de acceso temporal** debe estar activada.

Si necesita otorgar acceso temporal a un dispositivo, pero no puede añadirlo a la lista de dispositivos de confianza, puede utilizar el modo sin conexión. Este modo permite otorgar acceso a un dispositivo bloqueado aun cuando un equipo no tiene conexión a la red o se encuentra fuera de la red corporativa.

Estos son los pasos para otorgar acceso a un dispositivo en el modo sin conexión:

1. El usuario crea un archivo de solicitud de acceso y se lo envía al administrador.
2. Con el archivo de solicitud de acceso, el administrador crea una clave de acceso y se la envía al usuario.
3. El usuario activa la clave de acceso.



Esquema para otorgar acceso a un dispositivo en el modo sin conexión

Modo con conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo con conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. También es necesario que el equipo pueda comunicarse con el Servidor de administración.

Para solicitar acceso a un dispositivo bloqueado como usuario:

1. Conecte el dispositivo al equipo.

   Kaspersky Endpoint Security mostrará una notificación para indicar que el acceso al dispositivo está bloqueado (vea la imagen de más abajo).

2. Haga clic en el enlace **Solicitar acceso**.

   Se abre una ventana con un mensaje para el administrador. El mensaje contendrá información sobre el dispositivo bloqueado.

3. Haga clic en **Enviar**.



Notificación de Control de dispositivos

A continuación, el administrador de la consola de Kaspersky Security Center recibe el evento *Mensaje al administrador por bloqueo del acceso al dispositivo*. El evento incluye el nombre de usuario, el nombre del equipo, información sobre el dispositivo al que el usuario intenta acceder y otra información. Puede configurar cómo recibe las notificaciones de dichos eventos el administrador y, por ejemplo, seleccionar notificaciones de correo electrónico. La consola de Kaspersky Security Center tiene una selección de eventos preestablecida *Solicitudes de los usuarios* para facilitar el seguimiento de los mensajes de los usuarios.

Para permitir el acceso, debe añadir el dispositivo a la lista de confianza. Después de actualizar la configuración de Kaspersky Endpoint Security en el equipo, el usuario podrá acceder al dispositivo.

Modo sin conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo sin conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. En la configuración de la directiva, dentro de la sección **Control de dispositivos**, la casilla **Permitir solicitudes de acceso temporal** debe estar activada.

Para solicitar acceso a un dispositivo bloqueado como usuario:

1. Conecte el dispositivo al equipo.

   Kaspersky Endpoint Security mostrará una notificación para indicar que el acceso al dispositivo está bloqueado (vea la imagen de más abajo).

2. Haga clic en el enlace **Solicitar acceso temporal**.

   Esto abre una ventana que incluye una lista de dispositivos conectados.

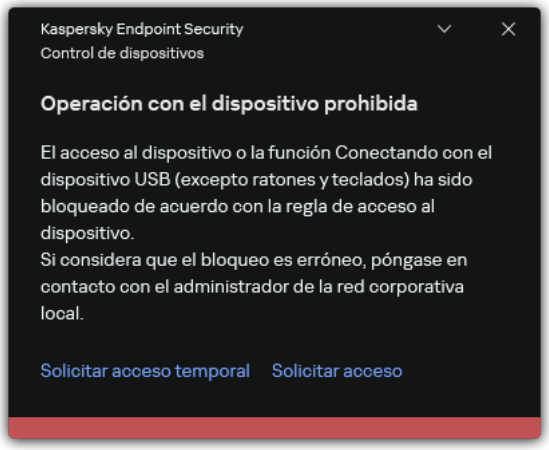
3. En la lista de dispositivos conectados, seleccione el dispositivo al que desee obtener acceso.

4. Haga clic en **Generar archivo de solicitud de acceso**.

5. En el campo **Duración del acceso**, especifique el período de tiempo durante el que desea disponer de acceso al dispositivo.

6. Guarde el archivo en el equipo.

Como resultado, se descargará al equipo un archivo de solicitud de acceso (cuya extensión será *.akey). Envíe este archivo al administrador de la LAN corporativa utilizando cualquier método a su disposición.



Notificación de Control de dispositivos

Cómo puede el administrador crear una clave de acceso para el dispositivo bloqueado en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la lista de equipos cliente, seleccione el equipo de un usuario que necesite obtener acceso temporal a un dispositivo bloqueado.
5. En el menú contextual del equipo, seleccione el elemento **Conceder acceso en modo sin conexión**.
6. Se abre una ventana; en ella, seleccione la pestaña **Control de dispositivos**.
7. Haga clic en el botón **Examinar** y descargue el archivo de solicitud de acceso que recibió del usuario.

   Verá información sobre el dispositivo bloqueado al que el usuario desea acceder.
8. De ser necesario, cambie el valor del parámetro **Duración del acceso**.

   De manera predeterminada, el valor de **Duración del acceso** es el mismo que indicó el usuario al crear el archivo de solicitud de acceso.
9. Especifique el valor del parámetro **Activar el**.

   Este parámetro define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado mediante la clave de acceso proporcionada.
10. Guarde el archivo clave de acceso en el equipo.

Cómo puede el administrador crear una clave de acceso para el dispositivo bloqueado en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. En la lista de equipos cliente, seleccione el equipo de un usuario que necesite obtener acceso temporal a un dispositivo bloqueado.
3. Haga clic en el botón de elipsis (**...**) sobre la lista de equipos y, a continuación, en el botón **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione la sección **Control de dispositivos**.
5. Haga clic en el botón **Descripción general** y descargue el archivo de solicitud de acceso que recibió del usuario.

   Verá información sobre el dispositivo bloqueado al que el usuario desea acceder.
6. De ser necesario, cambie el valor del parámetro **Duración del acceso (horas)**.

   De manera predeterminada, el valor de **Duración del acceso (horas)** es el mismo que indicó el usuario al crear el archivo de solicitud de acceso.

7. Especifique el periodo de tiempo durante el que se puede activar la clave de acceso en el dispositivo.

   Este parámetro define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado mediante la clave de acceso proporcionada.

8. Guarde el archivo clave de acceso en el equipo.

Como resultado, se descargará al equipo una clave de acceso para el dispositivo bloqueado. Los archivos clave de acceso tienen la extensión *.acode. Envíe el archivo clave de acceso al usuario utilizando cualquier método a su disposición.

Para activar una clave de acceso como usuario:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Solicitud de acceso**, haga clic en el botón **Solicitar acceso al dispositivo**.
4. En la ventana que se abre, haga clic en el botón **Activar clave de acceso**.
5. En la ventana que se abre, seleccione el archivo con la clave de acceso que le envió el administrador de la LAN corporativa.

   Se abrirá una ventana con información sobre el acceso que le han otorgado.

6. Haga clic en **Aceptar**.

Como resultado, el usuario obtendrá acceso al dispositivo por el tiempo que haya definido el administrador. El usuario tendrá acceso completo (derechos de lectura y de escritura) al dispositivo. Cuando la clave caduque, se bloqueará el acceso al dispositivo. Si el usuario necesita acceso permanente al dispositivo, añada el dispositivo a la lista de dispositivos de confianza.

Edición de plantillas de mensajes de Control de dispositivos

Cuando el usuario intenta acceder a un dispositivo bloqueado, Kaspersky Endpoint Security muestra un mensaje que afirma que el acceso al dispositivo está bloqueado o que una operación con los contenidos del dispositivo está prohibida. Los expertos de Kaspersky proporcionan al usuario una plantilla de mensaje que describe los motivos por los que se bloqueó el acceso al dispositivo (consulte la figura a continuación).

Se proporcionan variables especiales para administrar la plantilla de mensaje (por ejemplo, %USER_NAME%). Las variables permiten utilizar una única plantilla de mensaje para diferentes ordenadores. Al generar un mensaje, Kaspersky Endpoint Security recupera el valor de la variable de la configuración del sistema operativo y lo inserta en el mensaje correspondiente al equipo, usuario y evento específicos.



Notificación de Control de dispositivos

Si el usuario cree que el acceso al dispositivo se bloqueó por error o que una operación con contenidos del dispositivo se prohibió por error, el usuario puede enviar un mensaje al administrador de la red corporativa local haciendo clic en el enlace del mensaje mostrado sobre la acción bloqueada. Para hacerlo, el usuario debe hacer clic en los botones **Solicitar acceso** o **Solicitar acceso temporal** y enviar un mensaje al administrador describiendo la situación. También puede preparar una plantilla del mensaje para el administrador, añadiéndole datos que pueden informar de su decisión de permitir o bloquear el acceso al dispositivo. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso al dispositivo**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

Cómo cambiar la plantilla de mensaje de Control de dispositivos en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de dispositivos**.
4. En el bloque **Configuración de la plantilla de mensajes**, haga clic en el botón **Plantillas**.
5. Esto abre una ventana; dentro de esa ventana, configure las plantillas de Control de aplicaciones:

   - **Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo.
   - **Mensaje al administrador**. Una plantilla del mensaje que se envía al administrador de la LAN cuando el usuario cree que el acceso al dispositivo está bloqueado o que se ha prohibido una operación con el contenido del dispositivo por error.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y elija la variable requerida de la lista de opciones disponibles.

También puede restaurar el texto predeterminado de la plantilla.

6. Guarde los cambios.

Cómo cambiar la plantilla del mensaje de Control de dispositivos en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control de dispositivos**.
5. En el bloque **Plantillas de mensajes**, configure plantillas para mensajes de Control de aplicaciones:

   - **Mensaje al usuario**. Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo.
   - **Mensaje al administrador**. Una plantilla del mensaje que se envía al administrador de la LAN cuando el usuario cree que el acceso al dispositivo está bloqueado o que se ha prohibido una operación con el contenido del dispositivo por error.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla.
6. Guarde los cambios.

Cómo cambiar la plantilla del mensaje de Control de dispositivos en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. En el bloque **Modelos de mensajes**, configure plantillas para mensajes de Control de aplicaciones:

   - **Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo.
   - **Mensaje para el administrador**. Una plantilla del mensaje que se envía al administrador de la LAN cuando el usuario cree que el acceso al dispositivo está bloqueado o que se ha prohibido una operación con el contenido del dispositivo por error.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla.
4. Guarde los cambios.

Anti-Bridging

Anti-Bridging impide establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red. La finalidad es resguardar la red de la empresa de los ataques que puedan realizarse a través de redes desprotegidas y no autorizadas.

Para regular la posibilidad de establecer conexiones de red, Anti-Bridging utiliza *reglas de conexión*.

Las reglas de conexión se crean para estos tipos predefinidos de dispositivos:

- Adaptadores de red;
- Adaptadores wifi;
- Módems.

Si una regla de conexión está activada, Kaspersky Endpoint Security:

- Bloquea la conexión activa al establecer una nueva conexión si el tipo de dispositivo especificado en la regla se usa para ambas conexiones;
- Bloquea las conexiones que se establecen usando los tipos de dispositivos para los que se utilizan reglas de prioridad inferior.

Activar el componente Anti-Bridging

La función Anti-Bridging está desactivada de forma predeterminada.

Para activar el componente Anti-Bridging:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Anti-Bridging**.
4. Utilice el interruptor **Activar el componente Anti-Bridging** para activar o desactivar esta función.
5. Guarde los cambios.

Con Anti-Bridging activado, Kaspersky Endpoint Security bloquea conexiones ya establecidas según lo indicado en las reglas de conexión.

Cambio del estado de una regla de conexión

Para cambiar el estado de una regla de conexión:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Anti-Bridging**.
4. En el bloque **Reglas para dispositivos**, seleccione la regla cuyo estado desea cambiar.
5. Utilice los interruptores de la columna **Control** para activar o desactivar la regla.
6. Guarde los cambios.

Cambio de la prioridad de una regla de conexión

Para cambiar la prioridad de una regla de conexión:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Anti-Bridging**.
4. En el bloque **Reglas para dispositivos**, seleccione la regla cuya prioridad desea cambiar.
5. Utilice los botones **Arriba**/**Abajo** para establecer la prioridad de la regla de conexión.

   Cuanto más arriba está una regla en la tabla, mayor es su prioridad. Anti-Bridging bloquea todas las conexiones excepto una conexión establecida usando el tipo de dispositivo para el que se utiliza la regla de la prioridad más alta.
6. Guarde los cambios.

Control de anomalías adaptativo

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos en una red de la empresa. El Control de anomalías adaptativo utiliza un conjunto de reglas para supervisar el comportamiento atípico (por ejemplo, la regla *Inicio de Microsoft Powershell desde una aplicación de Office*). Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa. Puede configurar el modo en que el Control de anomalías adaptativo gestiona cada regla y, por ejemplo, permitir la ejecución de scripts de PowerShell que automatizan determinadas tareas de flujo de trabajo. Kaspersky Endpoint Security actualiza el conjunto de reglas junto con las bases de datos de la aplicación. Las actualizaciones de los conjuntos de reglas deben confirmarse manualmente.

Parámetros del Control de anomalías adaptativo

Para configurar el Control de anomalías adaptativo se tienen que realizar los pasos siguientes:

1. Autoaprendizaje del Control de anomalías adaptativo.

   Después de habilitar el Control de anomalías adaptativo, sus reglas funcionan en el *modo de autoaprendizaje*. Durante el aprendizaje, el Control de anomalías adaptativo supervisa la activación de reglas y envía eventos de activación a Kaspersky Security Center. Cada regla tiene su propia duración del modo de autoaprendizaje. La duración del modo de autoaprendizaje es establecida por los expertos de Kaspersky. Por lo general, el modo de autoaprendizaje está activo durante dos semanas.

   Si una regla no se ha activado nunca durante el autoaprendizaje, el Control de anomalías adaptativo considerará las acciones asociadas a esta regla como no típicas. Kaspersky Endpoint Security bloqueará todas las acciones asociadas a esa regla.

   Si se activó una regla durante el autoaprendizaje, Kaspersky Endpoint Security registra los eventos en el informe de activación de las reglas y en el repositorio de **Activación de reglas en el estado Aprendizaje inteligente**.

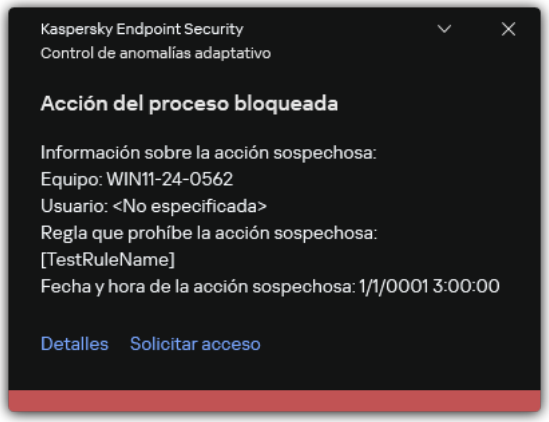
2. Analizar el informe de activación de las reglas.

   El administrador analiza el informe de activación de reglas o el contenido del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. A continuación, el administrador puede seleccionar el comportamiento del Control de anomalías adaptativo cuando se active la regla para bloquearlo o permitirlo. El administrador también puede seguir supervisando el funcionamiento de la regla y ampliar su duración durante el modo de autoaprendizaje. Si el administrador no realiza ninguna acción, la aplicación también seguirá funcionando en el modo de autoaprendizaje. El plazo de aprendizaje se reiniciará.

El Control de anomalías adaptativo se configura en tiempo real a través de los siguientes canales:

- El Control de anomalías adaptativo empieza a bloquear automáticamente las acciones asociadas con las reglas que no se activaron nunca en el modo de autoaprendizaje.
- Kaspersky Endpoint Security añade nuevas reglas o elimina las obsoletas.
- El administrador configura el funcionamiento del Control de anomalías adaptativo tras revisar el informe de activación de las reglas o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. Recomendamos consultar el informe sobre la activación de reglas y el contenido del almacenamiento de **Activación de reglas en el estado Aprendizaje inteligente**.

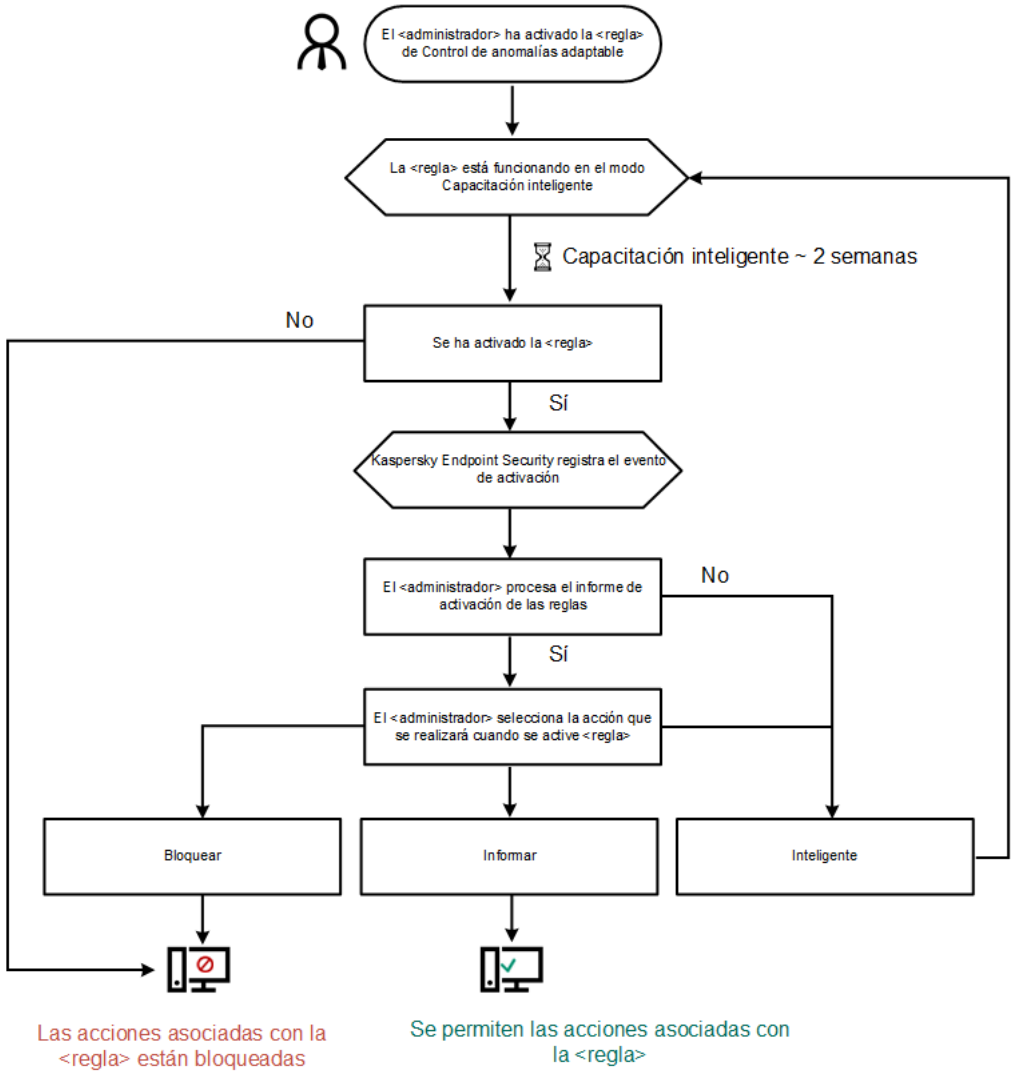
Cuando una aplicación maliciosa intenta realizar una acción, Kaspersky Endpoint Security bloqueará dicha acción y mostrará una notificación (vea la figura a continuación).



Notificación del Control de anomalías adaptativo

Algoritmo de funcionamiento del Control de anomalías adaptativo

Kaspersky Endpoint Security decide si se autoriza o se bloquea una acción que esté asociada con una regla de acuerdo al siguiente algoritmo (consulte la siguiente figura).



Algoritmo de funcionamiento del Control de anomalías adaptativo

Autoaprendizaje del Control de anomalías adaptativo

El Control de anomalías adaptativo incluye un conjunto de reglas (patrones de comportamiento). Después de habilitar el Control de anomalías adaptativo, sus reglas funcionan en el *modo de autoaprendizaje*. Durante el aprendizaje, el Control de anomalías adaptativo supervisa la activación de reglas y envía eventos de activación a Kaspersky Security Center. El Control de anomalías adaptativo no bloquea la actividad de la aplicación en el equipo, solo informa al administrador. También puede seleccionar manualmente la acción que se realiza cuando se activa una regla del Control de anomalías adaptativo:

Cómo ver la lista de reglas de Control de anomalías adaptativo en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Controles de seguridad → Control de anomalías adaptativo**.
5. Seleccione la casilla **Control de anomalías adaptativo**.
6. En **Configuración de regla de Control de anomalías adaptativo**, mire la lista de reglas.
   De forma predeterminada, todas las reglas funcionan en el modo **Inteligente**.
7. Si es necesario, confirme la actualización de la regla de Control de anomalías adaptativo.
8. Si es necesario, seleccione una acción para cuando se active una regla del Control de anomalías adaptativo:
   - **Bloquear**. Si se selecciona esta acción, cuando se active una regla del Control de anomalías adaptativo, Kaspersky Endpoint Security bloqueará la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.
   - **Informar**. Si se selecciona esta acción, cuando se active una regla de Control de anomalías adaptativo, Kaspersky Endpoint Security permitirá la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.
9. Si es necesario, desactive las reglas que no desee utilizar.
10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo ver las reglas de Control de anomalías adaptativo en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad → Control de anomalías adaptativo**.
5. Active la opción **Control de anomalías adaptativo ACTIVADO**.

6. En **Reglas**, mire la lista de reglas.

   De forma predeterminada, todas las reglas funcionan en el modo **Inteligente**.

7. Si es necesario, confirme la actualización de la regla de Control de anomalías adaptativo.

8. Si es necesario, seleccione una acción para cuando se active una regla del Control de anomalías adaptativo:

   - **Bloquear**. Si se selecciona esta acción, cuando se active una regla del Control de anomalías adaptativo, Kaspersky Endpoint Security bloqueará la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.

   - **Informar**. Si se selecciona esta acción, cuando se active una regla de Control de anomalías adaptativo, Kaspersky Endpoint Security permitirá la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.

9. Si es necesario, desactive las reglas que no desee utilizar.

10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo ver la lista de reglas de Control de anomalías adaptativo en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de anomalías adaptativo**.

3. Active la opción **Control de anomalías adaptativo**.

4. En el bloque **Reglas**, haga clic en el enlace **Editar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo. De forma predeterminada, todas las reglas funcionan en el modo **Inteligente**.

5. Si es necesario, confirme la actualización de la regla de Control de anomalías adaptativo.

6. Si es necesario, seleccione una acción para cuando se active una regla del Control de anomalías adaptativo:

   - **Bloquear**. Si se selecciona esta acción, cuando se active una regla del Control de anomalías adaptativo, Kaspersky Endpoint Security bloqueará la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.

   - **Informar**. Si se selecciona esta acción, cuando se active una regla de Control de anomalías adaptativo, Kaspersky Endpoint Security permitirá la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.

7. Si es necesario, desactive las reglas que no desee utilizar.

8. Guarde los cambios.

Cada regla tiene su propia duración del modo de autoaprendizaje. La duración del modo de autoaprendizaje es establecida por los expertos de Kaspersky. Por lo general, el modo de autoaprendizaje está activo durante dos semanas.

Si, durante el entrenamiento, una regla nunca se activó, el Control de anomalías adaptativo considera que dicho comportamiento es atípico y cambia el estado de la regla a **Bloqueo inteligente**. Posteriormente, la aplicación bloquea cualquier actividad que coincida con esta regla.

Si una regla se activa durante el entrenamiento, debe configurar manualmente la acción que aplica la aplicación a la actividad detectada que coincide con esta regla. Si no selecciona la acción cuando se activa la regla, el Control de anomalías adaptativo continúa en el modo de entrenamiento.

Activación y desactivación de una regla del Control de anomalías adaptativo

Para activar o desactivar una regla del Control adaptable de anomalías:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.
4. En la tabla, seleccione un conjunto de reglas (por ejemplo, *Actividad de las aplicaciones de Office*) y amplíe el conjunto.
5. Seleccione una regla (por ejemplo, *Inicio de Microsoft Powershell desde una aplicación de Office*).
6. Utilice el interruptor en la columna **Condición** para activar o desactivar la regla de Control de anomalías adaptativo.
7. Guarde los cambios.

Cambio de la acción que se realiza al activarse una regla del Control de anomalías adaptativo

Para cambiar lo que ocurre cuando se activa una regla del Control de anomalías adaptativo:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.
4. Seleccione una regla en la tabla.
5. Haga clic en **Editar**.

   Se abre la ventana de propiedades de las reglas de Control de anomalías adaptativo.

6. En el bloque **Acción**, seleccione una de las opciones siguientes:

   - **Inteligente**. Si elige esta opción, la regla del Control de anomalías adaptativo funcionará en estado Aprendizaje inteligente durante el plazo definido por los expertos de Kaspersky. En este modo, cuando una regla del Control de anomalías adaptativo se activa, Kaspersky Endpoint Security permite la actividad determinada por la regla y añade una entrada de registro en el repositorio **Activación de reglas en el estado Aprendizaje inteligente** del Servidor de administración de Kaspersky Security Center. Cuando concluye el período de trabajo en el estado Aprendizaje inteligente, Kaspersky Endpoint Security bloquea la actividad determinada por la regla y añade una entrada de registro con información sobre la actividad.

   - **Bloquear**. Si se selecciona esta acción, cuando se active una regla del Control de anomalías adaptativo, Kaspersky Endpoint Security bloqueará la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.

   - **Informar**. Si se selecciona esta acción, cuando se active una regla de Control de anomalías adaptativo, Kaspersky Endpoint Security permitirá la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.

7. Guarde los cambios.

Crear una exclusión de una regla del Control de anomalías adaptativo

No es posible crear más de 1000 exclusiones para las reglas del Control de anomalías adaptativo. No se recomienda crear más de 200 exclusiones. Si necesita reducir el número de exclusiones que utiliza, considere usar máscaras en la configuración de las exclusiones.

Una exclusión de una regla del Control de anomalías adaptable incluye una descripción de los objetos de origen y de destino. El *objeto de origen* es el que realiza las acciones. El *objeto de destino* es el que se ve afectado por dichas acciones. Supongamos que se abre un archivo denominado `file.xlsx`. Como resultado se carga en la memoria del equipo un archivo de biblioteca con la extensión DLL. Esta biblioteca se utiliza en un navegador (archivo ejecutable denominado `browser.exe`). En el marco de este ejemplo, `file.xlsx` es el objeto de origen, Excel es el proceso de origen, `browser.exe` es el objeto de destino y Navegador es el proceso de destino.

Para crear una exclusión de una regla del Control de anomalías adaptativo:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de anomalías adaptativo**.

3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.

4. Seleccione una regla en la tabla.

5. Haga clic en **Editar**.

   Se abre la ventana de propiedades de las reglas de Control de anomalías adaptativo.

6. En el bloque **Exclusiones**, haga clic en el botón **Añadir**.

   Se abre la ventana de propiedades de exclusiones.

7. Seleccione el usuario para el que desea configurar una exclusión.

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   El Control de anomalías adaptativo no admite exclusiones para grupos de usuarios. Si selecciona un grupo de usuarios, Kaspersky Endpoint Security no aplicará la exclusión.

8. En el campo **Descripción**, describa la exclusión.

9. Defina los parámetros del objeto de origen o de el proceso de origen iniciados por el objeto:

   - **Proceso de origen**. Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, `C:\Dir\File.exe` o `Dir\*.exe`).
   - **Hash de proceso de origen**. Hash SHA256 del archivo.
   - **Objeto de origen**. Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, `C:\Dir\File.exe` o `Dir\*.exe`). También podría usar, por ejemplo, la ruta a un archivo de nombre `document.docm`, que utilice un script o una macro para iniciar los procesos de destino.

     También es posible especificar otras clases de objetos, como direcciones web, macros, comandos para la línea de comandos o rutas del Registro. Para ello, utilice la plantilla: `object://<object>`, donde `<object>` indica el nombre del objeto; por ejemplo, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. También puede usar máscaras (por ejemplo, `object://*C:\Windows\temp\*`).
   - **Hash de objeto de origen**. Hash SHA256 del archivo.

   La regla del Control de anomalías adaptable no se aplicará a las acciones que el objeto realice o a los procesos que el objeto inicie.

10. Especifique los parámetros del objeto de destino o de los procesos de destino iniciados en los que el objeto esté involucrado.

    - **Proceso de destino**. Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, `C:\Dir\File.exe` o `Dir\*.exe`).
    - **Hash de proceso de destino**. Hash SHA256 del archivo.
    - **Objeto de destino**. Comando para iniciar el proceso de destino. Para especificar el comando, utilice el modelo `object://<command>` (por ejemplo, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`). También puede usar máscaras (por ejemplo, `object://*C:\Windows\temp\*`).
    - **Hash de objeto de destino**. Hash SHA256 del archivo.

    La regla del Control de anomalías adaptable no se aplicará a las acciones que afecten al objeto o a los procesos en los que el objeto esté involucrado.

11. Guarde los cambios.

Importar e importar exclusiones para las reglas del Control de anomalías adaptativo

Para exportar o importar la lista de exclusiones para las reglas seleccionadas:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.
4. Para exportar la lista de reglas:
   a. Seleccione las reglas cuyas excepciones quiera exportar.
   b. Haga clic en **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
   d. Confirme que desea exportar solo las exclusiones seleccionadas o exportar la lista completa de exclusiones.
   e. Guarde el archivo.
5. Para importar la lista de exclusiones:
   a. Haga clic en **Importar**.
   b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
   c. Abra el archivo.

      Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
6. Guarde los cambios.

Actualización de las reglas del Control de anomalías adaptativo

Cuando se actualizan las bases de datos antivirus, la tabla de reglas del Control de anomalías adaptativo puede modificarse: puede ocurrir que se incorporen reglas nuevas y que se eliminen otras existentes. Si hay una actualización de reglas que está pendiente de aplicarse, Kaspersky Endpoint Security distingue las reglas del Control de anomalías adaptativo que van a añadirse o eliminarse.

Cuando una actualización aún no se ha aplicado, las reglas del Control de anomalías adaptativo que se eliminarán con la actualización continúan mostrándose en la tabla de reglas, pero Kaspersky Endpoint Security les asigna el estado *Desactivado*. No es posible cambiar la configuración de estas reglas.

Para actualizar las reglas del Control de anomalías adaptativo:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.
4. En la ventana que se abre, haga clic en el botón **Aprobar actualizaciones**.

   El botón **Aprobar actualizaciones** estará activo cuando haya una actualización disponible para las reglas del Control de anomalías adaptativo.
5. Guarde los cambios.

Modificación de las plantillas de mensajes del Control de anomalías adaptativo

Cuando un usuario intenta realizar una acción bloqueada por las reglas de Control de anomalías adaptativo, Kaspersky Endpoint Security muestra un mensaje notificando que se han bloqueado acciones potencialmente dañinas. Si el usuario cree que una acción se ha bloqueado por error, el usuario puede utilizar el enlace incluido en el texto del mensaje para enviar un mensaje al administrador de la red corporativa local.

Hay plantillas especiales disponibles para enviar mensajes al administrador sobre el bloqueo de acciones potencialmente dañinas. Se proporcionan variables especiales para administrar la plantilla de mensaje (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensaje para diferentes ordenadores. Al generar un mensaje, Kaspersky Endpoint Security recupera el valor de la variable de la configuración del sistema operativo y lo inserta en el mensaje correspondiente al equipo, usuario y evento específicos.

Para editar una plantilla de mensaje:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de anomalías adaptativo**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control de anomalías adaptativo:

   - **Mensaje sobre el bloqueo**. Plantilla del mensaje que se muestra a un usuario cuando se activa una regla del Control de anomalías adaptativo que bloquea una acción no típica.
   - **Mensaje para el administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red corporativa local si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo de la actividad de aplicaciones**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Restablecer**.

4. Guarde los cambios.

Supervisión de las operaciones de Control de anomalías adaptativo

El Control de anomalías adaptativo incluye varias herramientas de supervisión. El objetivo principal de la supervisión del Control de anomalías adaptativo es configurar el componente durante el entrenamiento.

Informes de Control de anomalías adaptativo

El Control de anomalías adaptativo utiliza los siguientes informes:

- **Informe de estado de reglas de Control de anomalías adaptativo**. El informe contiene información sobre el estado de las reglas de Control de anomalías adaptativo (*Desactivado*, *Entrenamiento inteligente*, *Bloqueo inteligente*, *Notificar* y *Bloquear*). Este informe permite analizar el nivel de entrenamiento del Control de anomalías adaptativo y evaluar el número de reglas que han cambiado del modo *Entrenamiento inteligente* al modo de funcionamiento normal (por ejemplo, *Bloqueo inteligente*).

- **Informe de reglas de Control de anomalías adaptativo activado**. El informe contiene información sobre los activadores de reglas. El informe también muestra el modo de activación de la regla: *Bloquear* (incluyendo *Bloqueo inteligente*) o *Notificar*. Este informe permite evaluar la actividad del Control de anomalías adaptativo en los equipos de los usuarios.

Cómo ver los informes de Control de anomalías adaptativo en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de anomalías adaptativo**.

4. Realice una de las siguientes acciones:

   - Si desea ver el informe sobre el estado de las reglas del Control de anomalías adaptativo, haga clic en enlace **Informe de estado de reglas de Control de anomalías adaptativo**.

   - Si desea ver el informe sobre las reglas activadas del Control de anomalías adaptativo, haga clic en el enlace **Informe de reglas de Control de anomalías adaptativo activado**.

5. Se inicia el proceso de generación de informes.

El informe se muestra en una nueva ventana.

Cómo ver los informes de Control de anomalías adaptativo en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad → Control de anomalías adaptativo**.
5. En el bloque **Reglas**, lleve a cabo una de estas acciones:
   - Si desea ver el informe sobre el estado de las reglas del Control de anomalías adaptativo, elija **Ver informe → Estado de las reglas**.
   - Si desea ver el informe sobre las reglas activadas del Control de anomalías adaptativo, haga clic en **Ver informe → Detecciones**.
6. Se inicia el proceso de generación de informes.

El informe se muestra en una nueva ventana.

Para generar informes en la consola de Kaspersky Security Center , debe activar la transferencia de datos al Servidor de administración. La transferencia de datos está activada de forma predeterminada.

Cómo activar la transferencia de datos para Control de anomalías adaptativo en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Informes y Almacenamiento**.
4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.
5. Marque las siguientes casillas:
   - **Informe de estado de reglas de Control de anomalías adaptativo**.
   - **Informe de reglas de Control de anomalías adaptativo activado**.
6. Guarde los cambios.

Cómo activar la transferencia de datos para Control de anomalías adaptativo en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Integración con KSC**.

5. En **Transferencia de datos al Servidor de administración**, seleccione las siguientes casillas:

   - **Informe de estado de reglas de Control de anomalías adaptativo**.
   - **Informe de reglas de Control de anomalías adaptativo activado**.

6. Guarde los cambios.

Almacenamiento de Activación de reglas en el estado Aprendizaje inteligente

En el modo de entrenamiento, el Control de anomalías adaptativo envía información sobre las reglas activadas a un almacenamiento independiente, **Activación de reglas en el estado Aprendizaje inteligente**. La información sobre las reglas activadas se representa en el almacenamiento como una lista de eventos. Para ajustar el Control de anomalías adaptativo, puede confirmar el comportamiento atípico en el equipo o añadir una exclusión de la regla.

Eventos del Control de anomalías adaptativo

Los registros de Control de anomalías adaptativo desencadenan eventos en los modos *Bloquear* (incluyendo *Bloqueo inteligente*) y *Notificar*. Los siguientes eventos se proporcionan para este propósito:

Acción del proceso bloqueada

Acción del proceso omitida

Los eventos contienen información sobre la actividad sospechosa, incluidas las sumas de comprobación de archivos, los usuarios involucrados, la hora de activación de la regla y el nombre del equipo. Después de analizar el evento, puede agregar exclusiones de la regla inmediatamente si encuentra que la actividad es legítima.

Control de aplicaciones

El Control de aplicaciones gestiona el inicio de aplicaciones en los equipos de los usuarios. Esto le permite implementar una directiva corporativa de seguridad al usar aplicaciones. El Control de aplicaciones también reduce el riesgo de infección del equipo al restringir el acceso a las aplicaciones.

La configuración del Control de aplicaciones consta de los siguientes pasos:

1. Creación de categorías de aplicaciones.

   El administrador crea categorías de aplicaciones que el administrador quiere gestionar. Las categorías de aplicaciones están destinadas a todos los equipos de la red corporativa, independientemente de los grupos de administración. Para crear una categoría, puede usar los siguientes criterios: categoría KL (por ejemplo, *Navegadores*) u otra categoría, hash de archivo, proveedor de aplicaciones y otros criterios.

2. Crear reglas de Control de aplicaciones.

   El administrador crea reglas de Control de aplicaciones en la directiva para el grupo de administración. La regla incluye las categorías de aplicaciones y el estado de inicio de las aplicaciones de estas categorías: bloqueadas o permitidas. El administrador puede crear muchas reglas. Una aplicación puede coincidir con los criterios de varias reglas. La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. Kaspersky Endpoint Security comprueba si una aplicación coincide con una regla cada vez que se inicia. Kaspersky Endpoint Security compara secuencialmente la aplicación con todas las reglas de Control de aplicaciones.

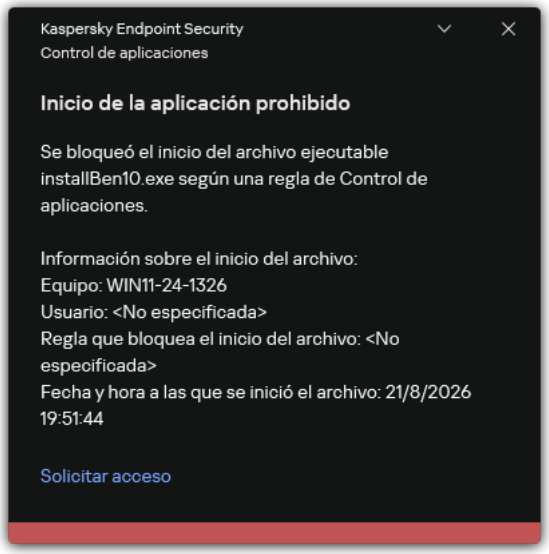
3. Seleccionar el modo de Control de aplicaciones.

   El administrador elige el modo para trabajar con las aplicaciones que no estén incluidas en ninguna de las reglas (listas de aplicaciones admitidas y rechazadas).

Cuando un usuario intenta iniciar una aplicación prohibida, Kaspersky Endpoint Security bloqueará el inicio de dicha aplicación y mostrará una notificación (vea la figura a continuación).

Se proporciona un *modo de prueba* para comprobar la configuración de Control de aplicaciones. En este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite el inicio de aplicaciones, incluidas las prohibidas.
- Muestra una notificación sobre el inicio de una aplicación prohibida y añade información al informe en el equipo del usuario.
- Envía datos sobre el inicio de aplicaciones prohibidas a Kaspersky Security Center.



Notificación de Control de aplicaciones

Modos de funcionamiento de Control de aplicaciones

El componente Control de aplicaciones funciona en dos modos:

- **Lista de rechazados**. En este modo, Control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de Control de aplicaciones.

  Este modo de Control de aplicaciones está activado de forma predeterminada.

- **Lista de permitidos**. En este modo, Control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de Control de aplicaciones.

Si las reglas de autorización de Control de aplicaciones están totalmente configuradas, el componente bloquea el inicio de todas las aplicaciones nuevas que no haya verificado el administrador de la red de área local, mientras que autoriza el funcionamiento del sistema operativo y de las aplicaciones de confianza en las que los usuarios confían en su trabajo.

Puede leer las recomendaciones sobre la configuración de reglas de Control de aplicaciones en el modo de lista de admitidos.

El Control de aplicaciones puede configurarse para que funcione en estos modos tanto mediante la interfaz local de Kaspersky Endpoint Security como mediante Kaspersky Security Center.

Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas que son necesarias para las siguientes tareas:

- Creación de categorías de aplicaciones.

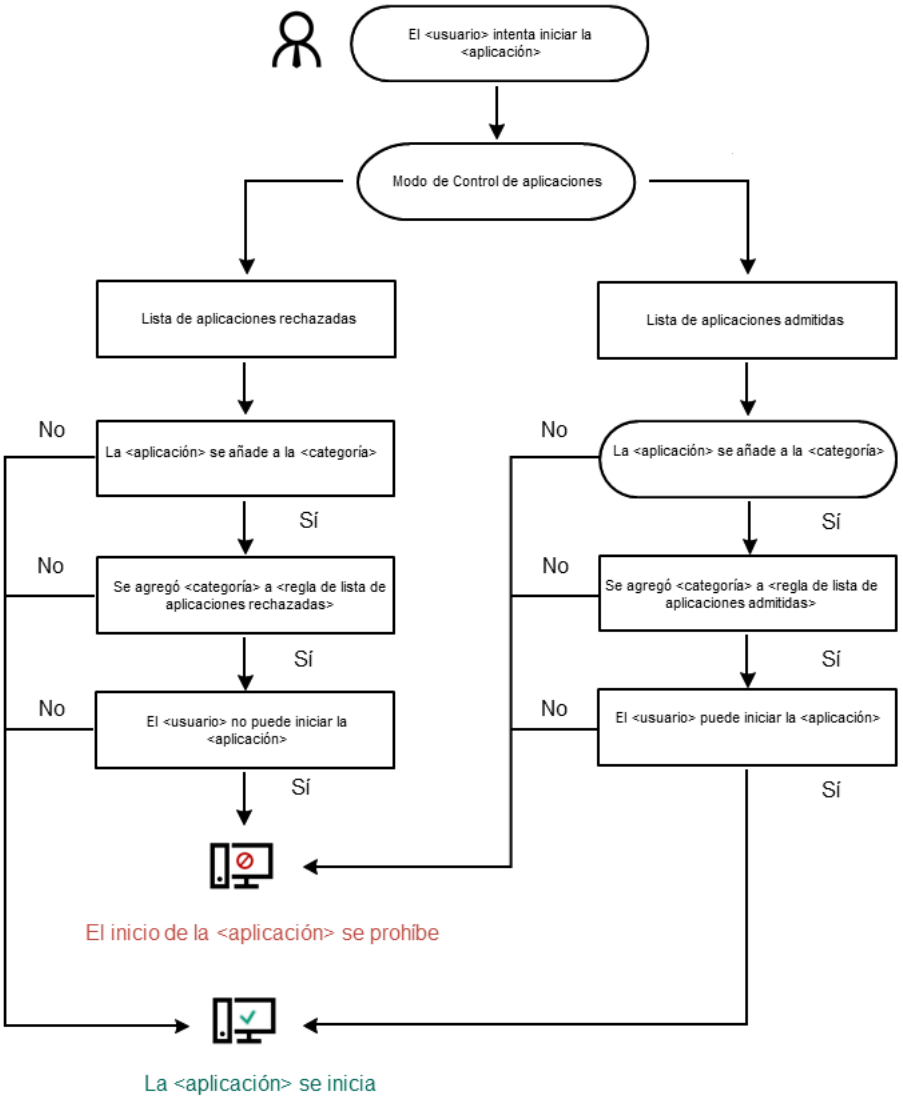
  Las reglas del componente Control de aplicaciones de la consola de administración de Kaspersky Security Center se basan en categorías de aplicaciones predeterminadas, y no en reglas de inclusión y exclusión, como sucede en la interfaz local de Kaspersky Endpoint Security.

- Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN.

Por eso, se recomienda usar Kaspersky Security Center para configurar el funcionamiento del componente Control de aplicaciones.

Algoritmo de funcionamiento de Control de aplicaciones

Kaspersky Endpoint Security utiliza un algoritmo para tomar una decisión sobre el inicio de una aplicación (vea la figura a continuación).



Algoritmo de funcionamiento de Control de aplicaciones

Limitaciones de funcionalidad de Control de aplicaciones

El funcionamiento del componente Control de aplicaciones queda limitado en los casos siguientes:

- Cuando se actualiza la versión de la aplicación, no se admite la importación de la configuración del componente Control de aplicaciones.
- Si no hay conexión con los servidores del KSN, Kaspersky Endpoint Security recibe la información sobre la reputación de las aplicaciones y sus módulos solo desde las bases de datos locales.

  La lista de aplicaciones que Kaspersky Endpoint Security designa como categoría KL **Otro software\Aplicaciones de confianza de acuerdo con la reputación en KSN** puede diferir dependiendo de si está disponible o no una conexión a los servidores de KSN.

- En la base de datos de Kaspersky Security Center, es posible almacenar información acerca de 150 000 archivos procesados. Una vez que se alcance este número de archivos, no se procesarán nuevos archivos. Para reanudar las operaciones de inventario, debe eliminar los archivos que se inventariaron anteriormente en la base de datos de Kaspersky Security Center desde el equipo en el cual se instaló Kaspersky Endpoint Security.
- El componente no controla el inicio de scripts a menos que el script se envíe al intérprete mediante la línea de comandos.

  Si está permitido el inicio de un intérprete por parte de reglas de Control de aplicaciones, el componente no bloqueará un script iniciado por este intérprete.

  Basta que uno de los scripts especificados en la línea de comandos del intérprete esté bloqueado desde el inicio por las Reglas de control de aplicaciones, para que el componente bloquee todos los scripts especificados en la línea de comandos del intérprete.

- El componente no controla el inicio de scripts desde aquellos intérpretes no admitidos por Kaspersky Endpoint Security.

  Kaspersky Endpoint Security admite los siguientes intérpretes:

  - Java
  - PowerShell

  Se admiten los siguientes tipos de intérpretes:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe

- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Obtener información sobre las aplicaciones instaladas

Para crear reglas óptimas de Control de aplicaciones, se recomienda obtener primero una imagen de las aplicaciones que se utilizan en los equipos de la red de área local corporativa. Para ello, puede obtener la siguiente información:

- Proveedores, versiones y localizaciones de las aplicaciones utilizadas en la red de área local corporativa.
- Frecuencia de las actualizaciones de la aplicación.
- Las directivas de uso de aplicaciones adoptadas en la empresa (puede tratarse de directivas de seguridad o directivas administrativas).
- Ubicación donde se almacenan los paquetes de distribución de la aplicación.

Visualización de información de la aplicación

La información sobre las aplicaciones instaladas la proporciona Kaspersky Security Center Network Agent. La información sobre las aplicaciones instaladas está disponible en la consola de Kaspersky Security Center, en la carpeta **Registro de aplicaciones**. El Agente de red actualiza la información en cada sincronización con Kaspersky Security Center. Para obtener más detalles sobre la información enviada por el Agente de red, consulte la Ayuda de Kaspersky Security Center.

Para abrir la ventana de propiedades de aplicaciones en la carpeta Registro de aplicaciones:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione **Avanzado → Administración de aplicaciones → Registro de aplicaciones**.
3. Seleccione una aplicación.
4. En el menú contextual de la aplicación, seleccione **Propiedades**.

Ver información sobre archivos ejecutables

Puede reducir la carga en la base de datos al consultar información sobre archivos ejecutables. Para lograr esto, recomendamos ejecutar la tarea *Inventario* en varios equipos de referencia que tengan instalado su conjunto de software estándar.

Kaspersky Endpoint Security proporciona información sobre los archivos ejecutables. Para recibir información sobre el hardware, debe aplicar una directiva activa que permita transmitir información sobre las aplicaciones instaladas (esta transmisión está activada de forma predeterminada).

Cómo activar el envío de información de la aplicación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Informes y Almacenamiento**.
4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.
5. Seleccione la casilla **Aplicaciones iniciadas**.
6. Guarde los cambios.

Cómo activar el envío de información de la aplicación mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Integración con KSC**.
5. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración avanzada**.

6. En la ventana que se abre, active la casilla **Acerca de aplicaciones iniciadas**.

7. Guarde los cambios.

Puede obtener una lista de archivos ejecutables con la tarea *Inventario* de Kaspersky Endpoint Security. Puede ver la lista de archivos ejecutables en la consola de Kaspersky Security Center, en la carpeta **Archivos ejecutables**.

Antes de ejecutar la tarea *Inventario*, asegúrese de que la base de datos cumpla con las recomendaciones de Kaspersky Security Center. Para obtener más información sobre las limitaciones de la base de datos, consulte la Ayuda de Kaspersky Security Center.

Cómo ejecutar la tarea Inventario en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Inventario**.

Paso 2. Cobertura del inventario

Cree una lista de carpetas en las que desea que Kaspersky Endpoint Security busque archivos ejecutables. Configure los parámetros del inventario (consulte la tabla a continuación).

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Selección de la cuenta para ejecutar la tarea

Seleccione una cuenta para ejecutar la tarea *Inventario*. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local. Si la cobertura del inventario incluye unidades de red u otros objetos con acceso restringido, seleccione una cuenta de usuario con los derechos de acceso suficientes.

Paso 5. Configurar una planificación de inicio de tarea

Configure la planificación de la tarea; por ejemplo, manualmente.

Paso 6. Definir el nombre de la tarea

Introduzca un nombre para la tarea: por ejemplo, *Inventario de línea de base*.

Paso 7. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, se realiza una búsqueda de archivos ejecutables en los equipos de los usuarios de acuerdo con el programa configurado.

Cómo ejecutar una tarea Inventario en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Inventario**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve; por ejemplo, *Inventario de línea de base*.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Para configurar la tarea, vaya a las propiedades de la tarea (consulte la tabla a continuación).

8. Active la casilla ubicada junto a la tarea.

9. Haga clic en **Iniciar**.

   Puede supervisar el estado de la tarea y el número de dispositivos en los que se completó correctamente o con errores. Como resultado, se buscan archivos ejecutables en los equipos de usuario según la planificación especificada.

Para abrir la ventana de propiedades de un archivo ejecutable en la carpeta Archivos ejecutables:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la Consola de administración, seleccione **Avanzado → Administración de aplicaciones → Archivos ejecutables**.

3. Seleccione un archivo ejecutable.

4. En el menú contextual del archivo ejecutable, seleccione **Propiedades**.

Para ver la información general acerca de la aplicación y sus archivos ejecutables, así como la lista de equipos en los que se instala una aplicación, abra la ventana de propiedades de una aplicación que esté seleccionada en la carpeta **Registro de aplicaciones** o en la carpeta **Archivos ejecutables**.

Actualización de la información sobre las aplicaciones y archivos ejecutables instalados

Se ha optimizado el funcionamiento del componente Control de aplicaciones con la base de datos de archivos ejecutables en Kaspersky Endpoint Security. Kaspersky Endpoint Security actualiza automáticamente la base de datos después de que se elimine el archivo del equipo. Esto permite mantener la base de datos actualizada y ahorrar recursos de Kaspersky Security Center. Para mantener la base de datos de aplicaciones instaladas actualizada, se debe activar el envío de información de la aplicación al Servidor de administración (activada de forma predeterminada).

Configuración de inventario

Parámetro	Descripción
Coberturas del inventario	Lista de objetos que formarán la cobertura del inventario.
Inventario de módulos de DLL	Kaspersky Endpoint Security busca módulos DLL en la cobertura del inventario y envía información a Kaspersky Security Center. Habilitar el inventario de módulos DLL aumenta significativamente el tiempo que lleva completar la tarea de Inventario y el tamaño de la base de datos.

Parámetro	Descripción
Inventario de archivos de script	Kaspersky Endpoint Security busca scripts en la cobertura del inventario y envía la información a Kaspersky Security Center. Habilitar el inventario de archivos de scripts aumenta significativamente el tiempo que lleva completar la tarea de Inventario y el tamaño de la base de datos.
Ejecutar solo cuando el equipo está inactivo	Inicio pospuesto de la tarea cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.
Analizar solamente archivos nuevos y modificados	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
Omitir archivo cuyo análisis dure más de (seg) N s	Al limitar el tiempo de ejecución de la tarea. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.
Analizar archivos	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
No descomprimir archivos compuestos de gran tamaño	Si esta casilla de verificación está marcada, la aplicación no analiza archivos compuestos cuyo tamaño exceda el valor especificado. Si esta casilla de verificación no está marcada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.

Cómo activar el modo de aplicaciones bloqueadas

En el modo *Aplicaciones bloqueadas*, Control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de Control de aplicaciones. Es decir, si no existe una regla de denegación, el Control de aplicaciones permite iniciar la aplicación. Este modo de Control de aplicaciones está activado de forma predeterminada.

Antes de activar el modo *Aplicaciones bloqueadas*, recomendamos probar las reglas de Control de aplicaciones. Para ello, puede activar el modo de prueba.

Cómo activar el modo de aplicaciones bloqueadas en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de aplicaciones**.
5. Seleccione la casilla **Control de aplicaciones**.
6. En el bloque **Configuración de Control de aplicaciones**, use la lista desplegable **Modo de control** para seleccionar **Lista de rechazados**.

7. En la lista desplegable **Acción**, seleccione la acción para Control de aplicaciones:

- **Probar reglas**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución no está permitida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, se bloquearían.
- **Aplicar reglas**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

8. Seleccione el estado de las reglas de Control de aplicaciones:

- **Activa**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Inactiva**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplican la regla, pero registra datos sobre el inicio de esas aplicaciones en el informe.

Si necesario, añada nuevas reglas de Control de aplicaciones.

9. Configure los parámetros avanzados de Control de aplicaciones:

- **Supervisar la carga de los módulos DLL (incrementa significativamente la carga del sistema)**. Si se selecciona, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. La información sobre el módulo de DLL y la aplicación que cargó dicho módulo se registra en el informe.

  Si planea activar el control sobre los controladores y módulos DLL que se carguen, asegúrese de que, en la configuración Control de aplicaciones, esté activada la regla **Golden Image** predeterminada u otra regla que contenga la categoría KL "**Golden Image\Certificados de confianza**" y garantice que los controladores y módulos DLL de confianza se carguen antes de que se inicie Kaspersky Endpoint Security. Activar la supervisión de la carga de los módulos DLL y los controladores cuando la regla **Golden Image** esté desactivada puede causar inestabilidad en el sistema operativo.

  Kaspersky Endpoint Security solamente supervisa los controladores y módulos DLL que se carguen desde el momento en que se selecciona la casilla de verificación. Después de seleccionar la casilla de verificación, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.

- **Usar verificación de firma digital estricta**. Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si esta casilla está seleccionada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas con certificados solo del almacén de certificados del sistema de confianza. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección; por ejemplo, la tarea *Análisis antimalware*. Sin embargo, si especifica un certificado de un almacén tienda diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla.

  Si la casilla está desactivada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas por un certificado de la Trusted Root Certificate Store de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección supervisan la actividad de dichas aplicaciones.

- **Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.

- **Mensaje al administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error.

10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar el modo de aplicaciones bloqueadas en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de aplicaciones**.

5. Active la opción **Control de aplicaciones ACTIVADO**.

6. En el bloque **Modo de funcionamiento**, seleccione **Bloquear todo excepto la lista de reglas**.

7. En el bloque **Acción**, seleccione la acción para Control de aplicaciones:

   - **Informar**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución no está permitida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, se bloquearían.

   - **Aplicar reglas**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

8. Seleccione el estado de las reglas de Control de aplicaciones:

   - **Activado**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.

   - **Desactivado**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.

   - **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplican la regla, pero registra datos sobre el inicio de esas aplicaciones en el informe.

   Si necesario, añada nuevas reglas de Control de aplicaciones.

9. Configure los parámetros avanzados de Control de aplicaciones:

   - **Supervisar carga de los módulos DLL**. Si se selecciona, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. La información sobre el módulo de DLL y la aplicación que cargó dicho módulo se registra en el informe.

Si planea activar el control sobre los controladores y módulos DLL que se carguen, asegúrese de que, en la configuración Control de aplicaciones, esté activada la regla **Golden Image** predeterminada u otra regla que contenga la categoría KL "**Golden Image\Certificados de confianza**" y garantice que los controladores y módulos DLL de confianza se carguen antes de que se inicie Kaspersky Endpoint Security. Activar la supervisión de la carga de los módulos DLL y los controladores cuando la regla **Golden Image** esté desactivada puede causar inestabilidad en el sistema operativo.

Kaspersky Endpoint Security solamente supervisa los controladores y módulos DLL que se carguen desde el momento en que se selecciona la casilla de verificación. Después de seleccionar la casilla de verificación, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.

- **Usar verificación de firma digital estricta**. Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si esta casilla está seleccionada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas con certificados solo del almacén de certificados del sistema de confianza. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección; por ejemplo, la tarea *Análisis antimalware*. Sin embargo, si especifica un certificado de un almacén tienda diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla.

  Si la casilla está desactivada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas por un certificado de la Trusted Root Certificate Store de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección supervisan la actividad de dichas aplicaciones.

- **Mensaje al usuario**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.

- **Mensaje al administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error.

10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar el modo de aplicaciones bloqueadas en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de aplicaciones**.
3. Active la opción **Control de aplicaciones**.
4. En el bloque **Modo de control de inicio de la aplicación**, seleccione **Lista de rechazados. Se permiten todas las aplicaciones, excepto las que figuran en la lista de reglas**.
5. En el bloque **Acción al iniciar aplicaciones bloqueadas por reglas**, seleccione la acción para Control de aplicaciones:

   - **Informar (Modo de prueba) y registrar eventos en informe**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución no está permitida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, se bloquearían.

   - **Bloquear**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

6. Seleccione el estado de las reglas de Control de aplicaciones:

- **Activado**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Desactivado**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplican la regla, pero registra datos sobre el inicio de esas aplicaciones en el informe.

Si necesario, añada nuevas reglas de Control de aplicaciones.

7. Configure los parámetros avanzados de Control de aplicaciones:

- **Supervisar carga de los módulos DLL**. Si se selecciona, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. La información sobre el módulo de DLL y la aplicación que cargó dicho módulo se registra en el informe.

  Si planea activar el control sobre los controladores y módulos DLL que se carguen, asegúrese de que, en la configuración Control de aplicaciones, esté activada la regla **Golden Image** predeterminada u otra regla que contenga la categoría KL "**Golden Image\Certificados de confianza**" y garantice que los controladores y módulos DLL de confianza se carguen antes de que se inicie Kaspersky Endpoint Security. Activar la supervisión de la carga de los módulos DLL y los controladores cuando la regla **Golden Image** esté desactivada puede causar inestabilidad en el sistema operativo.

  Kaspersky Endpoint Security solamente supervisa los controladores y módulos DLL que se carguen desde el momento en que se selecciona la casilla de verificación. Después de seleccionar la casilla de verificación, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.

- **Usar verificación de firma digital estricta**. Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si esta casilla está seleccionada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas con certificados solo del almacén de certificados del sistema de confianza. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección; por ejemplo, la tarea *Análisis antimalware*. Sin embargo, si especifica un certificado de un almacén tienda diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla.

  Si la casilla está desactivada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas por un certificado de la Trusted Root Certificate Store de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección supervisan la actividad de dichas aplicaciones.

- **Plantillas de mensajes sobre el bloque de aplicaciones**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.
- **Texto del mensaje de la plantilla que se muestra cuando se bloquea el inicio de una aplicación**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error.

8. Guarde los cambios.

Como resultado, Control de aplicaciones bloquea las aplicaciones bloqueadas. Kaspersky Endpoint Security también genera eventos de *Inicio de la aplicación prohibido*. Puede utilizar estos eventos para generar el informe *Informe sobre aplicaciones prohibidas* en la consola de Kaspersky Security Center. En el resumen del informe, puede ver la lista de aplicaciones y equipos en los que se activó la regla de Control de aplicaciones.

Control de aplicaciones basado en un equipo de línea de base

Puede usar un equipo de línea de base para crear una imagen con un conjunto de aplicaciones que necesite. A continuación, puede usar esta imagen para implementar el sistema operativo y las aplicaciones en otros equipos. No siempre es posible mantener actualizada la imagen. El Control de aplicaciones le permite mantener una lista de aplicaciones permitidas basada en un equipo de línea de base. El Control de aplicaciones determina automáticamente qué aplicaciones están instaladas en el equipo de línea de base y actualiza la categoría. De esta forma, los equipos obtienen una lista actualizada de aplicaciones permitidas.

La configuración del Control de aplicaciones en función de un equipo de línea de base implica los siguientes pasos:

1. Creación de una categoría de actualización automática. Al crear la nueva categoría, seleccione la categoría **Categoría que incluye archivos ejecutables de una carpeta específica** y seleccione su equipo de línea de base.

   Cómo crear una categoría de actualización automática en la Consola de administración (MMC)

   1. Abra la Consola de administración de Kaspersky Security Center.
   2. En el árbol de la Consola de administración, seleccione **Avanzado → Administración de aplicaciones → Categorías de aplicaciones**.
   3. Haga clic en el botón **Categoría nueva** en el espacio de trabajo.

      Esto inicia el asistente de creación de categorías de aplicaciones.
   4. Siga las instrucciones del asistente de creación de categorías de aplicaciones.

   ### Paso 1. Selección del tipo de categoría

   Seleccione **Categoría que incluye archivos ejecutables de dispositivos seleccionados** como tipo de categoría.

   ### Paso 2. Introducción de un nombre de categoría de usuario

   En este paso, especifique un nombre para la categoría de aplicación.

Paso 3. Configuración

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**.

En este paso, haga clic en el botón **Añadir** y especifique los equipos cuyos archivos ejecutables añadirá Kaspersky Security Center a la categoría de aplicaciones. Kaspersky Security Center añadirá a la categoría de aplicación todos los archivos ejecutables de los equipos especificados presentados en la carpeta **Archivos ejecutables**.

En este paso, también puede ajustar la configuración siguiente:

- Algoritmo para el cálculo de la función hash. Para elegir un algoritmo, debe marcar como mínimo una de las siguientes casillas:
  - **Calcular SHA256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.
  - **Calcular MD5 para archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.
- La casilla **Sincronizar datos con el repositorio del Servidor de administración**. Seleccione esta casilla si desea que Kaspersky Security Center borre periódicamente la categoría de aplicaciones y añada a ella todos los archivos ejecutables desde los equipos especificados incluidos en la carpeta **Archivos ejecutables**.

  Si la casilla de verificación **Sincronizar datos con el repositorio del Servidor de administración** está desactivada, Kaspersky Security Center no realizará ninguna modificación en una categoría de aplicación después de crearla.

Paso 4. Filtro

En este paso, configure un filtro para archivos.

Puede especificar el tipo de archivo que desea usar para crear la categoría de aplicaciones.

- **Todos los archivos**. La categoría coincidirá con todos los archivos. Esta opción está seleccionada de forma predeterminada.
- **Solo archivos fuera de las categorías de aplicaciones**. La categoría coincidirá solo con archivos fuera de las categorías de aplicación.

Puede especificar carpetas de equipos seleccionados que contengan archivos que desee usar para crear la categoría de aplicaciones.

- **Todas las carpetas**. La categoría coincidirá con todas las carpetas. Esta opción está seleccionada de forma predeterminada.
- **Carpeta especificada**. La categoría coincidirá solo con la carpeta especificada. Si selecciona esta opción, debe especificar una ruta de carpeta.

Paso 5. Creación de una categoría personalizada

Finalice el asistente.

Cómo crear una categoría con contenido añadido automáticamente en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Operaciones → Aplicaciones de terceros → Categorías de aplicaciones**.

   Esto abre la lista de categorías de aplicaciones.

2. Haga clic en **Añadir**.

   Esto inicia el asistente de creación de categorías de aplicaciones.

3. Configure los parámetros generales de la categoría de aplicaciones

   - Nombre de la categoría.
   - Método de creación de la categoría. Seleccione **Categoría que incluye archivos ejecutables de dispositivos seleccionados** como tipo de categoría.

   Ir al paso siguiente.

4. Configure los parámetros avanzados de la categoría de aplicaciones:

   - Especifique los equipos desde los cuales Kaspersky Security Center agregará archivos ejecutables a la categoría de aplicaciones. Kaspersky Security Center añadirá a la categoría de aplicación todos los archivos ejecutables de los equipos especificados presentados en la carpeta **Archivos ejecutables**.
   - Seleccione un algoritmo para el cálculo de la función hash.
   - Configure un intervalo para sincronizar los datos con el almacenamiento del Servidor de administración.
   - Configure un filtro para archivos.

5. Finalice el asistente.

Al crear una categoría que se actualiza automáticamente, puede ser conveniente subdividir los archivos en varias categorías. Por ejemplo, archivos del sistema operativo y archivos de la carpeta Program Files. Para hacerlo, puede usar un filtro en la configuración de categoría y seleccionar carpetas individuales.

2. Seleccionar el modo de Control de aplicaciones. Debe evitar la ejecución de todas las aplicaciones que no estén permitidas explícitamente. Para ello, seleccione el modo *Aplicaciones bloqueadas*.

3. Crear una regla de Control de aplicaciones. En la configuración de reglas, seleccione la categoría a la que pertenecen los archivos ejecutables del equipo de línea de base.

   Cómo configurar el Control de aplicaciones basado en un equipo de línea de base en la Consola de administración (MMC)

   1. Abra la Consola de administración de Kaspersky Security Center.
   2. En el árbol de la consola, seleccione **Directivas**.
   3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Controles de seguridad → Control de aplicaciones**.

5. Seleccione la casilla **Control de aplicaciones**.

6. En el bloque **Configuración de Control de aplicaciones**, use la lista desplegable **Modo de control** para seleccionar **Lista de rechazados**.

7. En la lista desplegable **Acción**, seleccione la acción para Control de aplicaciones:

   - **Probar reglas**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución no está permitida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, se bloquearían.

   - **Aplicar reglas**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

8. En la de reglas del Control de aplicaciones, haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir una regla de Control de aplicaciones.

9. En en la lista desplegable **Categoría**, seleccione una categoría actualizada automáticamente según el equipo de línea de base.

10. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de Control de aplicaciones.

11. Configure los parámetros avanzados de la regla de Control de aplicaciones:

    - **Denegar a los demás usuarios**. La aplicación evita el lanzamiento de aplicaciones que pertenecen a la categoría seleccionada para todos los usuarios que no están en la lista.

    - **Actualizadores de confianza**. Kaspersky Endpoint Security considera las aplicaciones incluidas en la categoría seleccionada como actualizadores de confianza autorizados a crear archivos ejecutables que, posteriormente, tendrán permitido ejecutarse.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar el Control de aplicaciones basado en un equipo de línea de base en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad → Control de aplicaciones**.

5. Active la opción **Control de aplicaciones ACTIVADO**.

6. En el bloque **Modo de funcionamiento**, seleccione **Bloquear todo excepto la lista de reglas**.

7. En el bloque **Acción**, seleccione la acción para Control de aplicaciones:

   - **Informar**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución no está permitida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, se bloquearían.

   - **Aplicar reglas**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

8. En la de reglas del Control de aplicaciones, haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir una regla de Control de aplicaciones.

9. En **Categorías/aplicaciones**, seleccione una categoría actualizada automáticamente según el equipo de línea de base.

10. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de Control de aplicaciones.

11. Configure los parámetros avanzados de la regla de Control de aplicaciones:

    - **Usuarios**. La aplicación evita el lanzamiento de aplicaciones que pertenecen a la categoría seleccionada para todos los usuarios que no están en la lista.

    - **Actualizadores de confianza**. Kaspersky Endpoint Security considera las aplicaciones incluidas en la categoría seleccionada como actualizadores de confianza autorizados a crear archivos ejecutables que, posteriormente, tendrán permitido ejecutarse.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar el Control de aplicaciones basado en un equipo de línea de base en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de aplicaciones**.

3. Active la opción **Control de aplicaciones**.

4. En el bloque **Modo de control de inicio de la aplicación**, seleccione **Lista de rechazados. Se permiten todas las aplicaciones, excepto las que figuran en la lista de reglas**.

5. En el bloque **Acción al iniciar aplicaciones bloqueadas por reglas**, seleccione la acción para Control de aplicaciones:

   - **Informar (Modo de prueba) y registrar eventos en informe**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución no está permitida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, se bloquearían.

   - **Bloquear**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

6. En la de reglas del Control de aplicaciones, haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir una regla de Control de aplicaciones.

7. En **Categoría**, seleccione una categoría actualizada automáticamente según el equipo de línea de base.

8. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de Control de aplicaciones.

9. Configure los parámetros avanzados de la regla de Control de aplicaciones:

    - **Denegar a los demás usuarios**. La aplicación evita el lanzamiento de aplicaciones que pertenecen a la categoría seleccionada para todos los usuarios que no están en la lista.

    - **Actualizadores de confianza**. Kaspersky Endpoint Security considera las aplicaciones incluidas en la categoría seleccionada como actualizadores de confianza autorizados a crear archivos ejecutables que, posteriormente, tendrán permitido ejecutarse.

10. Guarde los cambios.

Administrar reglas de Control de aplicaciones

Kaspersky Endpoint Security controla el inicio de las aplicaciones que hayan realizado los usuarios mediante el uso de reglas. Una regla de Control de aplicaciones especifica las condiciones de activación y las acciones realizadas por el Control de aplicaciones cuando se activa la regla (lo que permite o impide a los usuarios que inicien la aplicación).

Condiciones de activación de reglas

Una condición de activación de reglas tiene la siguiente correlación: "tipo de condición - criterio de condición - valor de condición". En función de las condiciones de activación de reglas, Kaspersky Endpoint Security aplicará (o no) la regla en cuestión a una aplicación.

Los siguientes tipos de condiciones se utilizan en las reglas:

- *Condiciones de inclusión*. Kaspersky Endpoint Security aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de inclusión.

- *Condiciones de exclusión*. Kaspersky Endpoint Security no aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de exclusión, pero no cumple ninguna de las condiciones de inclusión.

Las condiciones de activación de reglas se crean a partir de criterios. Los siguientes criterios se utilizan para crear reglas en Kaspersky Endpoint Security:

- Ruta de la carpeta que contiene el archivo ejecutable de la aplicación, o bien ruta al archivo ejecutable de la aplicación.

- Metadatos: nombre del archivo ejecutable de la aplicación, versión del archivo ejecutable de la aplicación, nombre de la aplicación, versión de la aplicación, proveedor de la aplicación.

- Hash del archivo ejecutable de la aplicación.

- Certificado: emisor, asunto, huella digital.

- Inclusión de la aplicación en una categoría KL.

- Ubicación del archivo ejecutable de la aplicación en una unidad extraíble.

El valor del criterio se debe especificar para cada criterio utilizado en la condición. Si los parámetros de la aplicación que se va a iniciar coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, Control de aplicaciones realiza la acción prescrita en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, Control de aplicaciones no controla el inicio de la aplicación.

Si ha seleccionado un certificado como condición de activación de la regla, debe asegurarse de que este certificado se añada al almacenamiento del sistema de confianza en el equipo y verificar la configuración de uso de almacenamiento del sistema de confianza en la aplicación.

Decisiones tomadas por el componente Control de aplicaciones cuando se activa una regla

Cuando se activa una regla, Control de aplicaciones permite que los usuarios (o los grupos de usuarios) inicien aplicaciones o bloquea el inicio de dichas aplicaciones, según lo que dicte la regla. Puede seleccionar usuarios particulares o grupos de usuarios que tienen o no permiso para iniciar aplicaciones que activan una regla.

A la regla que no especifica los usuarios que pueden iniciar aplicaciones que cumplan con la regla, se la denomina regla *de bloqueo*.

A la regla que no especifica los usuarios que no pueden iniciar aplicaciones que coincidan con la regla, se la denomina regla *de permiso*.

La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. Por ejemplo, si se ha especificado una regla de permiso de Control de aplicaciones para un grupo de usuarios y, al mismo tiempo, se ha especificado una regla de bloqueo de Control de aplicaciones para un usuario en este grupo de usuarios, se bloqueará a este usuario para que no ejecute la aplicación.

Estado operativo de una regla

Las reglas de Control de Aplicaciones pueden tener uno de estos valores de estado de funcionamiento:

- **Activado**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Desactivado**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite el inicio de aplicaciones a las que se aplican las reglas, pero registra en el informe datos sobre el inicio de esas aplicaciones.

Añadir una condición de activación para la regla de Control de aplicaciones

Para que crear reglas de Control de aplicaciones resulte más práctico, puede crear categorías de aplicaciones.

Se recomienda crear una categoría "Aplicaciones de trabajo" que abarque el conjunto estándar de las aplicaciones que se utilicen en la empresa. Si hay distintos grupos de usuarios que utilicen distintos conjuntos de aplicaciones en su trabajo, puede crearse una categoría de aplicaciones independiente para cada grupo de usuarios.

Para crear un categoría de aplicación en la Consola de administración:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione **Avanzado → Administración de aplicaciones → Categorías de aplicaciones**.
3. Haga clic en el botón **Categoría nueva** en el espacio de trabajo.

   Se iniciará el asistente de creación de categorías del usuario.
4. Siga las instrucciones del asistente de creación de la nueva categoría.

Paso 1. Selección del tipo de categoría

En este paso, seleccione uno de los siguientes tipos de categorías de aplicaciones:

- Categoría con contenido añadido manualmente. Los datos de los archivos ejecutables se añaden manualmente a la categoría Si seleccionó este tipo de categoría, en el paso *Configurar condiciones para incluir aplicaciones en categorías* y el paso *Configurar condiciones para excluir aplicaciones de categorías*, podrá definir los criterios por los cuales los archivos ejecutables se incluirán en la categoría.
- Categoría que incluye archivos ejecutables de dispositivos seleccionados. Estos archivos ejecutables se procesan automáticamente y sus métricas se añaden a la categoría Si seleccionó este tipo de la categoría, en el paso *Configuración* podrá especificar un equipo cuyos archivos ejecutables se incluirán automáticamente en la categoría.
- Categoría que incluye archivos ejecutables de una carpeta específica. Los archivos ejecutables de las aplicaciones copiadas a la carpeta especificada se procesan automáticamente y sus métricas se añaden a la categoría Si seleccionó este tipo de categoría, en el paso *Carpeta de repositorio* podrá especificar una carpeta cuyos archivos ejecutables se incluirán automáticamente en la categoría.

Al crear una categoría con contenido añadido manualmente, Kaspersky Security Center realiza un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR.

Paso 2. Introducción de un nombre de categoría de usuario

En este paso, especifique un nombre para la categoría de aplicación.

Paso 3. Configuración de las condiciones para incluir aplicaciones en una categoría

Al añadir una gran cantidad de condiciones a las reglas de Control de aplicaciones (por ejemplo, hashes de archivos), aumenta el consumo de recursos del equipo. Cuando el número total de condiciones llega a 50 000, pueden producirse problemas de rendimiento. Para optimizar el rendimiento, se recomienda revisar y reducir la cantidad de condiciones.

Este paso está disponible si selecciona el tipo de categoría **Categoría con contenido añadido manualmente**.

En este paso, en la lista desplegable **Añadir**, seleccione las condiciones para incluir aplicaciones en la categoría:

- **Desde la lista de archivos ejecutables**. Añada aplicaciones de la lista de archivos ejecutables en el dispositivo del cliente a la categoría personalizada.
- **De propiedades del archivo**. Especifique datos detallados de archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Metadatos desde archivos en carpeta**. Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de verificación de los archivos en la carpeta**. Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los hash de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Certificados para los archivos de la carpeta**. Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para añadir aplicaciones a la categoría personalizada.

  No se recomienda usar condiciones cuyas propiedades no tengan el parámetro **Huella digital del certificado** especificado.

- **Metadatos de archivos del programa de instalación MSI**. Seleccione el paquete MSI. Kaspersky Security Center indicará los metadatos de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de comprobación de los archivos del programa de instalación MSI de la aplicación**. Seleccione el paquete MSI. Kaspersky Security Center indicará los hash de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **De categoría KL**. Especifique una categoría KL como condición para añadir aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL conocida como *Aplicaciones de Office* incluye a las aplicaciones del paquete Microsoft Office y a Adobe Acrobat, entre otros.

  Puede seleccionar todas las categorías KL para generar una lista ampliada de aplicaciones de confianza.
- **Especifique la ruta a la aplicación (se admiten máscaras)**. Seleccione una carpeta en el dispositivo del cliente. Kaspersky Security Center añadirá archivos ejecutables desde esta carpeta a la categoría personalizada.
- **Seleccionar certificado del repositorio**. Seleccione los certificados que se usaron para firmar archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.

  No se recomienda usar condiciones cuyas propiedades no tengan el parámetro **Huella digital del certificado** especificado.

Puede elegir el almacén de certificados. De forma predeterminada, Control de aplicaciones aplica reglas solo para las aplicaciones firmadas con un certificado de la tienda de certificados del sistema de confianza. Esto se activa mediante la casilla de verificación **Usar verificación de firma digital estricta**.

- **Tipo de unidad**. Especifique un tipo de dispositivo de almacenamiento (todas las unidades de disco duro y extraíbles o solo las unidades extraíbles) como una condición para añadir aplicaciones a la categoría personalizada.

Paso 4. Configuración de las condiciones para excluir aplicaciones de una categoría

Este paso está disponible si selecciona el tipo de categoría **Categoría con contenido añadido manualmente**.

Las aplicaciones especificadas en este paso se excluyen de la categoría aunque estas aplicaciones se especificaran en el paso "Configuración de las condiciones incluir aplicaciones en una categoría".

En este paso, en la lista desplegable **Añadir**, seleccione las condiciones para excluir aplicaciones de la categoría:

- **Desde la lista de archivos ejecutables**. Añada aplicaciones de la lista de archivos ejecutables en el dispositivo del cliente a la categoría personalizada.
- **De propiedades del archivo**. Especifique datos detallados de archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Metadatos desde archivos en carpeta**. Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de verificación de los archivos en la carpeta**. Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los hash de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Certificados para los archivos de la carpeta**. Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para añadir aplicaciones a la categoría personalizada.
- **Metadatos de archivos del programa de instalación MSI**. Seleccione el paquete MSI. Kaspersky Security Center indicará los metadatos de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de comprobación de los archivos del programa de instalación MSI de la aplicación**. Seleccione el paquete MSI. Kaspersky Security Center indicará los hash de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **De categoría KL**. Especifique una categoría KL como condición para añadir aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL conocida como *Aplicaciones de Office* incluye a las aplicaciones del paquete Microsoft Office y a Adobe Acrobat, entre otros.

  Puede seleccionar todas las categorías KL para generar una lista ampliada de aplicaciones de confianza.

- **Especifique la ruta a la aplicación (se admiten máscaras)**. Seleccione una carpeta en el dispositivo del cliente. Kaspersky Security Center añadirá archivos ejecutables desde esta carpeta a la categoría personalizada.

- **Seleccionar certificado del repositorio**. Seleccione los certificados que se usaron para firmar archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.

- **Tipo de unidad**. Especifique un tipo de dispositivo de almacenamiento (todas las unidades de disco duro y extraíbles o solo las unidades extraíbles) como una condición para añadir aplicaciones a la categoría personalizada.

Paso 5. Configuración

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**.

En este paso, haga clic en el botón **Añadir** y especifique los equipos cuyos archivos ejecutables añadirá Kaspersky Security Center a la categoría de aplicaciones. Kaspersky Security Center añadirá a la categoría de aplicación todos los archivos ejecutables de los equipos especificados presentados en la carpeta **Archivos ejecutables**.

En este paso, también puede ajustar la configuración siguiente:

- Algoritmo para el cálculo de la función hash. Para elegir un algoritmo, debe marcar como mínimo una de las siguientes casillas:

  - **Calcular SHA256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.

  - **Calcular MD5 para archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.

- La casilla **Sincronizar datos con el repositorio del Servidor de administración**. Seleccione esta casilla si desea que Kaspersky Security Center borre periódicamente la categoría de aplicaciones y añada a ella todos los archivos ejecutables desde los equipos especificados incluidos en la carpeta **Archivos ejecutables**.

  Si la casilla de verificación **Sincronizar datos con el repositorio del Servidor de administración** está desactivada, Kaspersky Security Center no realizará ninguna modificación en una categoría de aplicación después de crearla.

Paso 6. Carpeta repositorio

Este paso está disponible si ha seleccionado el tipo de **Categoría que incluye archivos ejecutables de una carpeta específica**.

En este paso, especifique la carpeta en la cual Kaspersky Security Center buscará archivos ejecutables para añadir automáticamente aplicaciones a la categoría de aplicación.

En este paso, también puede ajustar la configuración siguiente:

- La casilla **Incluir bibliotecas de vínculo dinámico (DLL) en esta categoría**. Seleccione esta casilla de verificación si desea que las bibliotecas de enlace dinámico (archivos DLL) se incluyan en la categoría de la aplicación.

  Incluir archivos DLL en la categoría de aplicación puede reducir el rendimiento de Kaspersky Security Center.

- La casilla **Incluir datos de script en esta categoría**. Seleccione esta casilla de verificación si desea que los scripts se incluyan en la categoría de la aplicación.

  Incluir scripts en la categoría de aplicación puede reducir el rendimiento de Kaspersky Security Center.

- Algoritmo para el cálculo de la función hash. Para elegir un algoritmo, debe marcar como mínimo una de las siguientes casillas:

  - **Calcular SHA256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.

  - **Calcular MD5 para archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.

- La casilla **Forzar el análisis de la carpeta en busca de cambios**. Seleccione esta casilla si desea que Kaspersky Security Center busque periódicamente archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación.

  Si desactiva la casilla **Forzar el análisis de la carpeta en busca de cambios**, Kaspersky Security Center busca los archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación solamente si se han realizado cambios en la carpeta, añadiendo o borrando un archivo de la misma.

- El campo **Intervalo de análisis (1 a 168 horas)**. En este campo puede especificar el intervalo de tiempo (en horas) después del cual Kaspersky Security Center buscará archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación.

  El campo está disponible si la casilla **Forzar el análisis de la carpeta en busca de cambios** está seleccionada.

Paso 7. Creación de una categoría personalizada

Finalice el asistente.

Para añadir una nueva condición de activación para una regla de Control de aplicaciones en la interfaz de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de aplicaciones**.

3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Se desplegará la lista de reglas de Control de aplicaciones.

4. Seleccione la regla para la que desea configurar una condición de activación.

   Se abre la configuración de la regla de Control de aplicaciones.

5. Seleccione la pestaña **Condiciones: N** o **Exclusiones: N** y haga clic en el botón **Añadir**.

6. Seleccione las condiciones de activación para la regla de Control de aplicaciones:

   - **Condiciones de propiedades de las aplicaciones iniciadas**. En la lista de aplicaciones en ejecución, puede seleccionar las aplicaciones a las que se aplicará la regla de Control de aplicaciones. Kaspersky Endpoint Security también enumera las aplicaciones que se estaban ejecutando anteriormente en el equipo. Debe elegir el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta al archivo o carpeta**.

   - **Condiciones "Categoría KL"**. Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL conocida como "Aplicaciones de Office" incluye a las aplicaciones del paquete Microsoft Office y a Adobe® Acrobat®, entre otros.

   - **Condición personalizada**. Puede elegir el archivo de la aplicación y elegir una de las condiciones de activación de la regla: **Hash del archivo**, **Certificado**, **Metadatos** o **Ruta al archivo o carpeta**.

   - **Condición por unidad de archivos (unidad extraíble)**. La regla de Control de aplicaciones se aplica solo a los archivos que se ejecutan en una unidad extraíble.

   - **Condiciones de las propiedades de los archivos en la carpeta especificada**. La regla de Control de aplicaciones se aplica solo a los archivos en la carpeta especificada. También puede incluir o excluir archivos de subcarpetas. Debe elegir el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta al archivo o carpeta**.

7. Guarde los cambios.

Al añadir condiciones, tenga en cuenta las siguientes consideraciones especiales para el Control de aplicaciones:

- Kaspersky Endpoint Security admite los caracteres `*` y `?` para introducir una máscara en los metadatos: **Nombre de archivo**, **Nombre de la aplicación**, **Proveedor**.

- Kaspersky Endpoint Security no admite el hash de un archivo MD5 y no controla el inicio de aplicaciones basado en un hash de MD5. Se utiliza un hash SHA256 como condición de activación de reglas.

- No se recomienda usar solo los criterios de **Emisor** y **Sujeto del certificado** como condiciones de activación de la regla. El uso de estos criterios no es fiable.

- Si está usando enlaces simbólicos en el campo **Ruta al archivo o carpeta**, le aconsejamos resolver los enlaces simbólicos para que la regla de Control de Aplicaciones funcione correctamente. Para ello, haga clic en el botón **Resolver vínculo simbólico**.

Añadir archivos ejecutables desde la carpeta Archivos ejecutables a la categoría de aplicación

En la carpeta **Archivos ejecutables** se muestra la lista de archivos ejecutables detectados en los equipos. Kaspersky Endpoint Security genera una lista de archivos ejecutables después de ejecutar la Tarea de inventario.

Para añadir archivos ejecutables desde la carpeta Archivos ejecutables a la categoría de aplicación:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione **Avanzado → Administración de aplicaciones → Archivos ejecutables**.
3. En el espacio de trabajo, seleccione los archivos ejecutables que desee añadir a la categoría de aplicación.
4. Haga clic con el botón derecho para abrir el menú contextual de los archivos ejecutables seleccionados y seleccione **Agregar a categoría**.
5. En la ventana que se abre, haga lo siguiente:
   - En la parte superior de la ventana, elija una de las opciones siguientes:
     - **Añadir a una nueva categoría de aplicaciones**. Elija esta opción si desea crear una nueva categoría de aplicación y añadirle archivos ejecutables.
     - **Añadir a una categoría de aplicaciones existente**. Elija esta opción si desea escoger una categoría de aplicación existente y añadirle archivos ejecutables.
   - En el bloque **Tipo de regla**, elija una de las opciones siguientes:
     - **Reglas para añadir inclusiones**. Seleccione esta opción si desea crear una condición que añada archivos ejecutables a la categoría de aplicación.
     - **Reglas para añadir exclusiones**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de aplicación.
   - En el bloque **Parámetro utilizado como condición**, seleccione una de las opciones siguientes:
     - **Detalles del certificado (o hashes SHA256 para archivos sin certificado)**.
     - **Detalles del certificado (se omitirán los archivos sin certificado)**.
     - **Solo SHA256 (los archivos sin hash se omitirán)**.
     - **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**.
6. Guarde los cambios.

Añadir archivos ejecutables relacionados con eventos a la categoría de aplicación

Para añadir archivos ejecutables relacionados con los eventos de Control de aplicaciones a la categoría de la aplicación:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.

3. Elija una selección de eventos relacionados con el funcionamiento del componente Control de aplicaciones (Ver eventos resultantes del funcionamiento del componente Control de aplicaciones, Ver eventos resultantes de la comprobación del funcionamiento del componente Control de aplicaciones) en la lista desplegable **Selecciones de eventos**.

4. Haga clic en el botón **Ejecutar selección**.

5. Seleccione los eventos cuyos archivos ejecutables asociados desee añadir a la categoría de aplicación.

6. Haga clic con el botón derecho para abrir el menú contextual de los eventos seleccionados y seleccione **Agregar a categoría**.

7. En la ventana que se abre, configure los parámetros de la categoría de la aplicación:

   - En la parte superior de la ventana, elija una de las opciones siguientes:

     - **Añadir a una nueva categoría de aplicaciones**. Elija esta opción si desea crear una nueva categoría de aplicación y añadirle archivos ejecutables.

     - **Añadir a una categoría de aplicaciones existente**. Elija esta opción si desea escoger una categoría de aplicación existente y añadirle archivos ejecutables.

   - En el bloque **Tipo de regla**, elija una de las opciones siguientes:

     - **Reglas para añadir inclusiones**. Seleccione esta opción si desea crear una condición que añada archivos ejecutables a la categoría de aplicación.

     - **Reglas para añadir exclusiones**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de aplicación.

   - En el bloque **Parámetro utilizado como condición**, seleccione una de las opciones siguientes:

     - **Detalles del certificado (o hashes SHA-256 para archivos sin certificado)**.

     - **Detalles del certificado (se omitirán los archivos sin certificado)**.

     - **Solo SHA-256 (se omitirán los archivos sin hash)**.

     - **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Guarde los cambios.

Adición de una regla de Control de aplicaciones

Para añadir una regla de Control de aplicaciones con Kaspersky Security Center:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de aplicaciones.

4. Haga clic en **Añadir**.

   Se abre la ventana **Regla de Control de aplicaciones**.

5. Realice una de las siguientes acciones:

   - Si desea crear una nueva categoría:

     a. Haga clic en **Crear una categoría**.

        Se iniciará el asistente de creación de categorías del usuario.

     b. Siga las instrucciones del asistente de creación de la nueva categoría.

     c. En la lista desplegable **Categoría**, seleccione la categoría de aplicaciones que acaba de crear.

   - Si desea modificar una categoría existente:

     a. En la lista desplegable **Categoría**, seleccione la categoría de aplicaciones existente que desea modificar.

     b. Haga clic en **Propiedades**.

     c. Modifique la configuración de la categoría de aplicaciones seleccionada.

     d. Guarde los cambios.

     e. En la lista desplegable **Categoría**, seleccione la categoría de aplicación en función de la cual desea crear una regla.

6. En la tabla **Usuarios y sus derechos**, haga clic en el botón **Añadir**.

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

7. En la tabla **Usuarios y sus derechos**, haga lo siguiente.

   - Si desea permitir que los usuarios o los grupos de usuarios inicien aplicaciones que pertenecen a la categoría seleccionada, seleccione la casilla **Permitir** situada junto a esos usuarios o grupos.

   - Si quiere prohibir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione la casilla **Bloquear** en las filas correspondientes.

8. Seleccione la casilla **Denegar a los demás usuarios** si quiere que todos los usuarios que no aparecen en la columna **Usuario o grupo** y que no forman parte del grupo de usuarios especificados en la columna **Usuario o grupo** estén bloqueados para iniciar aplicaciones que pertenezcan a la categoría seleccionada.

9. Si desea que Kaspersky Endpoint Security considere las aplicaciones incluidas en la categoría de aplicación seleccionada como actualizadores de confianza autorizados a crear archivos ejecutables utilizables posteriormente, marque la casilla **Actualizadores de confianza**.

   Cuando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.

10. Guarde los cambios.

Para añadir una regla de Control de aplicaciones:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Se desplegará la lista de reglas de Control de aplicaciones.
4. Haga clic en **Añadir**.

   Se abre la ventana de configuración de las reglas de Control de aplicaciones.
5. En la pestaña **Configuración general**, defina la configuración principal de la regla:

   a. En el campo **Nombre de la regla**, introduzca el nombre de la regla.

   b. En el campo **Descripción**, introduzca una descripción de la regla.

   c. En la tabla **Usuarios y sus derechos**, haga clic en el botón **Añadir**.

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.

   La regla se aplica a todos los usuarios de forma predeterminada.

   > Si no hay ningún usuario especificado en la tabla, la regla no se puede guardar.

   d. En la tabla **Usuarios y sus derechos**, use el interruptor para definir el derecho de los usuarios a iniciar aplicaciones.

   e. Seleccione la casilla **Denegar a los demás usuarios** si quiere que la aplicación impida que se ejecuten las aplicaciones que cumplen las condiciones de activación de las reglas para todos los usuarios que no figuran en la tabla **Usuarios y sus derechos** y que no son miembros de los grupos de usuarios que figuran en la tabla **Usuarios y sus derechos**.

   > Si no selecciona la casilla **Denegar a los demás usuarios**, Kaspersky Endpoint Security no controlará la ejecución de aplicaciones por parte de usuarios que no aparezcan en la tabla **Usuarios y sus derechos** y que no formen parte de los grupos de usuarios especificados en la tabla **Usuarios y sus derechos**.

   f. Seleccione la casilla de verificación **Actualizadores de confianza** si desea que Kaspersky Endpoint Security considere las aplicaciones que cumplen las condiciones de activación de reglas como actualizadores de confianza. Los *Actualizadores de confianza* son aplicaciones que pueden crear otros archivos ejecutables que podrán ejecutarse posteriormente.

   Si una aplicación activa varias reglas, Kaspersky Endpoint Security establece el indicador *Actualizadores de confianza* si se cumplen las siguientes condiciones:

   - Todas las reglas permiten que la aplicación se ejecute.
   - Al menos una regla tiene la casilla de verificación **Actualizadores de confianza** seleccionada.
6. En la pestaña **Condiciones: N**, cree o edite la lista de condiciones de inclusión para activar la regla.

7. En la pestaña **Exclusiones: N**, cree o edite la lista de condiciones de exclusión para activar la regla.

   Cuando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.

8. Guarde los cambios.

Cambiar el estado de una regla de Control de aplicaciones mediante Kaspersky Security Center

Para cambiar el estado de una regla de Control de aplicaciones en la Consola de administración:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de aplicaciones.

4. En la columna **Estado**, haga clic con el botón izquierdo del ratón para que se muestre el menú contextual y realice una de las siguientes acciones:

   - **Activa**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
   - **Inactiva**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
   - **Prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplican la regla, pero registra datos sobre el inicio de esas aplicaciones en el informe.

5. Guarde los cambios.

Para cambiar el estado de una regla de Control de aplicaciones en la interfaz de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Se desplegará la lista de reglas de Control de aplicaciones.

4. En la columna **Estado**, abra el menú contextual y seleccione una de las siguientes:

   - **Activado**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
   - **Desactivado**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
   - **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplica esta regla, pero registra en el informe datos sobre el inicio de esas aplicaciones.

5. Guarde los cambios.

Exportación e importación de reglas de Control de aplicaciones

Puede exportar la lista de reglas de Control de aplicaciones a un archivo XML. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de Control de aplicaciones o para migrar la lista a un servidor diferente.

Al exportar e importar reglas de Control de aplicaciones, tenga en cuenta las siguientes consideraciones especiales:

- Kaspersky Endpoint Security exporta la lista de reglas solo para el modo Control de aplicaciones activo. En otras palabras, si Control de aplicaciones está funcionando en modo de lista de rechazados, Kaspersky Endpoint Security exportará las reglas solo para este modo. Para exportar la lista de reglas para modo de lista de admitidos, debe cambiar de modo y volver a ejecutar la operación de exportación.
- Kaspersky Endpoint Security usa categorías de aplicaciones para que funcionen las reglas de Control de aplicaciones. Al migrar la lista de reglas de Control de aplicaciones a otro servidor, también debe migrar la lista de categorías de aplicaciones. Para obtener más detalles sobre la exportación o la importación de categorías de aplicaciones, consulte la Ayuda de Kaspersky Security Center.

Cómo exportar e importar una lista de reglas de Control de aplicaciones en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de aplicaciones**.
4. Para exportar la lista de reglas de Control de aplicaciones:
   a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.

   b. Haga clic en el enlace **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.

5. Para importar una lista de reglas de Control de aplicaciones:

    a. Haga clic en el enlace **Importar**.

    En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.

    b. Abra el archivo.

    Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

6. Guarde los cambios.

Cómo exportar e importar una lista de reglas de Control de aplicaciones en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

    Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control de aplicaciones**.
5. En **Modo de funcionamiento**, seleccione una lista de reglas: Lista de aplicaciones admitidas o lista de aplicaciones rechazadas.
6. Para exportar la lista de reglas:

    a. Seleccione las reglas que quiera exportar.

    b. Haga clic en el botón → **Exportar**.

    Kaspersky Endpoint Security exporta la lista de reglas a un archivo JSON en la carpeta de descargas predeterminada.

7. Para importar la lista de reglas:

    a. Haga clic en el botón → **Importar**.

    En la ventana que se abre, seleccione el archivo JSON del que desea importar la lista de reglas.

    b. Abra el archivo.

    Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

8. Guarde los cambios.

Ver eventos resultantes del funcionamiento del componente Control de aplicaciones

Para ver los eventos resultantes del funcionamiento del componente Control de aplicaciones recibido por Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.
3. Haga clic en el botón **Crear una selección**.
4. En la ventana que se abre, vaya a la sección **Eventos**.
5. Haga clic en el botón **Borrar todo**.
6. En la tabla **Eventos**, seleccione la casilla **Inicio de la aplicación prohibido**.
7. Guarde los cambios.
8. En la lista desplegable **Selecciones de eventos**, seleccione la selección creada.
9. Haga clic en el botón **Ejecutar selección**.

Ver un informe sobre aplicaciones bloqueadas

Para ver el informe sobre aplicaciones bloqueadas:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en **Nueva plantilla de informe**.

   Se inicia el Asistente de nueva plantilla de informe.
4. Siga los pasos del Asistente de plantillas de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione **Otro → Informe sobre aplicaciones prohibidas**.

   Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.
5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

Probar reglas de Control de aplicaciones

Para asegurarse de que las reglas de Control de aplicaciones no bloquean las aplicaciones requeridas para el trabajo, se recomienda activar la comprobación de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear reglas nuevas. Cuando esté activado el modo de prueba de las reglas de Control de aplicaciones, Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio esté prohibido por el Control de aplicaciones, pero sí enviará notificaciones sobre su inicio al Servidor de administración.

Un análisis del funcionamiento de las reglas de Control de aplicaciones requiere la revisión de los eventos de Control de aplicaciones resultantes que se notifican a Kaspersky Security Center. Si el modo de prueba no genera eventos que implican el inicio bloqueado para todas las aplicaciones requeridas para el trabajo del usuario del equipo, esto significa que se crearon las reglas correctas. De lo contrario, se le recomienda actualizar la configuración de las reglas que ha creado, crear reglas adicionales o eliminar las reglas existentes.

De forma predeterminada, Kaspersky Endpoint Security permite el inicio de todas las aplicaciones, excepto las aplicaciones prohibidas por las reglas.

Activación y desactivación de la prueba de reglas de Control de aplicaciones

Para activar o desactivar la comprobación de las reglas de Control de aplicaciones en Kaspersky Security Center:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de aplicaciones.
4. En la lista desplegable **Modo de control**, seleccione uno de los siguientes elementos:

   - **Lista de rechazados**. Si se selecciona esta opción, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto las prohibidas por las condiciones de las reglas de bloqueo de Control de aplicaciones.
   - **Lista de permitidos**. Si se selecciona esta opción, Control de aplicaciones impide que los usuarios inicien las aplicaciones que no cumplen con las condiciones de las reglas de autorización de Control de aplicaciones.
5. Realice una de las siguientes acciones:

   - Si desea activar la comprobación para las Reglas de control de aplicaciones, seleccione la opción **Probar reglas** en la lista desplegable **Acción**.
   - Si desea activar el Control de aplicaciones para administrar el inicio de aplicaciones en los equipos de los usuarios, seleccione **Aplicar reglas** en la lista desplegable.
6. Guarde los cambios.

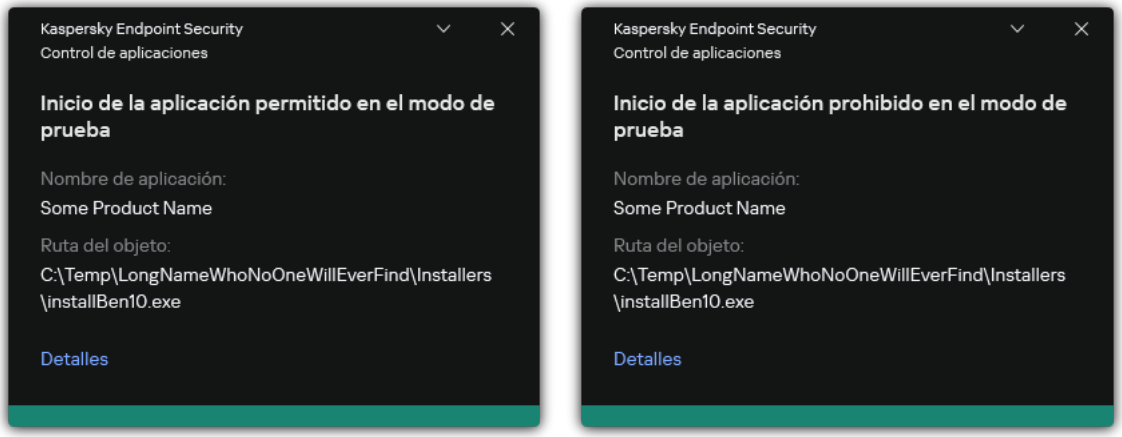
Para activar la comprobación de las reglas de Control de aplicaciones o para seleccionar una acción de bloqueo para el Control de aplicaciones:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Se desplegará la lista de reglas de Control de aplicaciones.
4. En la columna **Estado**, seleccione **Modo de prueba**.

   Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplica esta regla, pero registra en el informe datos sobre el inicio de esas aplicaciones.
5. Guarde los cambios.

Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio esté prohibido por el componente Control de aplicaciones, pero enviará notificaciones sobre su inicio al Servidor de administración. También puede configurar la visualización de notificaciones sobre la prueba de reglas en el equipo del usuario (ver la figura a continuación).



Notificaciones de Control de aplicaciones en modo de prueba

Ver un informe sobre las aplicaciones bloqueadas en el modo de prueba

Para ver el informe sobre las aplicaciones bloqueadas en el modo de prueba:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en **Nueva plantilla de informe**.

   Se inicia el Asistente de nueva plantilla de informe.

4. Siga los pasos del Asistente de plantillas de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione **Otro → Informe sobre aplicaciones prohibidas en modo de prueba**.

   Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.

5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

Ver eventos resultantes de la comprobación del funcionamiento del componente Control de aplicaciones

Para ver eventos de la comprobación del Control de aplicaciones recibidos por Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.
3. Haga clic en el botón **Crear una selección**.
4. En la ventana que se abre, vaya a la sección **Eventos**.
5. Haga clic en el botón **Borrar todo**.
6. En la tabla **Eventos**, seleccione las casillas **Inicio de la aplicación prohibido en modo de prueba** e **Inicio de la aplicación permitido en modo de prueba**.
7. Guarde los cambios.
8. En la lista desplegable **Selecciones de eventos**, seleccione la selección creada.
9. Haga clic en el botón **Ejecutar selección**.

Supervisión de la actividad de aplicaciones

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

Supervisión de la Actividad de Aplicaciones es una herramienta diseñada para ver información sobre la actividad de las aplicaciones en el equipo de un usuario en tiempo real.

El uso de Supervisión de la actividad de aplicaciones requiere la instalación de los componentes Control de aplicaciones y Prevención de intrusiones en el host. Si estos componentes no están instalados, la sección Supervisión de la actividad de aplicaciones en la ventana principal de la aplicación está oculta.

Para iniciar Supervisión de la Actividad de Aplicaciones:

En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Supervisión de la Actividad de Aplicaciones**.

En esta ventana, la información sobre la actividad de las aplicaciones se presenta en tres pestañas:

- La pestaña **Todas las aplicaciones** muestra información sobre todas las aplicaciones instaladas en el equipo.
- La pestaña **En ejecución** muestra información sobre el consumo de recursos del equipo por aplicación en tiempo real. En esta pestaña, además puede configurar los permisos de una aplicación individual.
- La pestaña **Ejecutar en el inicio** muestra la lista de aplicaciones que se ejecutan cuando se inicia el sistema operativo.

Si desea ocultar la información de la actividad de la aplicación en el equipo de un usuario, puede restringir el acceso del usuario a la herramienta Supervisión de la actividad de aplicaciones.

Cómo ocultar la Supervisión de la actividad de aplicaciones en la interfaz de la aplicación mediante la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Interfaz**.
4. Utilice la casilla de verificación **Ocultar la sección del monitor de actividad de la aplicación** para otorgar o revocar el acceso a la herramienta.
5. Guarde los cambios.

Cómo ocultar la Supervisión de la actividad de aplicaciones en la interfaz de la aplicación mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Interacción del usuario**.
5. Utilice la casilla de verificación **Ocultar la sección del monitor de actividad de la aplicación** para otorgar o revocar el acceso a la herramienta.
6. Guarde los cambios.

Reglas para crear máscaras de nombre para archivos o carpetas

Una *máscara de un archivo o nombre de carpeta* es una representación del nombre de una carpeta o nombre y extensión de un archivo con caracteres comunes.

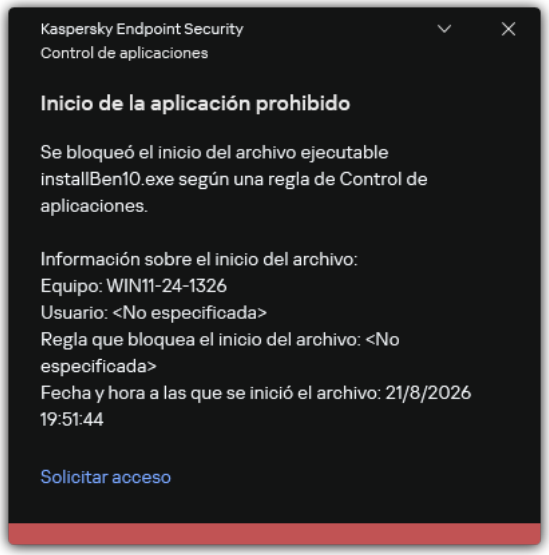
Puede usar los siguientes caracteres comunes para crear una máscara de nombre de archivo o carpeta:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío). Por ejemplo, la máscara `C:\*.txt` incluirá todas las rutas a archivos con la extensión `txt` ubicadas en carpetas y subcarpetas de la unidad (C:).

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Edición de plantillas de mensajes de Control de aplicaciones

Cuando un usuario intenta iniciar una aplicación que se encuentra bloqueada por una regla de Control de aplicaciones, Kaspersky Endpoint Security muestra un mensaje que indica que la aplicación está bloqueada desde el inicio. Los expertos de Kaspersky proporcionan al usuario una plantilla de mensaje que describe los motivos por los que se bloqueó la aplicación (consulte la figura a continuación). Se proporcionan variables especiales para administrar la plantilla de mensaje (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensaje para diferentes ordenadores. Al generar un mensaje, Kaspersky Endpoint Security recupera el valor de la variable de la configuración del sistema operativo y lo inserta en el mensaje correspondiente al equipo, usuario y evento específicos.



Notificación de Control de aplicaciones

Si el usuario cree que el inicio de la aplicación se bloqueó por error, puede utilizar el enlace del texto del mensaje para enviar un mensaje al administrador de la red de área local. Para hacerlo, el usuario debe hacer clic en el botón **Solicitar acceso** y enviar un mensaje al administrador describiendo la situación. También puede preparar una plantilla del mensaje para el administrador, añadiéndole datos que pueden informar de su decisión de permitir o bloquear el acceso a la aplicación. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del inicio de la aplicación**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

Cómo editar la plantilla de mensaje de Control de aplicaciones en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de aplicaciones**.
4. En el bloque **Configuración de la plantilla de mensajes**, haga clic en el botón **Plantillas**.
5. Esto abre una ventana; dentro de esa ventana, configure las plantillas de Control de aplicaciones:

   - **Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.

     No puede configurar plantillas de mensajes para Control de aplicaciones en el modo de prueba. Control de aplicaciones en modo de prueba muestra notificaciones preestablecidas.

   - **Mensaje al administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Predeterminado**.
6. Guarde los cambios.

Cómo cambiar la plantilla del mensaje de Control de aplicaciones en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad → Control de aplicaciones**.
5. En el bloque **Plantillas de mensajes**, haga clic en vínculo **Mensajes sobre el bloqueo de inicio de la aplicación** y configure plantillas para mensajes de Control de aplicaciones:

   - **Mensaje al usuario**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.

     No puede configurar plantillas de mensajes para Control de aplicaciones en el modo de prueba. Control de aplicaciones en modo de prueba muestra notificaciones preestablecidas.

   - **Mensaje al administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Restablecer valores predeterminados**.
6. Guarde los cambios.

Cómo cambiar la plantilla del mensaje de Control de aplicaciones en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. En el bloque **Plantillas de mensajes sobre el bloque de aplicaciones**, configure plantillas para mensajes de Control de aplicaciones:
   - **Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.

     No puede configurar plantillas de mensajes para Control de aplicaciones en el modo de prueba. Control de aplicaciones en modo de prueba muestra notificaciones preestablecidas.
   - **Mensaje para el administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Añadir variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Restablecer**.
4. Guarde los cambios.

Variables en las plantillas de mensajes de Control de aplicaciones

Puede utilizar las siguientes variables en las plantillas de mensajes de usuario o las plantillas de mensajes de administrador:

- **Nombre de la regla activada** - `%RULE%`.

  Nombre de la regla que bloqueó la ejecución de un archivo.
- **Fecha actual** - `%DATE%`.

  Fecha en que se bloqueó la ejecución del archivo en formato DD.MM.AAAA.
- **Hora actual** - `%TIME%`.

  Hora en la que se bloqueó la ejecución del archivo en formato HH: MM.
- **Nombre de usuario** - `%USER_NAME%`.

  Nombre de la cuenta de usuario actual en el equipo en el que se bloqueó la ejecución del archivo, en formato `<device name>\<user alias>` (por ejemplo, `DESKTOP-123\John.Smith`).
- **Nombre de equipo** - `%COMPUTER_NAME%`.

  Nombre del equipo en el que se bloqueó la ejecución del archivo.
- **Nombre del archivo ejecutable** - `%FILE_NAME%`.

  Nombre del archivo ejecutable de la aplicación bloqueada.
- **Categoría KL del archivo ejecutable** - `%KL_CAT%`.

  Categoría KL a la que pertenece la aplicación bloqueada (por ejemplo, *Navegadores* u otra categoría).

- **Ruta al archivo ejecutable** - `%FILE_PATH%`.

  Ruta completa al archivo ejecutable de la aplicación bloqueada.

- **Versión del archivo ejecutable** - `%FILE_VERSION%`.

  Versión del archivo ejecutable de la aplicación bloqueada.

- **Nombre original del archivo ejecutable** - `%ORIGINAL_FILE_NAME%`.

  Nombre original del archivo ejecutable de la aplicación bloqueada. El nombre del archivo se especifica en las propiedades del archivo ejecutable de la aplicación.

- **Proveedor** - `%FILE_PUBLISHER%`.

  Proveedor de la aplicación bloqueada.

- **Nombre de aplicación** - `%FILE_PRODUCT_NAME%`.

  Nombre de la aplicación de bloqueada.

- **Versión de la aplicación** - `%PRODUCT_VERSION%`.

  Versión de la aplicación bloqueada.

- **Hash del archivo ejecutable** - `%FILE_HASH%`.

  Hash del archivo ejecutable de la aplicación bloqueada.

- **Emisor del certificado** - `%CERT_ISSUER%`.

  Emisor del certificado con el que está firmado el archivo ejecutable.

- **Sujeto del certificado** - `%CERT_SUBJECT%`.

  Asunto del certificado con el que está firmado el archivo ejecutable.

- **Huella digital del certificado** - `%CERT_THUMBPRINT%`.

  Impresión digital del certificado con el que está firmado el archivo ejecutable.

Prácticas recomendadas para realizar un inventario de archivos ejecutables

La tarea *Inventory* obtiene información sobre archivos ejecutables (por ejemplo, EXE, BAT y CMD), módulos DLL y scripts (PowerShell, JS, entre otros). Esta información es necesaria para configurar las categorías de Control de aplicaciones y los permisos de aplicaciones para el componente Prevención de intrusiones en el host. La tarea *Inventory* debe ejecutarse periódicamente para mantener actualizada la información. La tarea *Inventory*, al igual que la tarea *Análisis antimalware*, consume muchos recursos. Por lo tanto, recomendamos configurar la tarea para que se ejecute por la noche o durante los fines de semana.

Pasos para realizar un inventario de archivos ejecutables

1. Seleccione el grupo de equipos de referencia en los que esté instalado el conjunto de software habitual. Recomendamos reducir al mínimo el número de equipos utilizados para realizar el inventario de archivos ejecutables. Cuantas menos tareas *Inventory* haya, menor será la carga en el Servidor de Administración de Kaspersky Security Center.

2. Mueva los equipos de referencia a un grupo de administración independiente en la consola de Kaspersky Security Center. Puede asignar al grupo, por ejemplo, el nombre *Equipos de referencia*.

3. Cree una tarea *Inventory* para el grupo de administración *Equipos de referencia*. Recomendamos mantener la configuración predeterminada de la tarea.

Ejemplo de inventario de archivos ejecutables en una organización

Por ejemplo, su organización tiene 100 equipos con Windows 11 25H2. Todos los equipos tienen la misma versión y localización del sistema operativo. El conjunto de actualizaciones instaladas en los equipos también es el mismo.

En una organización de este tipo, no es necesario ejecutar la tarea *Inventory* en todos los equipos. La mayoría de los archivos ejecutables de estos equipos son idénticos. Basta con crear una tarea para un equipo de referencia. Puede crear tareas *Inventory* adicionales para los equipos cuya configuración difiera de la del equipo de referencia.

Mejores prácticas para implementar una lista de aplicaciones permitidas

Al planear la implementación de la lista de aplicaciones permitidas, se recomienda realizar las acciones siguientes:

1. Forme los siguientes tipos de grupos:

   - Grupos de usuarios. Los grupos de usuarios para los que tiene que permitir el uso de varios conjuntos de aplicaciones.

   - Grupos de administración. Uno o varios grupos de equipos a los que Kaspersky Security Center aplicará la lista de aplicaciones permitidas. Es necesario crear varios grupos de equipos si se utiliza una configuración de lista de admitidos distinta para esos grupos.

2. Crear una lista de aplicaciones que se debe permitir comenzar.

   Antes de crear una lista, se le recomienda hacer lo siguiente:

   a. Ejecute la tarea de inventario.

      La información sobre la creación, reconfiguración e inicio de una tarea de inventario está disponible en la sección Gestión de tareas.

   b. Vea la lista de archivos ejecutables.

Configuración del modo de lista de admitidos para aplicaciones

Al configurar el modo de la lista de admitidos, se recomienda realizar las acciones siguientes:

1. Crear categorías de aplicaciones que contengan las aplicaciones cuya ejecución se debe permitir.

   Puede seleccionar uno de los siguientes métodos para crear categorías de aplicaciones:

   - **Categoría con contenido añadido manualmente**. Puede añadir contenido manualmente a esta categoría usando las condiciones siguientes:
     - Metadatos de archivo. Kaspersky Security Center añade todos los archivos ejecutables con los metadatos especificados a la categoría de aplicación.
     - Código hash del archivo. Kaspersky Security Center añade todos los archivos ejecutables con el hash especificado a la categoría de aplicación.

       El uso de esta condición excluye la capacidad de instalar automáticamente actualizaciones porque las versiones diferentes de los archivos tendrán un hash diferente.

     - Certificado de archivo. Kaspersky Security Center añade todos los archivos ejecutables firmados con el certificado especificado a la categoría de aplicación.
     - Categoría KL. Kaspersky Security Center añade todos los archivos que están en la categoría KL especificada a la categoría de aplicación.
     - Carpeta de la aplicación. Kaspersky Security Center añade todos los archivos ejecutables de esta carpeta a la categoría de aplicación.

       El uso de la condición **Carpeta de la aplicación** puede no ser seguro porque se permitirá la ejecución de cualquier aplicación de la carpeta especificada. Se recomienda aplicar reglas que usen las categorías de aplicaciones con la condición de la **Carpeta de la aplicación** solo para aquellos usuarios que requieran la autorización de la instalación automática de actualizaciones.

   - **Categoría que incluye archivos ejecutables de una carpeta específica**. Puede especificar una carpeta desde la cual los archivos ejecutables se asignarán automáticamente a la categoría de aplicación creada.
   - **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**. Puede especificar un equipo para el que todos los archivos ejecutables se asignarán automáticamente a la categoría de aplicación creada.

     Al usar este método de creación de categorías de aplicaciones, Kaspersky Security Center recibe información sobre las aplicaciones en el equipo desde la carpeta **Archivos ejecutables**.

2. Seleccione el modo de lista de admitidos para el componente Control de aplicaciones.

3. Cree Reglas de control de aplicaciones usando las categorías de aplicaciones creadas.

   La regla **Golden Image** y la regla **Actualizadores de confianza** se definen inicialmente para el modo Lista de admitidos. Estas reglas de Control de aplicaciones corresponden a las categorías KL. La categoría KL *Golden Image* incluye programas que garantizan el funcionamiento normal del sistema operativo. La categoría KL *Actualizadores de confianza* incluye programas de actualización de los proveedores de software más prestigiosos. No puede eliminar estas reglas. La configuración de estas reglas no se puede editar. De forma predeterminada, la regla **Golden Image** está activada y la regla **Actualizadores de confianza** está desactivada. Todos los usuarios tienen permiso para iniciar aplicaciones que cumplan las condiciones de activación de estas reglas.

4. Determine las aplicaciones para las que hay que permitir la instalación automática de actualizaciones.

   Puede permitir la instalación automática de actualizaciones de una de estas formas:

   - Especifique una lista ampliada de aplicaciones permitidas autorizando el inicio de todas las aplicaciones que pertenecen a una categoría KL.
   - Especifique una lista ampliada de aplicaciones permitidas autorizando el inicio de todas las aplicaciones que están firmadas con certificados.

     Para permitir el inicio de todas las aplicaciones firmadas con certificados, puede crear una categoría con una condición basada en el certificado que solo use el parámetro **Sujeto** con el valor `*`.
   - Para la regla de Control de aplicaciones, seleccione el parámetro **Actualizadores de confianza**. Cuando esta casilla está seleccionada, Kaspersky Endpoint Security considera que las aplicaciones incluidas en la regla son actualizadores de confianza. Mientras no exista una regla de bloqueo que determine lo contrario, Kaspersky Endpoint Security permitirá que se inicien las aplicaciones que hayan sido instaladas o actualizadas por las aplicaciones de la regla.

     Cuando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.
   - Cree una carpeta y coloque en ella los archivos ejecutables de las aplicaciones que podrán actualizarse automáticamente. A continuación, cree una categoría de aplicaciones con la condición **Carpeta de la aplicación** y especifique la ruta de acceso a la carpeta. Por último, cree una regla de permiso y seleccione esta nueva categoría.

     El uso de la condición **Carpeta de la aplicación** puede no ser seguro porque se permitirá la ejecución de cualquier aplicación de la carpeta especificada. Se recomienda aplicar reglas que usen las categorías de aplicaciones con la condición de la **Carpeta de la aplicación** solo para aquellos usuarios que requieran la autorización de la instalación automática de actualizaciones.

Prueba del modo de lista de admitidos

Para asegurarse de que las reglas de Control de aplicaciones no bloquean las aplicaciones requeridas para el trabajo, se recomienda activar la comprobación de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear reglas nuevas. Cuando esté activado el modo de prueba, Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio esté prohibido por las reglas de Control de aplicaciones, pero sí enviará notificaciones sobre su inicio al Servidor de administración.

Al probar el modo de lista de admitidos, se recomienda realizar las acciones siguientes:

1. Determine el período de pruebas (puede ser desde varios días hasta dos meses).
2. Active la comprobación de las reglas de Control de aplicaciones.
3. Examinar, a fin de analizar los resultados de la prueba, los eventos que resulten de probar el funcionamiento de Control de aplicaciones y los informes sobre las aplicaciones bloqueadas en el modo de prueba.
4. Según los resultados de análisis, haga cambios en la configuración del modo de lista de admitidos.

   En particular, en función de los resultados de la prueba, puede añadir archivos ejecutables relacionados con eventos a una categoría de aplicación.

Soporte para el modo de lista de admitidos

Después de seleccionar una acción de bloqueo para el Control de aplicaciones, se recomienda continuar admitiendo el modo de lista de admitidos con las acciones siguientes:

- Examine los eventos generados por el funcionamiento del Control de aplicaciones y los informes sobre ejecuciones bloqueadas para analizar la eficacia del Control de aplicaciones.
- Analice las solicitudes de los usuarios para acceder a las aplicaciones.
- Analice los archivos ejecutables desconocidos comprobando su reputación en Kaspersky Security Network.
- Antes de instalar actualizaciones para el sistema operativo o para el software, instale esas actualizaciones en un grupo de prueba de equipos para verificar cómo serán procesadas por las reglas de Control de aplicaciones.
- Añada las aplicaciones necesarias a las categorías utilizadas en las reglas de Control de aplicaciones.

Supervisión de puertos de red

Durante el funcionamiento de Kaspersky Endpoint Security, los componentes Control web, Protección frente a amenazas en el correo, Protección frente a amenazas web, Detección de comportamiento y Prevención de exploits supervisan los flujos de datos que se transmiten mediante protocolos específicos y que pasan a través de puertos TCP y UDP concretos que se encuentran abiertos en el equipo del usuario. Por ejemplo, el componente Protección frente a amenazas en el correo analiza la información que se transmite mediante SMTP, mientras que el componente Protección frente a amenazas web analiza la información que se transmite mediante HTTP y FTP.

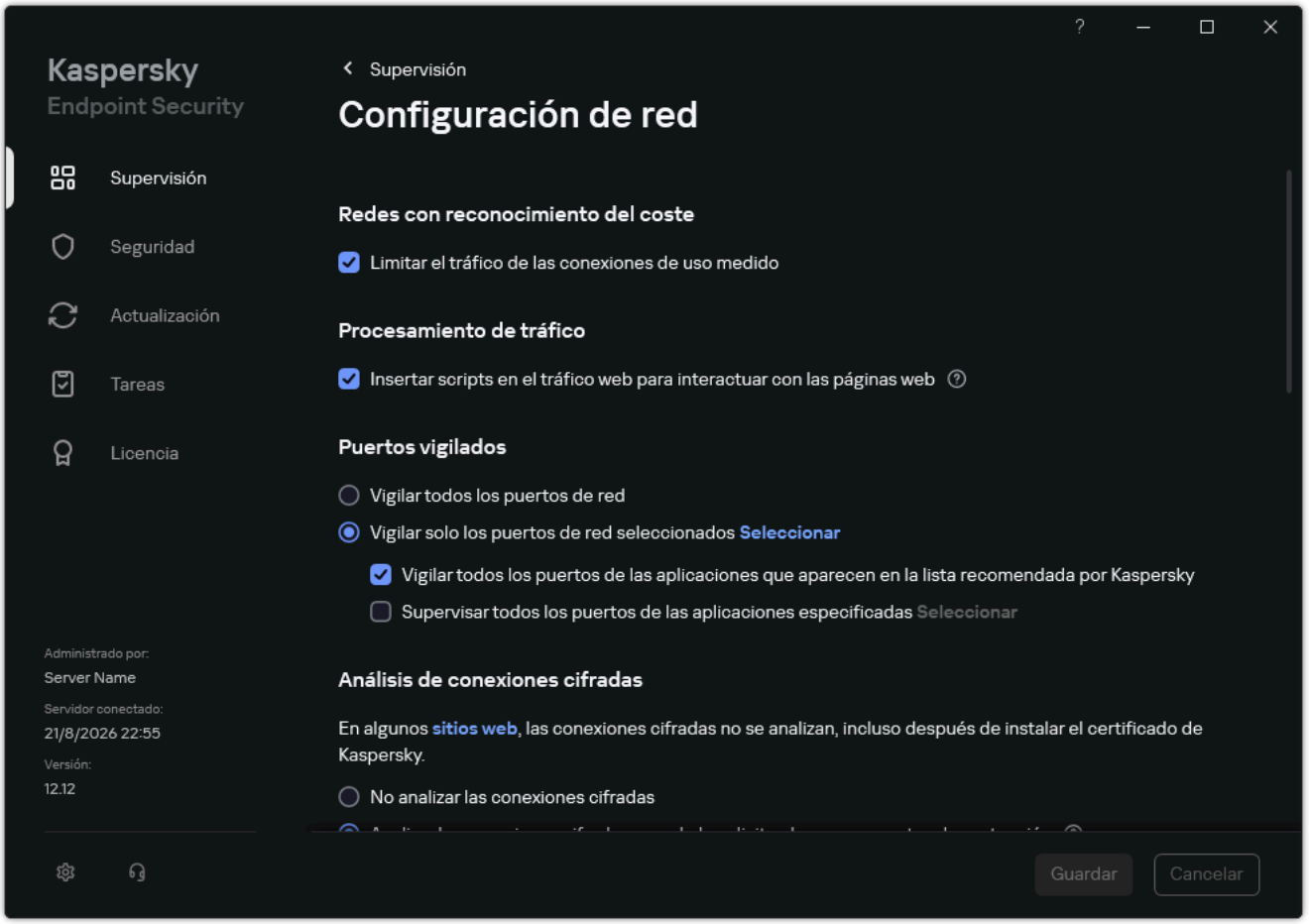
Kaspersky Endpoint Security divide los puertos TCP y UDP del equipo del usuario en varios grupos, según las probabilidades de que se vean en riesgo. Algunos puertos de red están reservados para servicios vulnerables. Se recomienda prestar especial atención a ellos: existe un riesgo mucho mayor de que se los utilice en un ataque de red. Si usa servicios no estándares que dependen de puertos de red no estándares, dichos puertos de red también pueden ser el objetivo de los equipos atacantes. Puede especificar una lista de puertos de red y una lista de aplicaciones que solicitan acceso a la red. Estos puertos y aplicaciones recibirán atención especial de los componentes Protección frente a amenazas en el correo y Protección de amenazas web durante la supervisión del tráfico de red.

Para ayudar a garantizar la seguridad del equipo, los componentes Detección de comportamiento y Prevención de exploits también supervisan los flujos de datos que pasan a través de los puertos de red. Los componentes supervisan continuamente el tráfico de red en busca de procesos individuales que puedan ser peligrosos.

Activación de la vigilancia de todos los puertos de red

Para activar la vigilancia de todos los puertos de red, haga lo siguiente:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.



Configuración de la supervisión de puertos de red

3. En el bloque **Puertos vigilados**, seleccione **Vigilar todos los puertos de red**.
4. Guarde los cambios.

Creación de una lista de puertos de red supervisados

Para crear una lista de puertos de red supervisados:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.

4. Haga clic en **Seleccionar**.

   Esto despliega una lista de puertos de red que se usan normalmente para la transmisión de correos electrónicos y el tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.

5. Utilice el interruptor en la columna **Estado** para activar o desactivar la supervisión del puerto de red.

6. Si no aparece un puerto de red en la lista de puertos de red, agréguelo del siguiente modo:

   a. Haga clic en **Añadir**.

   b. En la ventana que se abre, introduzca el número de puerto de red y una breve descripción.

   c. Configure el estado **Activo** o **Inactivo** para la supervisión del puerto de red.

7. Guarde los cambios.

Cuando el protocolo FTP se ejecuta en modo pasivo, la conexión se puede establecer a través de un puerto de red al azar que no se añade a la lista de puertos de red supervisados. Para proteger tales conexiones, habilite la supervisión de todos los puertos de red o configure el control de los puertos de red para aplicaciones que establecen conexiones FTP.

Creación de una lista de aplicaciones para las que se supervisan todos los puertos de red

Puede crear una lista de aplicaciones para las que Kaspersky Endpoint Security supervisa todos los puertos de red.

Recomendamos incluir las aplicaciones que reciben o transmiten datos mediante el protocolo FTP en la lista de aplicaciones para las que Kaspersky Endpoint Security supervisa todos los puertos de red.

Para crear una lista de aplicaciones para las que se supervisan todos los puertos de red:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Configuración de red**.

3. En el bloque **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.

4. Seleccione la casilla **Vigilar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky**.

   Cuando esta casilla está activada, Kaspersky Endpoint Security supervisa todos los puertos usados por las siguientes aplicaciones:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.

- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.
- Yandex Browser.

5. Seleccione la casilla **Supervisar todos los puertos de las aplicaciones especificadas**.
6. Haga clic en **Seleccionar**.
   Esto abre una lista de aplicaciones para las que Kaspersky Endpoint Security supervisa los puertos de red.
7. Utilice el interruptor en la columna **Estado** para activar o desactivar la supervisión del puerto de red.
8. Si una aplicación no está incluida en la lista, agréguela del modo siguiente:
   a. Haga clic en **Añadir**.
   b. En la ventana que se abre, introduzca la ruta al archivo ejecutable de la aplicación y una breve descripción.
   c. Configure el estado **Activo** o **Inactivo** para la supervisión de los puertos de red.
9. Guarde los cambios.

Exportación e importación de listas de puertos vigilados

Kaspersky Endpoint Security utiliza las siguientes listas para supervisar los puertos de red: lista de puertos de red y lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security. Puede exportar listas de puertos vigilados a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de puertos con la misma descripción. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de las listas de puertos vigilados o para migrar las listas a un servidor diferente.

Cómo exportar e importar listas de puertos vigilados en la Consola de administración (MMC)

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general → Configuración de red**.

5. Para exportar la lista de puertos de red:

   a. En el bloque **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.

   b. Haga clic en el enlace **seleccionada N puertos**.

   Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos que se usan normalmente para la transmisión de correo electrónico y tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.

   c. En la lista de puertos de red, seleccione los puertos que desea exportar.

   d. Haga clic en **Exportar**.

   e. En la ventana que se abre, ingrese el nombre del archivo XML al que desee exportar la lista de puertos de red y seleccione la carpeta en la que desee guardar este archivo.

   f. Guarde el archivo.

   Kaspersky Endpoint Security exporta la lista completa de puertos de red al archivo XML.

6. Para exportar la lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:

   a. En el bloque **Puertos vigilados**, seleccione la casilla de verificación **Vigilar todos los puertos de las aplicaciones especificadas**.

   b. Haga clic en el enlace **seleccionadas N aplicaciones**.

   c. En la lista de aplicaciones, seleccione las aplicaciones que desea exportar.

   d. Haga clic en **Exportar**.

   e. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de aplicaciones y seleccione la carpeta en la que desee guardar este archivo.

   f. Guarde el archivo.

   Kaspersky Endpoint Security exporta la lista completa de aplicaciones al archivo XML.

7. Para importar la lista de puertos de red:

   a. En la lista de puertos de red, haga clic en el botón **Importar**.

   En la ventana que se abre, seleccione el archivo XML del que quiera importar la lista de puertos de red.

   b. Abra el archivo.

   Si el equipo ya tiene una lista de puertos de red, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

8. Para importar una lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:

   a. En la lista de aplicaciones, haga clic en el botón **Importar**.

   En la ventana que se abre, seleccione el archivo XML del que importar la lista de aplicaciones.

b. Abra el archivo.

Si el equipo ya tiene una lista de aplicaciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

9. Guarde los cambios.

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general → Configuración de red**.

4. En el bloque **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.

5. Haga clic en **Configuración**.

Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos que se usan normalmente para la transmisión de correo electrónico y tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.

6. Para exportar la lista de puertos de red:

a. En la lista de puertos de red, seleccione los puertos que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

Si no seleccionó ningún puerto, Kaspersky Endpoint Security exportará todos los puertos.

b. Haga clic en **Exportar**.

c. En la ventana que se abre, ingrese el nombre del archivo XML al que desee exportar la lista de puertos de red y seleccione la carpeta en la que desee guardar este archivo.

d. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de puertos de red al archivo XML.

7. Para exportar la lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:

a. Seleccione la casilla **Vigilar todos los puertos de las aplicaciones especificadas**.

b. En la lista de aplicaciones, seleccione las aplicaciones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

Si no seleccionó ninguna aplicación, Kaspersky Endpoint Security exportará todas las aplicaciones.

c. Haga clic en **Exportar**.

d. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de aplicaciones y seleccione la carpeta en la que desee guardar este archivo.

e. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de aplicaciones al archivo XML.

8. Para importar la lista de puertos de red:

a. En la lista de puertos de red, haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo XML del que quiera importar la lista de puertos de red.

b. Abra el archivo.

Si el equipo ya tiene una lista de puertos de red, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

9. Para importar una lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:

a. En la lista de aplicaciones, haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo XML del que importar la lista de aplicaciones.

b. Abra el archivo.

Si el equipo ya tiene una lista de aplicaciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

10. Guarde los cambios.

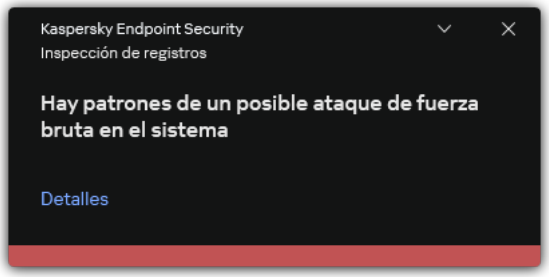
Inspección de registros

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo.

La inspección de registros supervisa la integridad del entorno protegido basándose en los resultados del análisis del Registro de eventos de Windows. Cuando la aplicación detecta señales de comportamientos atípicos en el sistema, informa al administrador debido a que este comportamiento puede indicar un intento de ataque cibernético.

Kaspersky Endpoint Security analiza los registro de eventos de Windows y detecta las violaciones de acuerdo con las reglas. El componente incluye reglas predefinidas. Las reglas predefinidas recibe alimentación del análisis heurístico. También puede añadir sus propias reglas (reglas personalizadas). Cuando se activa una regla, la aplicación crea un evento con el estado *Crítico* (consulte la figura siguiente).

Si desea usar la Inspección de registros, asegúrese de que la configuración de seguridad de la directiva de auditorías esté configurada y que el sistema esté registrando los eventos relevantes (para conocer más detalles, visite el sitio web de soporte técnico de Microsoft).



Notificación de inspección de registros

Configuración de reglas predefinidas

Las reglas predefinidas incluyen plantillas para la actividad anormal en el equipo protegido. La actividad anormal puede significar un intento de ataque. Las reglas predefinidas recibe alimentación del análisis heurístico. Hay siete reglas predefinidas disponibles para la Inspección de registros. Puede activar o desactivar cualquiera de estas reglas. Las reglas predefinidas no se pueden eliminar.

Puede configurar los criterios de activación para las reglas que supervisan eventos para las siguientes operaciones:

- Detección de ataque de fuerza bruta en contraseñas
- Detección de inicio de sesión de red

Cómo configurar reglas predefinidas en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Inspección de registros**.
4. Asegúrese de que la casilla de verificación **Inspección de registros** esté seleccionada.
5. En el bloque **Reglas predefinidas**, haga clic en el botón **Configuración**.
6. Seleccione o desactive las casillas de verificación para configurar reglas predefinidas:
   - **Hay patrones de un posible ataque de fuerza bruta en el sistema**.
   - **Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red**.
   - **Hay patrones de un posible abuso del Registro de eventos de Windows**.
   - **Se han detectado acciones atípicas en nombre de un nuevo servicio instalado**.
   - **Se ha detectado un inicio de sesión atípico que usa credenciales explícitas**.
   - **Hay patrones de un posible ataque de PAC de Kerberos (MS14-068) en el sistema**.
   - **Se han detectado cambios sospechosos en el grupo de administradores integrado con privilegios**.
7. Si es necesario, configure la regla: **Hay patrones de un posible ataque de fuerza bruta en el sistema**:
   a. Haga clic en el botón **Configuración** debajo de la regla.
   b. En la ventana que se abre, especifique el número de intentos y el plazo temporal durante el cual se deben realizar los intentos de introducir una contraseña para que la regla se active.
   c. Haga clic en **Aceptar**.

8. Si ha seleccionado la regla **Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red**, necesita configurar sus ajustes:

    a. Haga clic en el botón **Configuración** debajo de la regla.

    b. En el bloque **Detección de inicio de sesión de red**, especifique el inicio y el final del intervalo temporal.

    Kaspersky Endpoint Security tiene en cuenta los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

    De forma predeterminada, el intervalo no se define y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise continuamente los intentos de inicio de sesión, defina el intervalo en 00:00 h - 23:59 h. El inicio y el final del intervalo no deben coincidir. Si son iguales, la aplicación no supervisa los intentos de inicio de sesión.

    c. Cree la lista de usuarios de confianza y direcciones IP de confianza (IPv4 e IPv6).

    Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio. Kaspersky Endpoint Security no supervisa los intentos de inicio de sesión para estos usuarios y equipos.

    d. Haga clic en **Aceptar**.

9. Guarde los cambios.

Cómo configurar las reglas predefinidas en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

    Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Inspección de registros**.

5. Asegúrese de que el interruptor **Inspección de registro ACTIVADA** esté activado.

6. En el bloque **Reglas predefinidas**, active o desactive las reglas predefinidas mediante los interruptores:

    - **Hay patrones de un posible ataque de fuerza bruta en el sistema**.
    - **Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red**.
    - **Hay patrones de un posible abuso del Registro de eventos de Windows**.
    - **Se han detectado acciones atípicas en nombre de un nuevo servicio instalado**.
    - **Se ha detectado un inicio de sesión atípico que usa credenciales explícitas**.
    - **Hay patrones de un posible ataque de PAC de Kerberos (MS14-068) en el sistema**.

    a. **Se han detectado cambios sospechosos en el grupo de administradores integrado con privilegios**.

7. Si es necesario, configure la regla: **Hay patrones de un posible ataque de fuerza bruta en el sistema**:

   a. Haga clic en **Configuración** debajo de la regla.

   b. En la ventana que se abre, especifique el número de intentos y el plazo temporal durante el cual se deben realizar los intentos de introducir una contraseña para que la regla se active.

   c. Haga clic en **Aceptar**.

8. Si ha seleccionado la regla **Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red**, necesita configurar sus ajustes:

   a. Haga clic en **Configuración** debajo de la regla.

   b. En el bloque **Detección de inicio de sesión de red**, especifique el inicio y el final del intervalo temporal.

   Kaspersky Endpoint Security tiene en cuenta los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

   De forma predeterminada, el intervalo no se define y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise continuamente los intentos de inicio de sesión, defina el intervalo en 00:00 h - 23:59 h. El inicio y el final del intervalo no deben coincidir. Si son iguales, la aplicación no supervisa los intentos de inicio de sesión.

   c. En el bloque **Exclusiones**, añada los usuarios de confianza y las direcciones IP de confianza (IPv4 e IPv6).

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio. Kaspersky Endpoint Security no supervisa los intentos de inicio de sesión para estos usuarios y equipos.

   d. Haga clic en **Aceptar**.

9. Guarde los cambios.

Cómo configurar reglas predefinidas en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Inspección de registros**.
3. Asegúrese de que el interruptor **Inspección de registros** esté activado.
4. En el bloque **Reglas predefinidas**, haga clic en el botón **Configurar**.
5. Seleccione o desactive las casillas de verificación para configurar reglas predefinidas:

   - **Hay patrones de un posible ataque de fuerza bruta en el sistema**.
   - **Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red**.
   - **Hay patrones de un posible abuso del Registro de eventos de Windows**.
   - **Se han detectado acciones atípicas en nombre de un nuevo servicio instalado**.

- **Se ha detectado un inicio de sesión atípico que usa credenciales explícitas**.
- **Hay patrones de un posible ataque de PAC de Kerberos (MS14-068) en el sistema**.

a. **Se han detectado cambios sospechosos en el grupo de administradores integrado con privilegios**.

6. Si es necesario, configure la regla: **Hay patrones de un posible ataque de fuerza bruta en el sistema**:

   a. Haga clic en **Configuración** debajo de la regla.

   b. En la ventana que se abre, especifique el número de intentos y el plazo temporal durante el cual se deben realizar los intentos de introducir una contraseña para que la regla se active.

7. Si ha seleccionado la regla **Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red**, necesita configurar sus ajustes:

   a. Haga clic en **Configuración** debajo de la regla.

   b. En el bloque **Detección de inicio de sesión de red**, especifique el inicio y el final del intervalo temporal.

   Kaspersky Endpoint Security tiene en cuenta los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

   De forma predeterminada, el intervalo no se define y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise continuamente los intentos de inicio de sesión, defina el intervalo en 00:00 h - 23:59 h. El inicio y el final del intervalo no deben coincidir. Si son iguales, la aplicación no supervisa los intentos de inicio de sesión.

   c. En el bloque **Exclusiones**, añada los usuarios de confianza y las direcciones IP de confianza (IPv4 e IPv6).

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio. Kaspersky Endpoint Security no supervisa los intentos de inicio de sesión para estos usuarios y equipos.

8. Guarde los cambios.

Como resultado, cuando se activa la regla, Kaspersky Endpoint Security crea un *Evento crítico*.

Adición de reglas personalizadas

Puede configurar sus propios criterios para la activación de la regla de Inspección de registros. Para hacerlo, debe introducir un identificador del evento y seleccionar el origen de un evento. Puede buscar el identificador del evento en el sitio web de soporte técnico de Microsoft. Puede seleccionar el origen de un evento desde los registros estándar: *Application*, *Security* o *System*. También puede especificar el registro de una aplicación de terceros. Puede descubrir el nombre del registro de una aplicación de terceros usando la herramienta Visualizador de eventos. Los registros de las aplicaciones de terceros se conservan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro *Windows PowerShell*).

La aplicación no comprueba si el registro especificado se encuentra realmente en el registro de eventos de Windows. Si hay un error en el nombre del registro, la aplicación no supervisa los eventos de ese registro.

La lista de reglas personalizadas incluye tres reglas que crearon expertos de Kaspersky.

Cómo añadir una regla personalizada en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Inspección de registros**.
4. Asegúrese de que la casilla de verificación **Inspección de registros** esté seleccionada.
5. En el bloque **Reglas personalizadas**, haga clic en el botón **Configuración**.
6. En la ventana que se abre, seleccione las casillas al lado de las reglas personalizadas que desee activar.
7. Si es necesario, haga clic en **Añadir** para crear sus propias reglas personalizadas.
8. Esto abre una ventana; dentro de esa ventana, configure la regla personalizada:
   - **Nombre de la regla**.
   - **Nombre de registro**. Registro de eventos de Windows. Estos son los registros disponibles: *Application*, *Security*, *System*.
   - **Origen**. Registros de aplicaciones de terceros. Puede descubrir el nombre del registro de una aplicación de terceros usando la herramienta Visualizador de eventos. Los registros de las aplicaciones de terceros se conservan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro *Windows PowerShell*).
   - **Identificadores de eventos**. Identificadores de eventos en el Registro de eventos de Windows. Puede buscar el identificador del evento en la documentación técnica de Microsoft.
9. Guarde los cambios.

Cómo añadir una regla personalizada en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Inspección de registros**.
5. Asegúrese de que el interruptor **Inspección de registro ACTIVADA** esté activado.
6. En el bloque **Reglas personalizadas**, seleccione las reglas personalizadas que desea supervisar:
7. Si es necesario, haga clic en **Añadir** para crear sus propias reglas personalizadas.
8. Esto abre una ventana; dentro de esa ventana, configure la regla personalizada:
   - **Nombre de la regla**.
   - **Nombre de registro personalizado**. Registro de eventos de Windows. Estos son los registros disponibles: *Application*, *Security*, *System*.

- **Origen**. Registros de aplicaciones de terceros. Puede descubrir el nombre del registro de una aplicación de terceros usando la herramienta Visualizador de eventos. Los registros de las aplicaciones de terceros se conservan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro *Windows PowerShell*).

- **Identificadores de eventos**. Identificadores de eventos en el Registro de eventos de Windows. Puede buscar el identificador del evento en la documentación técnica de Microsoft.

9. Guarde los cambios.

Cómo añadir una regla personalizada en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Inspección de registros**.
3. Asegúrese de que el interruptor **Inspección de registros** esté activado.
4. En el bloque **Reglas personalizadas**, haga clic en el botón **Configurar**.
5. En la ventana que se abre, seleccione las casillas al lado de las reglas personalizadas que desee activar.
6. Si es necesario, haga clic en **Añadir** para crear sus propias reglas personalizadas.
7. Esto abre una ventana; dentro de esa ventana, configure la regla personalizada:

   - **Nombre de la regla**.

   - **Nombre de registro**. Registro de eventos de Windows. Estos son los registros disponibles: *Application*, *Security*, *System*.

   - **Origen**. Registros de aplicaciones de terceros. Puede descubrir el nombre del registro de una aplicación de terceros usando la herramienta Visualizador de eventos. Los registros de las aplicaciones de terceros se conservan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro *Windows PowerShell*).

   - **Identificador de eventos**. Identificadores de eventos en el Registro de eventos de Windows. Puede buscar el identificador del evento en la documentación técnica de Microsoft.

8. Guarde los cambios.

Como resultado, cuando se activa la regla, Kaspersky Endpoint Security crea un evento *Crítico*.

Control de integridad del sistema

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo.

A partir de la versión 12.6, Kaspersky Endpoint Security para Windows incluye el componente Control de integridad del sistema en lugar del componente Monitor de integridad de archivos. El componente Control de integridad del sistema incluye todas las funciones de Monitor de integridad de archivos y, además, permite supervisar los cambios en el registro y la conexión de dispositivos externos.

El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que pueden indicar infracciones de la seguridad del equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos correspondientes y alerta al administrador. El Control de integridad del sistema puede funcionar en tiempo real y también puede realizar comprobaciones de la integridad del sistema a demanda.

Control de integridad del sistema en tiempo real

En modo de tiempo real, el Control de integridad del sistema rastrea los cambios en los objetos que incluyó en la cobertura del componente (la *cobertura de la supervisión*). El Control de integridad del sistema también permite bloquear el acceso no autorizado a dichos objetos en tiempo real.

Comprobación de integridad del sistema a demanda

La Comprobación de integridad del sistema a demanda es una tarea que puede ejecutar manualmente o según una programación. Para ejecutar la tarea *Comprobación de la integridad del sistema*, debe configurar el alcance del componente (la *cobertura de la supervisión*) y crear una línea de base. Una *línea de base* es un estado registrado de los objetos en el sistema, que la aplicación utiliza como referencia al comparar con el estado actual.

Migración de la configuración del Monitor de integridad de archivos

Cuando actualiza Kaspersky Endpoint Security a la versión 12.6, la configuración del Monitor de integridad de archivos se migra automáticamente. Como parte de la migración, la aplicación mueve las reglas de supervisión a Control de integridad del sistema. Las reglas de Monitor de integridad de archivos también se migran a Control de integridad del sistema cuando se migra de KSWS a KES.

Para garantizar el correcto funcionamiento del Control de integridad del sistema, la aplicación Kaspersky Endpoint Security y el complemento de administración deben actualizarse a la versión 12.6. Si tiene instalada una versión anterior del complemento de administración, no puede configurar el Control de integridad del sistema porque el complemento de administración carece de la sección **Control de integridad del sistema**.

Acerca de las reglas del Control de integridad del sistema

Para que el Control de integridad del sistema funcione, debe añadir al menos una regla. Una *regla de Control de integridad del sistema* es un conjunto de criterios que definen el acceso de los usuarios a los archivos y al registro. El Control de integridad del sistema detecta cambios en los archivos y el registro dentro de la *cobertura de la supervisión* especificada. La cobertura de la supervisión es uno de los criterios de una regla del Control de integridad del sistema.

El Control de integridad del sistema permite supervisar los siguientes objetos:

- Archivos
- Registro
- Dispositivos externos

Consideraciones especiales involucradas en el control de archivos

El Control de integridad del sistema supervisa los cambios en los archivos y carpetas, así como los archivos que se añaden a la cobertura de la supervisión o se eliminan de ella. Estos cambios pueden indicar una filtración en la seguridad del equipo. Recomendamos añadir objetos que rara vez que modifican u objetos a los cuales solamente el administrador puede acceder. Esto ayuda a reducir el número de eventos del Control de integridad del sistema.

Control de integridad del sistema no supervisa los cambios en los archivos de las carpetas compartidas del servidor. Control de integridad del sistema solo se puede utilizar de forma local.

Kaspersky Endpoint Security supervisa los cambios de archivos y carpetas solo en aquellos discos que estaban conectados cuando el Control de integridad del sistema en tiempo real comenzó a funcionar. Si un disco no estaba conectado cuando el Control de integridad del sistema en tiempo real comenzó a funcionar, la aplicación no supervisa los cambios de archivos y carpetas en ese disco, incluso si los archivos y carpetas se añaden a la cobertura de la supervisión.

Consideraciones especiales involucradas en el control del registro

El Control de integridad del sistema supervisa el registro. Estos cambios pueden indicar una filtración en la seguridad del equipo.

El Control de integridad del sistema supervisa las siguientes claves raíz del registro:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (disponible solo en Supervisión de la integridad del sistema en tiempo real)

- `HKEY_CURRENT_USER` (disponible solo en Supervisión de la integridad del sistema en tiempo real)

  La tarea *Comprobación de la integridad del sistema* no es compatible con la clave `HKEY_CURRENT_USER`. Puede especificar una clave en `HKEY_USERS` como `HKEY_USERS\<user profile ID>\<key>`.

Consideraciones especiales involucradas en el control de dispositivos externos

El Control de integridad del sistema supervisa la conexión y desconexión de dispositivos externos. Esto es necesario para proteger el equipo de las amenazas a la seguridad que pueden resultar del intercambio de archivos con dichos dispositivos. El Control de integridad del sistema no supervisa el acceso a dispositivos externos y no bloquea el intercambio de archivos. Puede configurar el acceso a los dispositivos mediante un componente de aplicación diferente, Control de dispositivos.

Al ejecutar la tarea *Monitor de integridad del sistema de línea base*, la aplicación ignora la reconexión de dispositivos externos si los dispositivos tienen la misma letra de unidad en el sistema operativo. Para registrarse, los dispositivos reconectados deben tener letras de unidad diferentes.

El Control de integridad del sistema supervisa la conexión de los siguientes tipos de dispositivos externos:

- Unidad extraíble (incluidas las unidades flash USB)
- Disco duro
- Adaptador de red externo
- Unidad de CD/DVD/Blu-ray
- Escáner y cámara

Control de integridad del sistema en tiempo real

El Control de integridad del sistema permite realizar un seguimiento de los cambios en el sistema operativo en tiempo real. Puede realizar un seguimiento de los cambios que pueden indicar infracciones de seguridad en el equipo. El componente permite bloquear estos cambios o limitarse a registrar eventos de cambio.

Para que el Control de integridad del sistema funcione, debe añadir al menos una regla. Una *regla de Control de integridad del sistema* es un conjunto de criterios que definen el acceso de los usuarios a los archivos y al registro. El Control de integridad del sistema detecta cambios en los archivos y el registro dentro de la *cobertura de la supervisión* especificada. La cobertura de la supervisión es uno de los criterios de una regla del Control de integridad del sistema.

Modos de Control de integridad del sistema en tiempo real

Para asegurarse de que las reglas de Control de integridad del sistema no bloqueen ninguna acción con recursos que sean críticos para el funcionamiento del sistema operativo u otros servicios, recomendamos activar el modo de prueba y analizar cómo afecta al sistema el componente. Con el modo de prueba activado, Kaspersky Endpoint Security no bloquea la actividad del usuario que está prohibida por las reglas, sino que genera eventos *Advertencia* ⚠.

El componente Control de integridad del sistema en tiempo real tiene dos modos:

- Bloquear

  En este modo, el Control de integridad del sistema rastrea los cambios en el sistema y realiza una acción de acuerdo con las reglas: **Permitir** o **Bloquear**. El Control de integridad del sistema también genera un evento correspondiente y cambia el estado del dispositivo en la consola de Kaspersky Security Center.

- Informar

  En este modo, el Control de integridad del sistema permite acciones con archivos y claves de registro desde la cobertura de la supervisión. Si se prohíben la acción con archivos o el registro, la aplicación genera un evento: *La operación prohibida se permitió en el modo de prueba*. Para analizar cómo afectan las reglas al sistema, puede consultar informes.

Activación del Control de integridad del sistema en tiempo real

Cómo activar el Control de integridad del sistema en tiempo real en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de integridad del sistema**.
4. Seleccione la casilla **Control de integridad del sistema**.
5. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para el Control de integridad del sistema en tiempo real:
   - **Bloquear**. En este modo, el Control de integridad del sistema bloquea las acciones con archivos y claves de registro de la cobertura de la supervisión y genera un evento correspondiente.
   - **Informar**. En este modo, el Control de integridad del sistema permite acciones con archivos y claves de registro desde el cobertura de la supervisión y genera un evento correspondiente.
6. En el bloque **Control de integridad del sistema en tiempo real**, seleccione la casilla de verificación **Control de integridad del sistema en tiempo real**.

7. Configurar el control de dispositivos externos:

   a. Seleccione la casilla **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de control de dispositivos externos: *Informativo*, *Advertencia*, *Crítico*.

   El Control de integridad del sistema registra la conexión actual de dispositivos externos. La aplicación comienza a supervisar la conexión y desconexión de dispositivos externos después de que el componente se active en la configuración de la aplicación. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente.

8. Configure el Control de archivos y registros:

   a. Seleccione la casilla **Supervisar archivos y el registro**.

   b. Haga clic en **Configuración**.

   Esto abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Añadir**.

   También puede importar reglas de otra fuente.

   d. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar el Control de integridad del sistema en tiempo real en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de integridad del sistema**.

5. Active la opción **Control de integridad del sistema ACTIVADO**.

6. Seleccione la pestaña **Windows**.

7. En **Control de integridad del sistema en tiempo real**, seleccione un modo para el Control de integridad del sistema en tiempo real:

   - **Aplicar reglas**. En este modo, el Control de integridad del sistema bloquea las acciones con archivos y claves de registro de la cobertura de la supervisión y genera un evento correspondiente.

   - **Reglas de prueba (informar)**. En este modo, el Control de integridad del sistema permite acciones con archivos y claves de registro desde el cobertura de la supervisión y genera un evento correspondiente.

8. Configure el Control de archivos y registros:

   a. Seleccione la casilla **Supervisar archivos y el registro**.

   b. Haga clic en **Reglas**.

      Esto abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Añadir**.

      También puede importar reglas de otra fuente.

   d. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

9. Configurar el control de dispositivos externos:

   a. Seleccione la casilla **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de control de dispositivos externos: *Informativo*, *Advertencia*, *Crítico*.

   El Control de integridad del sistema registra la conexión actual de dispositivos externos. La aplicación comienza a supervisar la conexión y desconexión de dispositivos externos después de que el componente se active en la configuración de la aplicación. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente.

10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo activar el Control de integridad del sistema en tiempo real en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de integridad del sistema**.

3. Active el interruptor **Control de integridad del sistema**.

4. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para el Control de integridad del sistema en tiempo real:

   - **Bloquear**. En este modo, el Control de integridad del sistema bloquea las acciones con archivos y claves de registro de la cobertura de la supervisión y genera un evento correspondiente.

   - **Informar**. En este modo, el Control de integridad del sistema permite acciones con archivos y claves de registro desde el cobertura de la supervisión y genera un evento correspondiente.

5. En el bloque **Control de integridad del sistema en tiempo real**, seleccione la casilla de verificación **Control de integridad del sistema en tiempo real**.

6. Configurar el control de dispositivos externos:

   a. Seleccione la casilla **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de control de dispositivos externos: *Informativo*, *Advertencia*, *Crítico*.

El Control de integridad del sistema registra la conexión actual de dispositivos externos. La aplicación comienza a supervisar la conexión y desconexión de dispositivos externos después de que el componente se active en la configuración de la aplicación. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente.

7. Configure el Control de archivos y registros:

   a. Seleccione la casilla **Supervisar archivos y el registro**.

   b. Haga clic en **Configurar**.

   Esto abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Añadir**.

   También puede importar reglas de otra fuente.

8. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

9. Guarde los cambios.

Configuración de las reglas de Control de integridad del sistema en tiempo real

Parámetro	Descripción
Nombre de la regla	Nombre de la regla de Control de integridad del sistema en tiempo real
Operaciones con archivos y registro	• **Permitir**. El Control de integridad del sistema permite acciones con archivos y claves de registro desde la cobertura de la supervisión. • **Bloquear**. El comportamiento del Control de integridad del sistema depende del modo seleccionado. Si ha seleccionado el *Modo de protección del sistema*, el Control de integridad del sistema bloquea las acciones con archivos y claves de registro de la cobertura de la supervisión, genera un evento correspondiente y cambia el estado del dispositivo en la consola de Kaspersky Security Center. Si ha seleccionado el *Modo de prueba*, el Control de integridad del sistema permite acciones con archivos y claves de registro desde la cobertura de la supervisión.

Parámetro	Descripción
Nivel de gravedad del evento	Kaspersky Endpoint Security registra eventos de modificación de archivos cada vez que se modifica un archivo o clave de registro en la cobertura de supervisión. Estos son los niveles de gravedad del evento disponibles: *Informativo*, *Advertencia*, *Crítico*.

Cobertura de supervisión	• **Archivo**. Lista de archivos y carpetas supervisados por el componente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.
	Usar máscaras:
	  • El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
	  • Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
	• **Registro**. Lista de claves de registro y valores supervisados por el componente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

Exclusiones	• **Archivo**. Lista de exclusiones de la cobertura de supervisión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. Por ejemplo, `C:\Folder\Application\*.log`. Las entradas de exclusión tienen una prioridad más alta que las entradas de la cobertura de supervisión.
	Usar máscaras:
	  • El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
	  • Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
	• **Registro**. Lista de exclusiones de la cobertura de supervisión. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara. Las entradas de exclusión tienen una prioridad más alta que las entradas de la cobertura de supervisión.

Usuarios o grupos de usuarios de confianza	Un *usuario de confianza* es un usuario que tiene permiso para realizar acciones con archivos y claves de registro en la cobertura de la supervisión. Si Kaspersky Endpoint Security detecta una acción realizada por un usuario de confianza, el Control de integridad del sistema genera un evento *Informativo*. Puede seleccionar usuarios en Active Directory, en la lista de cuentas de Kaspersky Security Center o al introducir un nombre de usuario local de forma manual. Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio.
Marcadores de operaciones con archivos/Operaciones supervisadas	Marcadores que caracterizan la acción con archivos o claves de registro que supervisará la aplicación.
Hash	Cálculo del hash de un archivo al modificarlo. Kaspersky Endpoint Security añade información sobre el hash del archivo cuando se genera un evento.

Comprobación de integridad del sistema a demanda

La Comprobación de integridad del sistema a demanda es una tarea que puede ejecutar manualmente o según una programación. Al ejecutar la tarea *Comprobación de la integridad del sistema*, la aplicación compara el estado actual de los objetos incluidos en la cobertura de supervisión con su estado de *línea de base*. A diferencia del Control de integridad del sistema en tiempo real, la tarea *Comprobación de la integridad del sistema* ayuda a limitar el número de eventos y le permite generar un informe general de los cambios en el sistema operativo.

Para que el Control de integridad del sistema funcione, debe añadir al menos una regla. Una *regla de Control de integridad del sistema* es un conjunto de criterios que definen el acceso de los usuarios a los archivos y al registro. El Control de integridad del sistema detecta cambios en los archivos y el registro dentro de la *cobertura de la supervisión* especificada. La cobertura de la supervisión es uno de los criterios de una regla del Control de integridad del sistema. Puede configurar reglas para que las compartan el Control de integridad del sistema en tiempo real y la tarea *Comprobación de la integridad del sistema* o crear reglas independientes para la tarea. Para crear una línea de base, Kaspersky Endpoint Security aplica la cobertura de supervisión desde la tarea *Comprobación de la integridad del sistema* a la tarea *Actualización prevista*.

Crear y actualizar una línea de base

La tarea *Comprobación de la integridad del sistema* necesita una línea de base para funcionar. Una *línea de base* es un estado registrado de los objetos en el sistema, que la aplicación utiliza como referencia al comparar con el estado actual. Si el estado actual del sistema es diferente del estado del sistema registrado en la línea de base, Kaspersky Endpoint Security genera el evento correspondiente. Puede crear o actualizar una línea de base utilizando la tarea *Actualización prevista*.

Puede actualizar la línea de base en los siguientes modos:

- Actualización completa.

  La aplicación actualiza todos los objetos en la cobertura de la supervisión.

- Actualización incremental.

  La aplicación detecta y actualiza solo objetos nuevos o modificados.

Cómo crear o actualizar una línea de base en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Actualización prevista**.

Paso 2. Selección del modo de actualización de la línea de base

Seleccione un modo de actualización de la línea de base:

- **Actualización completa**. La aplicación actualiza todos los objetos en la cobertura de la supervisión.
- **Actualización incremental**. La aplicación detecta y actualiza solo objetos nuevos o modificados.

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Definir el nombre de la tarea

Introduzca el nombre de la tarea; por ejemplo, *Línea de base 2024*.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo crear o actualizar una línea de base en la consola web

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Actualización prevista**.

c. En el campo **Nombre de la tarea**, escriba una descripción breve; por ejemplo, *Línea de base 2024*.

d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.
5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.
6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.
7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.
8. Seleccione la pestaña **Configuración de la aplicación**.
9. Seleccione un modo de actualización de la línea de base:
   - **Actualización completa**. La aplicación actualiza todos los objetos en la cobertura de la supervisión.
   - **Actualización incremental**. La aplicación detecta y actualiza solo objetos nuevos o modificados.
10. Guarde los cambios.
11. Active la casilla ubicada junto a la tarea.
12. Haga clic en **Iniciar**.

Configuración de la cobertura de la supervisión para la tarea Comprobación de la integridad del sistema

De forma predeterminada, la cobertura de la supervisión de la tarea *Comprobación de la integridad del sistema* es la misma que la cobertura de la supervisión del Control de integridad del sistema en tiempo real. Puede configurar una cobertura de la supervisión diferente para la tarea.

> La supervisión de la integridad del sistema no admite la importación de las claves `HKEY_CURRENT_USER` y `HKEY_CURRENT_CONFIG` para la tarea *Comprobación de la integridad del sistema*. Si el alcance de la supervisión de la tarea contiene estas claves, la aplicación genera el evento *La cobertura de la supervisión incluye objetos incorrectos*.

Cómo configurar un cobertura de la supervisión diferente para la tarea Comprobación de la integridad del sistema en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de integridad del sistema**.
4. Seleccione la casilla **Control de integridad del sistema**.

5. En **Comprobación de la integridad del sistema**, seleccione el modo de configuración de la tarea: **Configuración personalizada**.

6. Configurar el control de dispositivos externos:

   a. Seleccione la casilla **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de control de dispositivos externos: *Informativo* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

   El Control de integridad del sistema registra información sobre los dispositivos externos conectados en el momento en que se crea la línea de base. Posteriormente, cuando se conecta un dispositivo externo, la aplicación genera un evento correspondiente. Al ejecutar la tarea *Comprobación de la integridad del sistema*, la aplicación no supervisa la desconexión de dispositivos externos.

7. Configure el Control de archivos y registros:

   a. Seleccione la casilla **Supervisar archivos y el registro**.

   b. Haga clic en **Configuración**.

   Esto abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Añadir**.

   También puede importar reglas de otra fuente.

   d. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

8. Guarde los cambios.

Cómo configurar un cobertura de la supervisión diferente para la tarea Comprobación de la integridad del sistema en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de integridad del sistema**.

5. Seleccione la pestaña **Windows**.

6. Active la opción **Control de integridad del sistema ACTIVADO**.

7. En **Comprobación de la integridad del sistema**, seleccione el modo de configuración de la tarea: **Configuración personalizada**.

8. Configurar el control de dispositivos externos:

   a. Seleccione la casilla **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de control de dispositivos externos: *Informativo* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

El Control de integridad del sistema registra información sobre los dispositivos externos conectados en el momento en que se crea la línea de base. Posteriormente, cuando se conecta un dispositivo externo, la aplicación genera un evento correspondiente. Al ejecutar la tarea *Comprobación de la integridad del sistema*, la aplicación no supervisa la desconexión de dispositivos externos.

9. Configure el Control de archivos y registros:

   a. Seleccione la casilla **Supervisar archivos y el registro**.

   b. Haga clic en **Reglas**.

      Esto abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Añadir**.

      También puede importar reglas de otra fuente.

   d. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

10. Guarde los cambios.

Cómo configurar un cobertura de la supervisión diferente para la tarea Comprobación de la integridad del sistema en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad → Control de integridad del sistema**.

3. Active el interruptor **Control de integridad del sistema**.

4. En **Comprobación de la integridad del sistema**, seleccione el modo de configuración de la tarea: **Configuración personalizada**.

5. Configurar el control de dispositivos externos:

   a. Seleccione la casilla **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de control de dispositivos externos: *Informativo* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

   El Control de integridad del sistema registra información sobre los dispositivos externos conectados en el momento en que se crea la línea de base. Posteriormente, cuando se conecta un dispositivo externo, la aplicación genera un evento correspondiente. Al ejecutar la tarea *Comprobación de la integridad del sistema*, la aplicación no supervisa la desconexión de dispositivos externos.

6. Configure el Control de archivos y registros:

   a. Seleccione la casilla **Supervisar archivos y el registro**.

   b. Haga clic en **Configurar**.

      Esto abre la lista de reglas de Control de integridad del sistema.

c. Haga clic en **Añadir**.

También puede importar reglas de otra fuente.

d. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

7. Guarde los cambios.

Configuración de una regla de la tarea Comprobación de la integridad del sistema

Parámetro	Descripción
Nombre de la regla	Nombre de la regla de la tarea *Comprobación de la integridad del sistema*.
Nivel de gravedad del evento	Kaspersky Endpoint Security registra eventos de modificación de archivos cada vez que se modifica un archivo o clave de registro en la cobertura de supervisión. Estos son los niveles de gravedad del evento disponibles: *Informativo*, *Advertencia*, *Crítico*.

Cobertura de supervisión	• **Archivo**. Lista de archivos y carpetas supervisados por el componente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.
	Usar máscaras:
	  • El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
	  • Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
	• **Registro**. Lista de claves de registro y valores supervisados por el componente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara.

Exclusiones	• **Archivo**. Lista de exclusiones de la cobertura de supervisión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. Por ejemplo, `C:\Folder\Application\*.log`. Las entradas de exclusión tienen una prioridad más alta que las entradas de la cobertura de supervisión.
	Usar máscaras:
	  • El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
	  • Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
	• **Registro**. Lista de exclusiones de la cobertura de supervisión. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara. Las entradas de exclusión tienen una prioridad más alta que las entradas de la cobertura de supervisión.

Ejecución de la tarea Comprobación de la integridad del sistema

La tarea *Comprobación de la integridad del sistema* permite verificar archivos o claves de registro para detectar cambios, así como verificar la conexión de dispositivos externos. Para comprobar si hay cambios en los archivos, puede ejecutar la tarea *Comprobación de la integridad del sistema* en los siguientes modos:

- Análisis rápido.

  Al comprobar los archivos en busca de cambios, las aplicaciones solo verifican los atributos de los archivos. La aplicación no comprueba el contenido de los mismos.

- Análisis completo.

  Al verificar los archivos en busca de cambios, las aplicaciones verifican todos los atributos de los archivos, así como su contenido.

El modo en el que se ejecuta la tarea no afecta la comprobación del registro o de los dispositivos externos.

Cómo ejecutar la tarea Comprobación de la integridad del sistema en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.

   Se abre la lista de tareas.
3. Haga clic en **Nueva tarea**.

   El Asistente de tareas comienza. Siga las instrucciones del Asistente.
4. Seleccione **Kaspersky Endpoint Security → Monitor de integridad del sistema de línea base**. Seleccione un modo de Control de integridad del sistema:

   - **Análisis completo**. En este modo, la aplicación comprueba todos los atributos y hashes de los archivos.
   - **Análisis rápido**. En este modo, la aplicación comprueba solo los atributos de los archivos.
5. Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

   - Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado dispositivos no asignados. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
   - Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.
   - Especifique la selección de dispositivos para los que desea ejecutar la tarea.
   - Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
6. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.
7. Configure una planificación para iniciar una tarea, por ejemplo, manualmente o un día concreto de la semana.

8. Introduzca un nombre para la tarea.

9. Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo ejecutar una tarea Comprobación de la integridad del sistema en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Comprobación de la integridad del sistema**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Comprobación de integridad del sistema semanal*).

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. Seleccione un modo de Comprobación de integridad del sistema:

   - **Análisis rápido**. La aplicación comprueba solo los atributos del archivo. La aplicación no comprueba el contenido de los mismos.

   - **Análisis completo**. La aplicación comprueba todos los atributos de los archivos, así como su contenido.

10. Guarde los cambios.

11. Active la casilla ubicada junto a la tarea.

12. Haga clic en **Iniciar**.

Para que la tarea *Comprobación de la integridad del sistema* finalice correctamente, la cobertura de la supervisión de la tarea *Comprobación de la integridad del sistema* debe coincidir completamente con la línea de base. Si la cobertura de la supervisión es diferente, la tarea termina con un error. Para sincronizar las coberturas de la supervisión, ejecute la tarea *Actualización prevista* con una nueva cobertura de la supervisión.

Exportación e importación de reglas de Control de integridad del sistema

Puede exportar la lista de reglas de Control de integridad del sistema a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de registros del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de Control de integridad del sistema o para migrar la lista a un servidor diferente.

La supervisión de la integridad del sistema no admite la importación de las claves `HKEY_CURRENT_USER` y `HKEY_CURRENT_CONFIG` para la tarea *Comprobación de la integridad del sistema*. Si el alcance de la supervisión de la tarea contiene estas claves, la aplicación genera el evento *La cobertura de la supervisión incluye objetos incorrectos*.

Cómo exportar e importar una lista de reglas de Control de integridad del sistema en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Controles de seguridad → Control de integridad del sistema**.
4. Para exportar o importar reglas de *Control de integridad del sistema en tiempo real*:
   a. En el bloque **Control de integridad del sistema en tiempo real**, haga clic en el botón **Configuración**.
   b. Para exportar una lista de reglas de Control de integridad del sistema en tiempo real:
      1. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
         Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
      2. Haga clic en el enlace **Exportar**.
      3. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
      4. Guarde el archivo.
         Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.
   c. Para importar una lista de reglas de Control de integridad del sistema en tiempo real:
      1. Haga clic en el enlace **Importar**.
         En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
      2. Abra el archivo.
         Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

5. Para exportar o importar reglas de *Comprobación de integridad del sistema*:

   a. En el bloque **Comprobación de la integridad del sistema**, seleccione **Configuración personalizada**.

   b. Haga clic en **Configuración**.

   c. Para exportar la lista de reglas de Comprobación de integridad del sistema:

      1. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

         Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.

      2. Haga clic en el enlace **Exportar**.

      3. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.

      4. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.

   d. Para importar una lista de reglas de Comprobación de integridad del sistema:

      1. Haga clic en el enlace **Importar**.

         En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.

      2. Abra el archivo.

      Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

6. Guarde los cambios.

Cómo exportar e importar una lista de reglas de Control de integridad del sistema en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad → Control de integridad del sistema**.

5. Seleccione la pestaña **Windows**.

6. Para exportar o importar reglas de *Control de integridad del sistema en tiempo real*:

   a. En el bloque **Control de integridad del sistema en tiempo real**, haga clic en el enlace **Reglas**.

   b. Para exportar una lista de reglas de Control de integridad del sistema en tiempo real:

      1. Seleccione las reglas que quiera exportar.

      2. Haga clic en el botón → **Exportar**.

         Kaspersky Endpoint Security exporta la lista de reglas a un archivo JSON en la carpeta de descargas predeterminada.

   c. Para importar una lista de reglas de Control de integridad del sistema en tiempo real:

      1. Haga clic en el botón → **Importar**.

         En la ventana que se abre, seleccione el archivo JSON del que importar la lista de direcciones de confianza.

      2. Abra el archivo.

         Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

7. Para exportar o importar reglas de *Comprobación de integridad del sistema*:

   a. En el bloque **Comprobación de la integridad del sistema a petición**, seleccione **Configuración personalizada**.

   b. Haga clic en el enlace **Reglas**.

   c. Para exportar la lista de reglas de Comprobación de integridad del sistema:

      1. Seleccione las reglas que quiera exportar.

      2. Haga clic en el botón → **Exportar**.

         Kaspersky Endpoint Security exporta la lista de reglas a un archivo JSON en la carpeta de descargas predeterminada.

   d. Para importar una lista de reglas de Comprobación de integridad del sistema:

      1. Haga clic en el botón → **Importar**.

         En la ventana que se abre, seleccione el archivo JSON del que importar la lista de direcciones de confianza.

      2. Abra el archivo.

         Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

8. Guarde los cambios.

Visualización de informes de Control de integridad del sistema

Para analizar el rendimiento de las reglas de Control de integridad del sistema, puede consultar los informes y eventos generados por la aplicación. Kaspersky Endpoint Security genera los siguientes informes sobre el componente:

- En la interfaz de la aplicación:
  - El informe de Control de integridad del sistema
  - El informe de Comprobación de integridad del sistema
  - El informe de actualización de la línea de base

  Los informes contienen eventos de Control de integridad del sistema.
- En la Consola de Kaspersky Security Center:
  - Informe sobre los equipos en los que se activaron las reglas de control el mayor número de veces
  - Informe sobre las reglas de control activadas con más frecuencia

  De forma predeterminada, se crea un informe para los 30 días anteriores, incluida la fecha en la que se crea el informe.

  Cómo ver los informes de Control de integridad del sistema en la Consola de administración (MMC)

  1. Abra la Consola de administración de Kaspersky Security Center.
  2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
  3. Haga clic en **Nueva plantilla de informe**.

     Se inicia el Asistente de nueva plantilla de informe.
  4. Siga los pasos del Asistente de plantillas de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione el informe de Supervisión de la integridad del sistema (sección **Otro**):
     - **Los 10 principales dispositivos en los que las reglas de Monitor de integridad de archivos/Control de integridad del sistema se activan con mayor frecuencia**.
     - **Las 10 reglas del Monitor de integridad de archivos/Control de integridad del sistema que se activaron en los dispositivos la mayoría de las veces**.

     Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.
  5. Abra el informe haciendo doble clic en él.

  Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

Cómo ver los informes de Control de integridad del sistema en Web Console

1. En la ventana principal de Web Console, seleccione **Supervisión → Informes**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente de nueva plantilla de informe.
3. En **Tipo de plantilla**, en la sección **Otros**, seleccione un informe de Control de integridad del sistema:

   - **Los 10 principales dispositivos en los que las reglas de Monitor de integridad de archivos/Control de integridad del sistema se activan con mayor frecuencia**.
   - **Las 10 reglas del Monitor de integridad de archivos/Control de integridad del sistema que se activaron en los dispositivos la mayoría de las veces**.

   Una vez haya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla.
4. Seleccione y ejecute el informe.

Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

Para ver los eventos generados por la aplicación, también puede usar las selecciones de eventos en la consola de Kaspersky Security Center.

Restablecimiento del estado de integridad del sistema

Los equipos de la consola de Kaspersky Security Center tienen uno de los siguientes estados: *Aceptar*, *Advertencia*, o *Crítico*. Si el Control de integridad del sistema detecta la modificación de archivos o claves de registro en la cobertura de la supervisión, el estado del equipo cambia a *Advertencia* o *Crítico*. El estado asignado por el Control de integridad del sistema se denomina *estado de integridad del sistema*. Puede restablecer el estado de integridad del sistema, por ejemplo, si el análisis le ha convencido de que la modificación de objetos detectada no afecta la seguridad del equipo.

Cómo restablecer el estado de integridad del sistema en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2) → Restablecimiento del estado de integridad del sistema**.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Configurar una planificación de inicio de tarea

Configure la planificación de la tarea; por ejemplo, manualmente.

Paso 4. Definir el nombre de la tarea

Introduzca el nombre de la tarea; por ejemplo, *Restablecer el estado después de modificar la cobertura de la supervisión*.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo restablecer el estado de integridad del sistema en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Restablecimiento del estado de integridad del sistema**.

c. En el campo **Nombre de la tarea**, introduzca una breve descripción; por ejemplo, *Restablecer el estado después de modificar la cobertura de la supervisión*.

d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta para ejecutar la tarea. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Active la casilla ubicada junto a la tarea.

8. Haga clic en **Iniciar**.

Como resultado, si el estado del equipo se cambia a *Advertencia* o *Crítico* debido a los eventos de Control de integridad del sistema, el estado del equipo se restablece a *Aceptar*. Si el estado del equipo también se modificó debido a otros eventos, el estado del equipo no se modifica.

Cloud Discovery

Cloud Discovery administra el acceso de los usuarios a los servicios en la nube. Los servicios en la nube incluyen, por ejemplo, Microsoft Teams, Salesforce y Microsoft Office 365. Los servicios en la nube se agrupan en categorías; por ejemplo, *Uso compartido de archivos*, *Programas de mensajería*, *Correo electrónico*. Los expertos de Kaspersky actualizan de forma periódica las categorías de Cloud Discovery y los servicios en la nube clasificados en las categorías. Kaspersky Endpoint Security actualiza el conjunto de categorías y servicios en la nube con las bases de datos de la aplicación. Esto significa que Cloud Discovery no usa Kaspersky Security Network para establecer categorías de servicios en la nube.

Cloud Discovery proporciona las siguientes funciones:

- Supervisión del uso de los servicios en la nube
- Bloqueo del acceso de los usuarios a los servicios en la nube

Requisitos del sistema

Cloud Discovery está disponible si se cumplen las siguientes condiciones:

- La aplicación está instalada en un equipo que ejecute Windows para estaciones de trabajo.

  El componente no está disponible para servidores.

- Kaspersky Security Center versión 15.1 o superior.

  El componente no está disponible en la Consola de administración (MMC). Puede configurar Cloud Discovery en Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console.

- Licencia de Kaspersky Next.

Habilite la funcionalidad de la aplicación que requiere el componente Cloud Discovery:

1. **Analizar conexiones cifradas**. Esto es necesario para la supervisión del tráfico HTTPS. Puede administrar esta funcionalidad en la sección **Configuración de red**.

2. **Insertar scripts en el tráfico web para interactuar con las páginas web**. El script permite el registro de eventos de Cloud Discovery. El script también proporciona un bloqueo integral del acceso a los servicios en la nube. Sin el script, la aplicación bloquea el acceso únicamente por dominios de los servicios en la nube. Puede administrar esta funcionalidad en la sección **Configuración de red**.

También puede activar la funcionalidad **Registrar el acceso a páginas permitidas**. La funcionalidad incluye la agrupación de eventos cuando un usuario visita páginas web que pertenecen al mismo dominio. De esta forma, cuando un usuario usa un servicio de nube, Cloud Discovery solo registra un evento en lugar de varios eventos por cada página web. Puede administrar esta funcionalidad en la sección **Control Web**.

Supervisión de los servicios en la nube

Cuando un usuario comienza a usar un servicio en la nube, Kaspersky Endpoint Security registra dicho evento y crea una entrada en el informe. Cloud Discovery controla el uso del servicio en la nube en el navegador, así como en las aplicaciones correspondientes. Cloud Discovery controla el uso de los servicios en la nube en HTTP y HTTPS.

Cómo activar la supervisión de servicios en la nube en Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Protección de comunicaciones y web → Cloud Discovery**.

5. Active la opción **Cloud Discovery ACTIVADO**.

6. Guarde los cambios.

Como resultado, la aplicación reenvía información sobre los servicios en la nube que se están usando a Kaspersky Security Center. Puede ver la información sobre el uso de los servicios en la nube en informes. Si es necesario, puede bloquear el acceso a servicios en la nube.

Bloqueo del acceso a los servicios en la nube

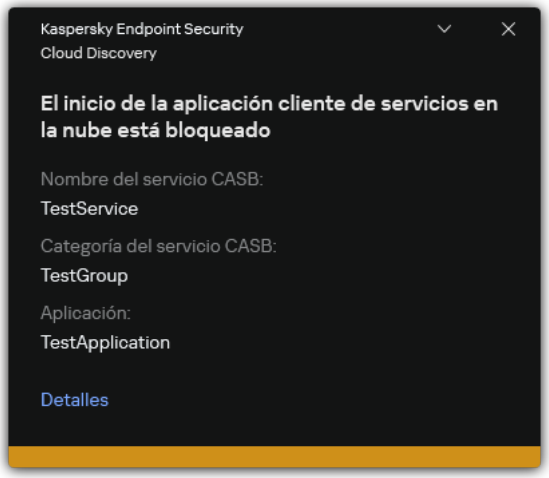
El bloqueo del acceso a servicios en la nube solo está disponible con la licencia de Kaspersky Next EDR Optimum y de XDR Expert. Esta función no está disponible para la licencia de Kaspersky Next EDR Foundations. Comparación de la funcionalidad de la aplicación según el tipo de licencia de Kaspersky Next, consulte la Ayuda de Kaspersky Next.

El administrador puede restringir el acceso de los usuarios a categorías de Cloud Discovery o a servicios en la nube individuales. De esta forma, el administrador puede permitir que solo se usen servicios en la nube seguros y evitar las filtraciones de datos. En Cloud Discovery aparece *información sobre el nivel de riesgo* de cada servicio en la nube. El nivel de riesgo ayuda a detectar servicios que no satisfacen los requisitos de seguridad de la organización.

El nivel de riesgo es una estimación, no implica ninguna afirmación sobre la calidad del servicio en la nube o sobre su proveedor. Es, simplemente, una recomendación de los expertos de Kaspersky.

Los niveles de riesgo de los servicios en la nube aparecen en la sección **Cloud Discovery** de la directiva, en la lista de todos los servicios de la nube controlados.

Otros componentes de Kaspersky Endpoint Security proporcionan protección ante amenazas y seguimiento de la actividad de usuarios sospechosos cuando usan servicios en la nube.



Notificación de Cloud Discovery

Cloud Discovery no bloquea las aplicaciones en la nube que se iniciaron antes que Kaspersky Endpoint Security.

Cómo bloquear el acceso a servicios en la nube en Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección de comunicaciones y web → Cloud Discovery**.
5. Active la opción **Cloud Discovery ACTIVADO**.

   Aparece una lista de los servicios en la nube. Los servicios en la nube se agrupan en categorías; por ejemplo, *Uso compartido de archivos*, *Programas de mensajería*, *Correo electrónico*. Los expertos de Kaspersky actualizan de forma periódica las categorías de Cloud Discovery y los servicios en la nube clasificados en las categorías. Kaspersky Endpoint Security actualiza el conjunto de categorías y servicios en la nube con las bases de datos de la aplicación.

6. Use el interruptor de la columna **Acceso** para configurar el acceso a los servicios en la nube.

7. Guarde los cambios.

Como resultado, la aplicación controla el uso del servicio en la nube en el navegador, así como en las aplicaciones correspondientes.

Zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza de manera independiente y tiene en cuenta las características de los objetos que se gestionan y de las aplicaciones que se instalan en el equipo. Puede que sea necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a ellos, si está seguro de que el objeto o la aplicación son inofensivos. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza, además de la zona de confianza general en una directiva.

A partir de Kaspersky Endpoint Security 12.5 para Windows, puede añadir telemetría EDR a la zona de confianza. Esto permite optimizar los datos que la aplicación envía al servidor de recopilación telemetría para la solución Kaspersky Anti Targeted Attack Platform (EDR).

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores.

A partir de Kaspersky Endpoint Security 12.8 para Windows, puede instalar la aplicación en modo Light Agent para proteger los entornos virtuales. Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware.

Creación de una exclusión del análisis

Una *exclusión de análisis* es un conjunto de condiciones que se deben cumplir para que Kaspersky Endpoint Security no analice un objeto en busca de virus u otras amenazas. Las exclusiones del análisis permiten utilizar de manera segura software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario. Estas aplicaciones no tienen necesariamente fines maliciosos, pero los atacantes pueden aprovecharlas. Para obtener información detallada sobre las aplicaciones legítimas que los intrusos pueden usar para poner en peligro el equipo o los datos del usuario, visite el sitio web de la Enciclopedia de Kaspersky.

Es posible que Kaspersky Endpoint Security bloquee estas aplicaciones. Para evitar que se bloqueen, puede configurar las exclusiones del análisis para las aplicaciones en uso. Para ello, añada el nombre o la máscara de nombre que figura en la Enciclopedia de Kaspersky a la zona de confianza. Por ejemplo, a menudo se utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security identifica esta actividad como sospechosa y puede que la bloquee. Para evitar el bloqueo de la aplicación, cree una exclusión del análisis con el nombre o la máscara de nombre que se muestra en la Enciclopedia de Kaspersky.

Si la aplicación que recopila la información y la envía para procesarse se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar que esto ocurra, puede excluir la aplicación del análisis mediante la configuración de Kaspersky Endpoint Security como se describe en este documento.

Los siguientes componentes de aplicaciones y tareas que el administrador del sistema configure pueden utilizar exclusiones del análisis:

- Detección de comportamiento.
- Prevención de exploits.
- Prevención de intrusiones en el host.
- Protección frente a amenazas en archivos.
- Protección frente a amenazas web.
- Protección frente a amenazas en el correo.
- Tarea *Análisis antimalware*.

Kaspersky Endpoint Security no analiza un objeto si la unidad de disco o la carpeta que contiene este objeto se incluyen en la cobertura del análisis al inicio de una de las tareas de análisis. Sin embargo, no se aplica la exclusión del análisis cuando se inicia una tarea de análisis personalizado para este objeto en particular.

Cómo crear una exclusión del análisis en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones y tipos de objeto**.
5. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Exclusiones del análisis**, haga clic en el botón **Configuración**.

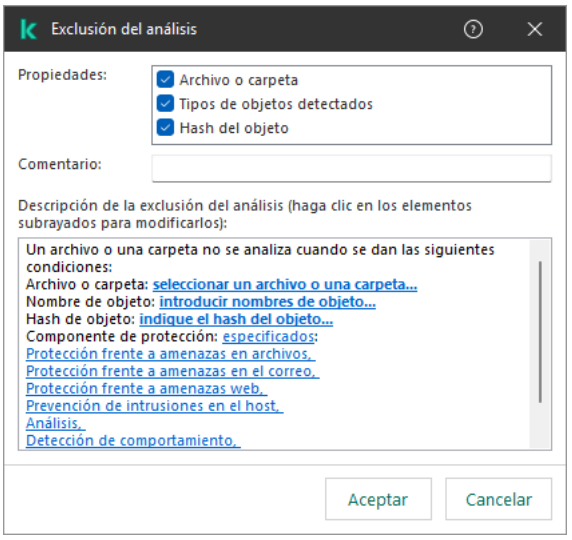
   Esto abre una ventana que incluye una lista de exclusiones.
6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.
7. Seleccione la casilla de verificación **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si se desmarca esta casilla, Kaspersky Endpoint Security ocultará la lista consolidada de exclusiones del análisis en la interfaz de usuario de la aplicación.

8. Haga clic en **Añadir** y seleccione una acción:

- **Categoría**. Puede agrupar las exclusiones del análisis en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una exclusión del análisis a la misma.
- **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva exclusión de análisis a la raíz de la lista.
- **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *exclusiones de análisis predefinidas*. También se han añadido exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar exclusiones del análisis predefinidas según el propósito del servidor protegido.
- **Nueva exclusión en la categoría seleccionada**. Para añadir una nueva exclusión de análisis a una categoría específica, seleccione una categoría.

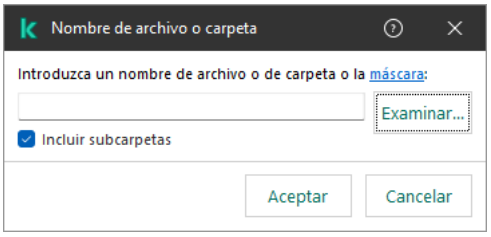
9. Para excluir un archivo o una carpeta del análisis:



Configuración de exclusión

a. En el bloque **Propiedades**, seleccione la casilla de verificación **Archivo o carpeta**.

b. Haga clic en el enlace que aparece abajo para abrir la ventana **Nombre de archivo o carpeta**.



Seleccionar archivo o carpeta

a. Escriba el nombre del archivo o carpeta (o la máscara de este nombre), o haga clic en **Examinar** y seleccione el archivo o carpeta en el árbol de carpetas.

Usar máscaras:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `?:\Users\*\Folder\`.

Kaspersky Endpoint Security admite variables de entorno

Puede excluir carpetas de red. Para hacer esto, introduzca la ruta a la carpeta de red manualmente (por ejemplo, `\\Network Share\*`).

> Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de exclusiones usando la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

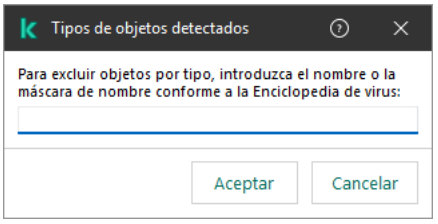
b. Si es necesario, desactive la funcionalidad **Incluir subcarpetas**. Si esta funcionalidad está activada, la aplicación no analiza los archivos de todas las subcarpetas. Si esta funcionalidad está desactivada, la aplicación excluye del alcance del análisis únicamente la carpeta seleccionada. Esta opción está activada de forma predeterminada.

c. Guarde los cambios.

10. Para excluir objetos que tengan un nombre específico del análisis:

    a. En el bloque **Propiedades**, seleccione la casilla de verificación **Tipos de objetos detectados**.

    b. Haga clic en el enlace que aparece abajo para abrir la ventana **Tipos de objetos detectados**.



Seleccionar objeto

    a. Introduzca el nombre del objeto según la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

    b. Guarde los cambios.

11. Si desea excluir un archivo individual de los análisis:

    a. En el bloque **Propiedades**, seleccione la casilla de verificación **Hash del objeto**.

    b. Haga clic en el enlace que aparece abajo para abrir la ventana **Hash del objeto**.



Seleccionar archivo

    a. Introduzca el hash del archivo o seleccione el archivo haciendo clic en el botón **Examinar**.

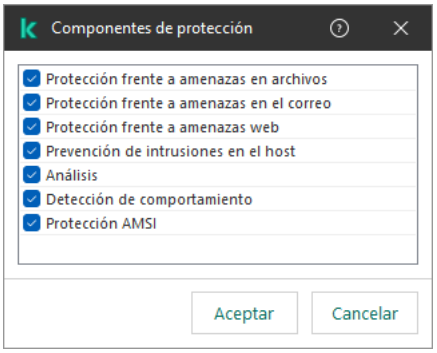
    Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.

    b. Guarde los cambios.

12. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

13. Especifique los componentes de Kaspersky Endpoint Security que van a emplearse en la exclusión del análisis:

    a. Haga clic en el enlace que aparece abajo para abrir la ventana **Componentes de protección**.



Seleccionar componentes de protección

    a. Seleccione las casillas de verificación situadas junto a los componentes a los cuales se debe aplicar la exclusión del análisis.

    Si especifica componentes en la configuración de la exclusión, esta se aplicará solo en los análisis que realicen esos componentes de Kaspersky Endpoint Security.

    Si no especifica ningún componente en la configuración de la exclusión, esta se aplicará en los análisis que realicen todos los componentes de Kaspersky Endpoint Security.

14. Haga clic en **Aceptar**.

    La nueva exclusión se añadirá a la lista. Puede desactivar la exclusión en cualquier momento utilizando la casilla de verificación situada junto al objeto.

15. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo crear una exclusión del análisis en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Zona de confianza**.

5. En la ventana que se abre, haga clic en el vínculo **Exclusiones del análisis antimalware**.

6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.

7. Seleccione la casilla de verificación **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si se desmarca esta casilla, Kaspersky Endpoint Security ocultará la lista consolidada de exclusiones del análisis en la interfaz de usuario de la aplicación.

8. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una exclusión del análisis a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva exclusión de análisis a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *exclusiones de análisis predefinidas*. También se han añadido exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar exclusiones del análisis predefinidas según el propósito del servidor protegido.

   Para añadir una nueva exclusión de análisis a una categoría específica, active la casilla de verificación situada junto a esa categoría y seleccione la opción **Nueva exclusión**.

9. Seleccione cómo desea añadir la exclusión: **Ruta al archivo o carpeta**, **Tipo de objeto** o **Hash del objeto**.

10. Para excluir un archivo o una carpeta del análisis, introduzca la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara:

    - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
    - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

      Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `?:\Users\*\Folder\`.

      Puede excluir carpetas de red. Para hacer esto, introduzca la ruta a la carpeta de red manualmente (por ejemplo, `\\Network Share\*`).

11. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Tipo de objeto**, introduzca el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

12. Si desea excluir un archivo individual de los análisis, introduzca el hash del archivo en el campo **Hash del objeto**.

    Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.

13. En el bloque **Aplicar exclusión a**, seleccione los componentes a los que desea que se aplique la exclusión del análisis.

14. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

15. Haga clic en **Aceptar**.

    La nueva exclusión se añadirá a la lista. Puede utilizar el interruptor para detener una exclusión en cualquier momento.

16. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

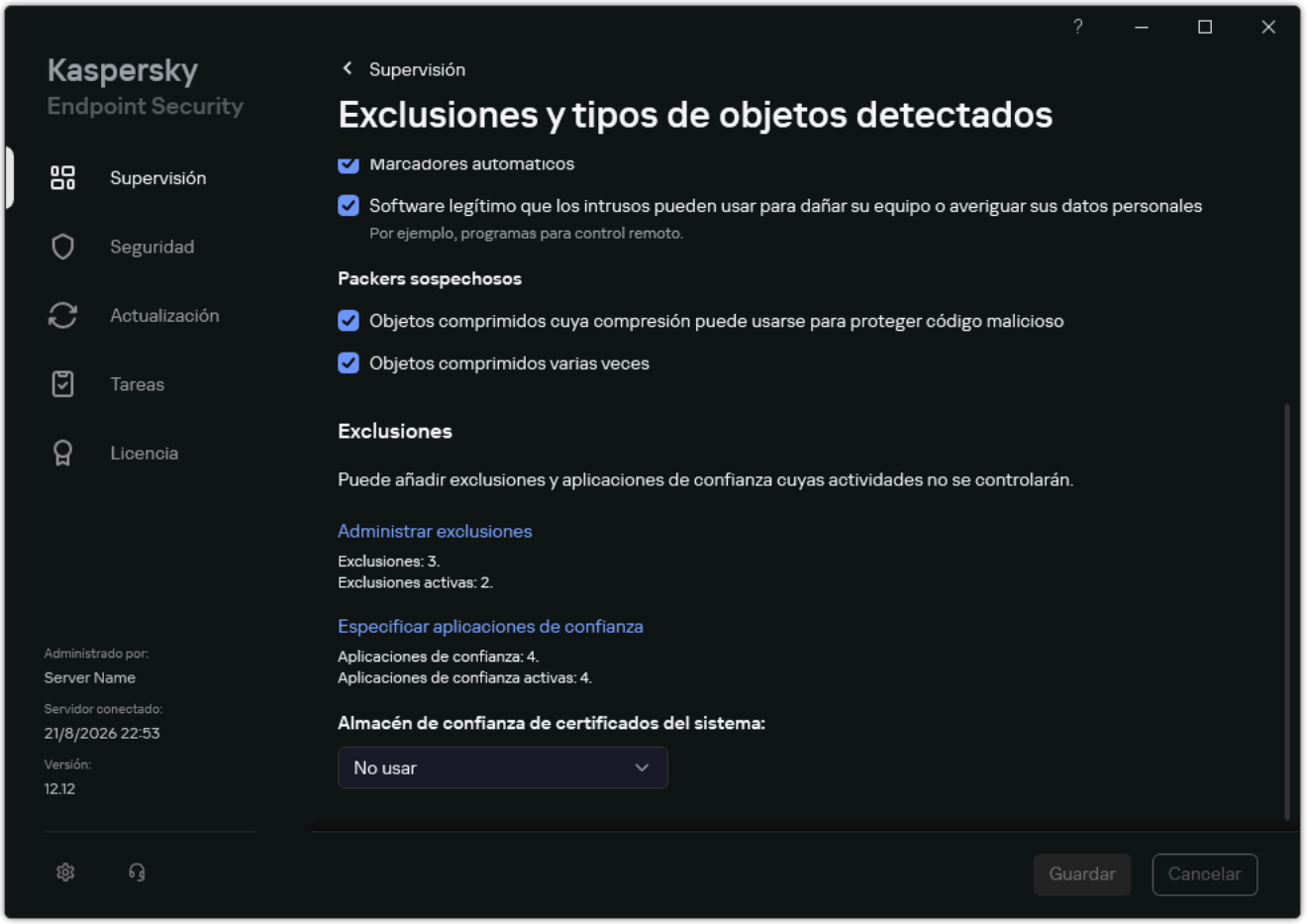
Cómo crear una exclusión del análisis en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.

3. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.

> Kaspersky Endpoint Security oculta la lista de exclusiones del análisis en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las exclusiones del análisis en la consola (símbolo de "candado cerrado") y las exclusiones del análisis locales están prohibidas (la casilla de verificación **Permitir el uso de exclusiones locales** se encuentra desactivada).



Configuración de exclusiones

4. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una exclusión del análisis a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva exclusión de análisis a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *exclusiones de análisis predefinidas*. También se han añadido exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar exclusiones del análisis predefinidas según el propósito del servidor protegido.

   Para añadir una nueva exclusión de análisis a una categoría específica, active la casilla de verificación situada junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Si desea excluir un archivo o carpeta de los análisis, seleccione el archivo o carpeta haciendo clic en el botón **Examinar**.

   También puede ingresar la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara:

   - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
   - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

     Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `?:\Users\*\Folder\`.

     Puede excluir carpetas de red. Para hacer esto, introduzca la ruta a la carpeta de red manualmente (por ejemplo, `\\Network Share\*`).

6. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Tipos de objetos detectados**, introduzca el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

7. Si desea excluir un archivo individual de los análisis, introduzca el hash del archivo en el campo **Hash de objeto**.

   Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.

8. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión del análisis.

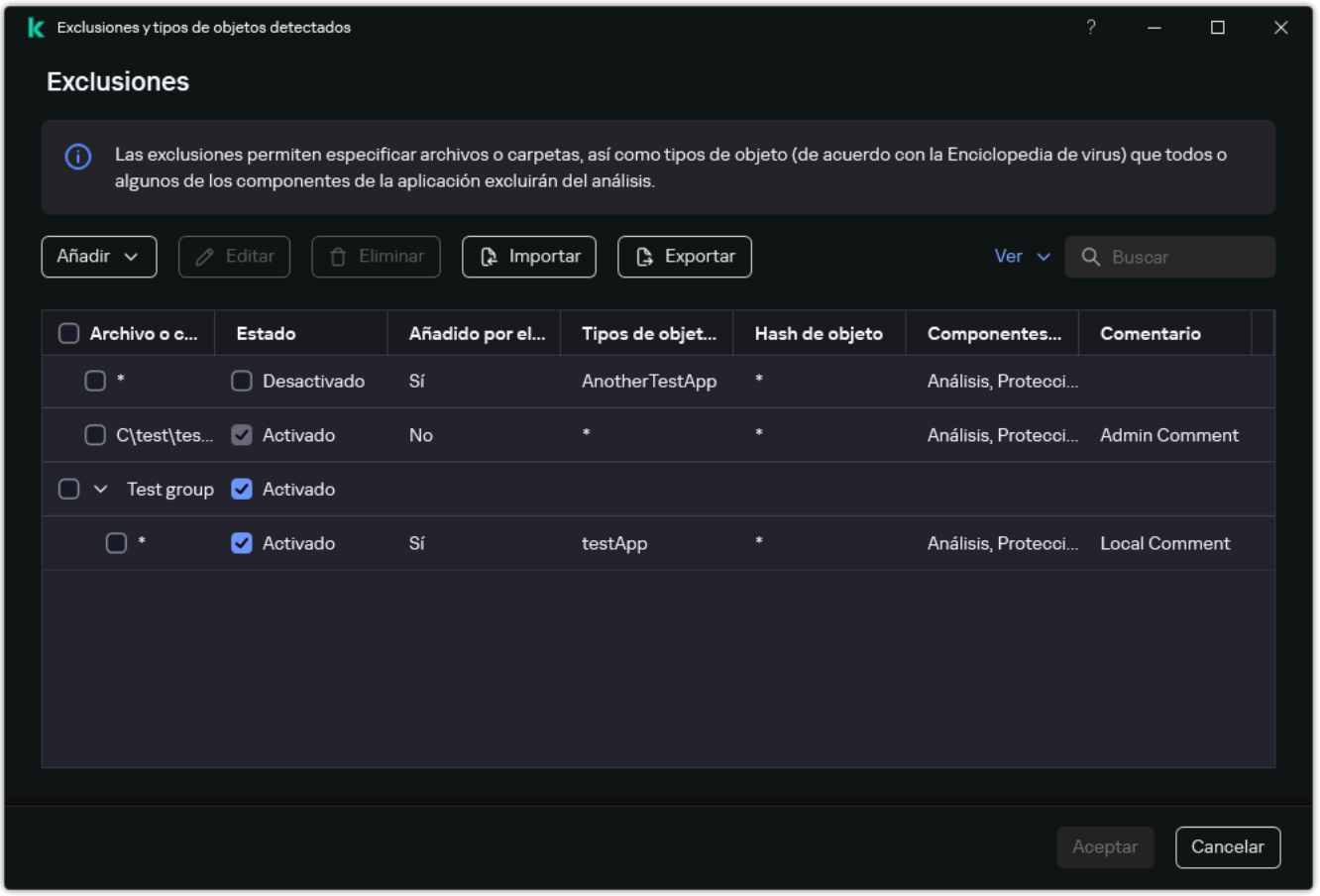
9. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

10. Seleccione el estado **Activo** para la exclusión.

11. Haga clic en **Añadir**.

    La nueva exclusión se añadirá a la lista. Puede desactivar la exclusión en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

12. Guarde los cambios.



Lista de exclusiones

Ejemplos de máscara de ruta:

Recomendamos especificar rutas relativas en lugar de rutas absolutas. Esto permite excluir no solo los objetos del sistema de archivos, sino también los objetos sin archivos. Por ejemplo, `*\Program Files (x86)\Folder\Subfolder`.

Rutas a los archivos de cualquier carpeta:

- La máscara `*.exe` comprende las rutas a todos los archivos de extensión exe.
- La máscara `example*` comprende las rutas a todos los archivos de nombre EXAMPLE.

Rutas a los archivos de una carpeta específica:

- La máscara `C:\dir\*.*` comprende las rutas a todos los archivos de la carpeta `C:\dir\`, pero no a los de las subcarpetas de `C:\dir\`.
- La máscara `C:\dir\*` incluirá todas las rutas a los archivos de la carpeta `C:\dir\`, incluidas las subcarpetas.
- La máscara `C:\dir\` incluirá todas las rutas a los archivos de la carpeta `C:\dir\`, incluidas las subcarpetas.
- La máscara `C:\dir\*.exe` comprende las rutas a todos los archivos de extensión EXE almacenados en `C:\dir\`, pero no a los de las subcarpetas de `C:\dir\`.
- La máscara `C:\dir\test` comprende las rutas a todos los archivos de nombre "test" almacenados en `C:\dir\`, pero no a los almacenados en las subcarpetas de `C:\dir\`.
- La máscara `C:\dir\*\test` comprende las rutas a todos los archivos de nombre "test" almacenados en C:\dir\ y en las subcarpetas de `C:\dir\`.
- La máscara `C:\dir1\*\dir3\` comprende todas las rutas a los archivos en las subcarpetas dir3 que estén un nivel dentro de la carpeta `C:\dir1\`.
- La máscara `C:\dir1\**\dirN\` comprende todas las rutas a los archivos en las subcarpetas dirN en la carpeta `C:\dir1\` en cualquier nivel.

Rutas a los archivos de cualquier carpeta que tenga un nombre específico:

- La máscara `dir\*.*` comprende todas las rutas a archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*` comprende todas las rutas a archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\` comprende todas las rutas a archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*.exe` comprende las rutas a todos los archivos de extensión EXE almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\test` comprende las rutas a todos los archivos de nombre "test" almacenados en carpetas de nombre "dir", pero no a los almacenados en subcarpetas de esas carpetas.

Crear una exclusión por tipo de objetos detectados

Kaspersky Endpoint Security clasifica los objetos detectados de la siguiente manera:

- **Virus y gusanos**

  Subcategoría: Virus y gusanos Viruses_and_Worms)

  Nivel de peligrosidad: Alto

  Los gusanos y virus tradicionales ejecutan acciones que no autoriza el usuario. Pueden crear copias de ellos mismos, que son capaces de reproducirse.

Virus tradicionales

Cuando un virus tradicional se introduce en un equipo, lo que hace es infectar un archivo, activarse, realizar acciones maliciosas y añadir copias de sí mismo a otros archivos.

Un virus tradicional se multiplica únicamente en los recursos locales del equipo; no puede penetrar en otros equipos por sí mismo. Solo puede pasar a otro equipo si añade una copia de sí mismo a un archivo almacenado en una carpeta compartida o un CD introducido, o si el usuario reenvía un mensaje de correo electrónico con un archivo infectado como adjunto.

Un código de virus tradicional puede penetrar en varias zonas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de secuencias de scripts* y *virus de macros*.

Los virus pueden infectar los archivos a través de una gran diversidad de técnicas. Los virus de *Overwriting* escriben su código sobre el código del archivo que se infecta, con lo que se borra el contenido del mismo. El archivo infectado deja de funcionar y no se puede restaurar. Los virus *Parasitic* modifican los archivos y los dejan parcial o completamente funcionales. Los virus *Companion* no modifican los archivos, pero crean duplicados. Cuando se abre un archivo infectado, se inicia un duplicado de él (lo que es un virus en realidad). También existen los siguientes tipos de virus: virus *Link*, *virus para archivos OBJ*, *virus para archivos LIB*, *virus para código fuente* y muchos otros.

Gusano

Como ocurre con los virus tradicionales, el código de los gusanos está diseñado para infiltrarse en un equipo, activarse y realizar acciones maliciosas. La denominación de los gusanos se debe a su capacidad para "arrastrarse" de un equipo a otro y para propagar copias a través de diversos canales sin el permiso del usuario.

La principal característica que permite distinguir entre varios tipos de gusanos es la forma en que se propagan. En la siguiente tabla, se ofrece una descripción general de varios tipos de gusanos, que se clasifican por el modo en que se propagan.

Formas de propagación de los gusanos

Tipo	Nombre	Descripción
Gusano de correo electrónico	Email-Worm	Se propagan a través del correo electrónico. Un mensaje de correo electrónico infectado contiene un archivo adjunto con una copia de un gusano o un enlace a un archivo que se ha cargado en un sitio que se puede haber pirateado o creado exclusivamente para dicho propósito. Al abrir el archivo adjunto, se activa el gusano. Al hacer clic en el enlace, descargar y, a continuación, abrir el archivo, el gusano también comienza a realizar sus acciones maliciosas. Después, continúa propagando copias de sí mismo y buscando otras direcciones de correo electrónico, a las que envía mensajes infectados.
Gusano de mensajería instantánea	Gusanos de cliente de MI	Se propagan a través de clientes de MI. Por lo general, dichos gusanos envían mensajes que contienen un enlace a un archivo con una copia del gusano en un sitio web; para ello usan las listas de contactos del usuario. Cuando el usuario descarga y abre el archivo, el gusano se activa.
Gusano IRC	Gusanos de chat de Internet	Se propagan a través de Internet Relay Chats, sistemas de servicios que permiten la comunicación con otros usuarios a través de Internet en tiempo real. Estos gusanos publican un archivo con una copia de ellos mismos o un enlace a un archivo en un chat de Internet. Cuando el usuario descarga y abre el archivo, el gusano se activa.
Gusano de red	Gusanos de red	Estos gusanos se propagan a través de redes de equipos. A diferencia de otros tipos de gusanos, un gusano de red tradicional se propaga sin intervención del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red especialmente creado (exploit) que contiene el código del gusano o una parte de este. Si un equipo "vulnerable" se encuentra en la red, recibe dicho paquete de red. Cuando el gusano penetra completamente en el equipo, se activa.

Tipo	Nombre	Descripción
Gusano de P2P	Gusanos de redes de uso compartido de archivos	Se propagan a través de las redes de uso compartido de archivos entre pares. Para penetrar en una red P2P, el gusano se copia en una carpeta de uso compartido de archivos, que se ubica normalmente en el equipo del usuario. La red P2P muestra información sobre este archivo para que el usuario pueda "encontrar" el archivo infectado en la red al igual que cualquier otro archivo y, a continuación, descargarlo y abrirlo. Los gusanos más sofisticados simulan el protocolo de red de una red P2P determinada: devuelven respuestas positivas a consultas de búsqueda y ofrecen sus copias para descargarlas.
Gusano	Otros tipos de gusanos	Entre otros tipos de gusanos, se incluyen: • Gusanos que propagan copias de sí mismos a través de recursos de red. Con las funciones del sistema operativo, pueden analizar las carpetas disponibles de la red, conectarse a equipos en Internet e intentar obtener acceso completo a sus unidades de disco. A diferencia de los tipos de gusanos descritos previamente, los otros tipos de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano. • Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono móvil a otro).

- **Troyanos (incluye ransomware)**

  Subcategoría: Troyanos

  Nivel de peligrosidad: Alto

  A diferencia de los gusanos y los virus, los troyanos no se replican. Por ejemplo, se introducen en un equipo a través del correo electrónico o un navegador cuando el usuario visita una página web infectada. Los troyanos se inician con intervención del usuario. Comienzan a realizar acciones maliciosas inmediatamente después de que se inician.

  Los distintos troyanos se comportan de forma diferente en los equipos infectados. Las funciones principales de los troyanos consisten en bloquear, modificar o destruir información, y desactivar equipos o redes. Los troyanos también pueden recibir o enviar archivos, ejecutarlos, mostrar mensajes en la pantalla, solicitar páginas web, descargar e instalar programas y reiniciar el equipo.

  Los piratas usan conjuntos de diversos troyanos con frecuencia.

  Los distintos tipos de comportamiento de los troyanos se describen en la tabla siguiente.

  Tipos de comportamiento de los troyanos en un equipo infectado

Tipo	Nombre	Descripción
Trojan-ArcBomb	Troyanos: "archivos bomba"	Al descomprimirlos, estos archivos aumentan de tamaño de tal forma que el funcionamiento del equipo se ve afectado. Cuando el usuario intenta descomprimir un archivo de esas características, es posible que el equipo se vea ralentizado o se congele; el disco duro puede llenarse de datos "vacíos". Los "archivos bomba" son especialmente peligrosos para los servidores de correo y archivos. Si el servidor usa un sistema automático para procesar la información entrante, un "archivo bomba" puede detener el servidor.
Backdoor	Troyanos para administración remota	Se considera que son los troyanos más peligrosos. En sus funciones, se parecen a las aplicaciones de administración remota que se instalan en los equipos. Estos programas se instalan en un equipo sin que el usuario se dé cuenta de ello, lo que permite que el intruso administre el equipo de forma remota.
Troyano	Troyanos	Incluyen las siguientes aplicaciones maliciosas: • **Troyanos tradicionales**. Estos programas solo ejecutan las funciones principales de los troyanos: bloqueo, modificación o destrucción de información y desactivación de equipos o redes. No cuentan con funciones avanzadas, a diferencia de otros tipos de troyanos descritos en la tabla. • **Troyanos versátiles**. Estos programas tienen funciones avanzadas comunes en varios tipos de troyanos.
Trojan-Ransom	Troyanos de rescate	Toman como "rehén" la información del usuario para modificarla, bloquearla o afectar al funcionamiento del equipo de modo que el usuario pierda la capacidad de usar la información. El intruso pide un rescate al usuario y le promete enviar una aplicación que restaure el rendimiento del equipo y los datos que estaban almacenados en él.

Tipo	Nombre	Descripción
Trojan-Clicker	Troyanos de clic	Acceden a las páginas web desde el equipo del usuario, ya sea enviando comandos a un navegador o cambiando las direcciones web que se especifican en los archivos del sistema operativo. Con estos programas, los intrusos perpetrarán ataques de red y aumentarán las visitas al sitio web mediante un mayor número de visualizaciones de anuncios publicitarios.
Trojan-Downloader	Descargador de troyanos	Acceden a la página web del intruso, descargan otras aplicaciones maliciosas desde ella y las instalan en el equipo del usuario. Pueden contener el nombre de archivo de la aplicación maliciosa que se va a descargar o recibirla desde la página web a la que se accede.
Trojan-Dropper	Troyanos lanzadera	Contienen otros troyanos que instalan en el disco duro y después se instalan. Los intrusos pueden usar programas del tipo Trojan Dropper para los siguientes propósitos: • Instalar una aplicación maliciosa sin que el usuario se dé cuenta: los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (pueden, por ejemplo, advertir sobre la existencia de un archivo dañado o sobre incompatibilidades con el sistema operativo). • Para proteger a otra aplicación maliciosa y evitar que se detecte: no todo el software antivirus puede detectar una aplicación maliciosa en una aplicación del tipo Trojan Dropper.
Trojan-Notifier	Troyanos de notificación	Le informan al atacante que el equipo infectado está accesible y le envían información: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso a través del correo electrónico o el FTP, mediante la página web del intruso o de otro modo. Los programas del tipo Trojan Notifier se usan normalmente como conjuntos compuestos de varios troyanos. Notifican al intruso de que se han instalado correctamente otros troyanos en el equipo del usuario.
Trojan-Proxy	Proxies de troyanos	Permiten al intruso acceder de forma anónima a las páginas web mediante el equipo del usuario; se usan normalmente para enviar correo no deseado.
Trojan-PSW	Software de robo de contraseñas	El software de robo de contraseñas es un tipo de troyano que roba cuentas de usuario, como datos de registro de software. Estos troyanos buscan datos confidenciales en los archivos del sistema y en el Registro, y los envían al "agresor" por correo electrónico, el FTP o mediante acceso a la página web del intruso, o de cualquier otro modo. Algunos de estos troyanos están clasificados en los distintos tipos que se describen en la tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan en Internet (Trojan-GameThief).
Trojan-Spy	Troyanos espía	Espían a los usuarios con el fin de recopilar información sobre las acciones que el usuario lleva a cabo cuando utiliza el equipo. Pueden interceptar los datos que el usuario introduce en el teclado, tomar instantáneas o recopilar listas de aplicaciones activas. Una vez que reciben la información, la transfieren al intruso a través de correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo.
Trojan-DDoS	Troyanos atacantes de redes	Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS). Con frecuencia, los piratas infectan diversos equipos con estos programas, de modo que puedan usar los equipos para atacar un solo servidor a la vez. Los programas de DoS perpetran los ataques desde un solo equipo con conocimiento del usuario. Los programas DDoS (Distributed DoS) perpetran los ataques distribuidos desde varios equipos sin que el usuario del equipo infectado lo perciba.
Trojan-IM	Troyanos que roban información de los usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de usuarios de programas de mensajería instantánea. Transfieren los datos al intruso mediante correo electrónico o FTP, accediendo a la página web del intruso o de otro modo.
Rootkit	Rootkits	Enmascaran otras aplicaciones maliciosas y su actividad, con lo que prolongan la persistencia de las aplicaciones en el sistema operativo. Además, pueden ocultar archivos, procesos en la memoria infectada del equipo o claves del registro que ejecutan aplicaciones maliciosas. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones del equipo del usuario y otros equipos de la red.
Trojan-SMS	Troyanos con formato de mensajes SMS	Infectan teléfonos móviles a través del envío de mensajes a números de teléfono de tarificación especial.
Trojan-GameThief	Troyanos que roban información de los usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, para después enviar estos datos al intruso mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo.

Tipo	Nombre	Descripción
Trojan-Banker	Troyanos que roban cuentas bancarias	Roban datos de cuentas bancarias o de sistemas de dinero electrónico y envían la información al hacker mediante su página web, por correo electrónico, por FTP o usando otros medios.
Trojan-Mailfinder	Troyanos que recopilan direcciones de correo electrónico	Recopilan direcciones de correo electrónico almacenadas en un equipo y las envían al intruso por correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado.

- **Herramientas maliciosas**

  Subcategoría: Herramientas maliciosas

  Nivel de peligrosidad: Medio

  A diferencia de otros tipos de software malicioso (malware), las herramientas maliciosas no llevan a cabo acciones inmediatamente después de que se inicien. Se pueden almacenar e iniciar de forma segura en el equipo del usuario. Los intrusos usan con frecuencia las funciones de estos programas para crear virus, gusanos y troyanos; perpetrar ataques de red en servidores remotos; piratear equipos o llevar a cabo otras acciones maliciosas.

  Varias funciones de herramientas maliciosas se agrupan por los tipos descritos en la tabla siguiente.

  Funciones de herramientas maliciosas

Tipo	Nombre	Descripción
Constructor	Constructores	Permiten la creación de nuevos virus, gusanos y troyanos. Algunos constructores cuentan incluso con una interfaz de ventanas estándar en la que el usuario puede seleccionar el tipo de aplicación maliciosa que creará, la forma de contrarrestar los depuradores y otras funciones.
Dos	Ataques de red	Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS).
Exploit	Exploits	Un *exploit* es un conjunto de datos o un código de programa que usa las vulnerabilidades de la aplicación en la que se procesa para llevar a cabo una acción maliciosa en un equipo. Por ejemplo, un exploit puede escribir o leer archivos, así como solicitar páginas web "infectadas". Los exploits utilizan las vulnerabilidades de distintas aplicaciones o servicios de red. Disfrazado como paquete de red, un exploit se transfiere a través de la red a diversos equipos. Busca equipos con servicios de red vulnerables. Un exploit en un archivo DOC usa las vulnerabilidades de un editor de textos. Puede comenzar a ejecutar las acciones preprogramadas por el pirata cuando el usuario abra el archivo infectado. Un exploit incrustado en un mensaje de correo electrónico busca vulnerabilidades en cualquier cliente de correo electrónico. Puede empezar a realizar acciones maliciosas en cuanto el usuario abra el mensaje infectado en este cliente de correo electrónico. Los Net-Worms se propagan por las redes mediante exploits. Los exploits Nuker son paquetes de red que desactivan equipos.
FileCryptor	Cifradores	Cifran otras aplicaciones maliciosas para ocultarlas frente a las aplicaciones antivirus.
Flooder	Programas para contaminar redes	Envían un gran número de mensajes a través de canales de red. Este tipo de herramientas incluye, por ejemplo, los programas que "contaminan" Internet Relay Chats. Las herramientas de tipo Flooder no incluyen programas que "contaminan" los canales que usa el correo electrónico, los clientes de MI y los sistemas de comunicación móvil. Estos programas se distinguen como los distintos tipos que se describen en esta tabla (Email-Flooder, IM-Flooder y SMS-Flooder).
HackTool	Herramientas de pirateo	Permiten hackear el equipo en el que están instalados o atacar a otro equipo (por ejemplo, añadiendo nuevas cuentas de sistema sin el permiso del usuario o borrando los registros del sistema para ocultar los rastros de su presencia en el sistema operativo). Este tipo de herramientas incluye sniffers, que incluyen funciones maliciosas, como la interceptación de contraseñas. Los sniffers son programas que permiten la visualización del tráfico de la red.
Hoax	Hoaxes	Avisan al usuario con mensajes parecidos a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario que el disco se ha formateado, aunque no haya sucedido en realidad.
Spoofer	Herramientas de spoofing	Envían mensajes y solicitudes de red con una dirección de remitente falsa. Los intrusos usan herramientas del tipo Spoofer para pasar como los verdaderos remitentes del mensaje, por ejemplo.

Tipo	Nombre	Descripción
VirTool	Herramientas que modifican aplicaciones maliciosas	Permiten la modificación de otros programas de software malicioso (malware) para ocultarlos de las aplicaciones antivirus.
Email-Flooder	Programas que "contaminan" direcciones de correo electrónico	Envían diversos mensajes a varias direcciones de correo electrónico y las "contaminan" de ese modo. Un gran volumen de mensajes entrantes impide a los usuarios ver los mensajes útiles en la bandeja de entrada.
IM-Flooder	Programas que "contaminan" el tráfico de clientes de MI	Inundan a los usuarios de clientes de MI con mensajes. El gran volumen de mensajes impide que los usuarios vean los mensajes entrantes útiles.
SMS-Flooder	Programas que "contaminan" el tráfico con mensajes SMS	Envían un gran número de mensajes SMS a teléfonos móviles.

- **Software publicitario**

  Subcategoría: Software publicitario (adware)

  Nivel de peligrosidad: Medio

  El software publicitario (adware) muestra información publicitaria al usuario. El software publicitario (adware) muestra anuncios publicitarios en la interfaz de otros programas y dirige las búsquedas a páginas web de publicidad. Algunos de ellos recopilan información de marketing del usuario y la envían al desarrollador. Esta información puede incluir los nombres de los sitios web que visita el usuario o el contenido de sus búsquedas. A diferencia de los programas del tipo Trojan-Spy, el software publicitario (adware) envía esta información al desarrollador con el permiso del usuario.

- **Marcadores automáticos**

  Subcategoría: Marcadores automáticos (Marcador).

  Nivel de peligrosidad: Medio

  Los marcadores automáticos pueden establecer subrepticiamente conexiones telefónicas mediante un módem.

- **Software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales**

  Subcategoría: Software legítimo que pueden utilizar los intrusos para dañar su equipo o datos personales.

  Nivel de peligrosidad: Medio

  La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de internet para FTP, HTTP y Telnet.

  No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
Client-IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).
Descargador	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
RemoteAdmin	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y gestionarlo. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.
Server-Web	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
NetTool	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
Client-P2P	Clientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
Client-SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
WebToolbar	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.

- **Objetos comprimidos cuya compresión puede usarse para proteger código malicioso**

  Subcategoría: Archivos comprimidos que pueden causar daños.

  Nivel de peligrosidad: Medio.

  El archivo se comprime con un compresor especial que se utiliza para comprimir malware: virus, gusanos, troyanos. Kaspersky Endpoint Security analiza el módulo de descompresión de los archivos SFX (autoextraíbles).

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen utilizando compresores especiales. Los expertos de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

- **Objetos comprimidos varias veces**

  Subcategoría: Archivos multicomprimidos.

  Nivel de peligrosidad: Medio.

  El archivo se comprime con uno o más compresores tres o más veces.

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos pueden comprimir un archivo varias veces. Kaspersky Endpoint Security analiza archivos comprimidos.

De forma predeterminada, Kaspersky Endpoint Security detecta todo tipo de objetos. Recomendamos dejar activada la detección de todo tipo de objetos para mejorar la seguridad del equipo. Si está utilizando utilidades internas que la aplicación detecta como maliciosas, añada estas utilidades a una lista de exclusión, pero no desactive la detección de todo el tipo de objetos.

Cómo seleccionar tipos de objetos detectables en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
5. En el bloque **Tipos de objetos detectados**, haga clic en el botón **Configuración**.
6. En la ventana que se abre, seleccione las casillas de verificación de los tipos de objetos que desea que Kaspersky Endpoint Security detecte.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar los tipos de objetos detectables en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

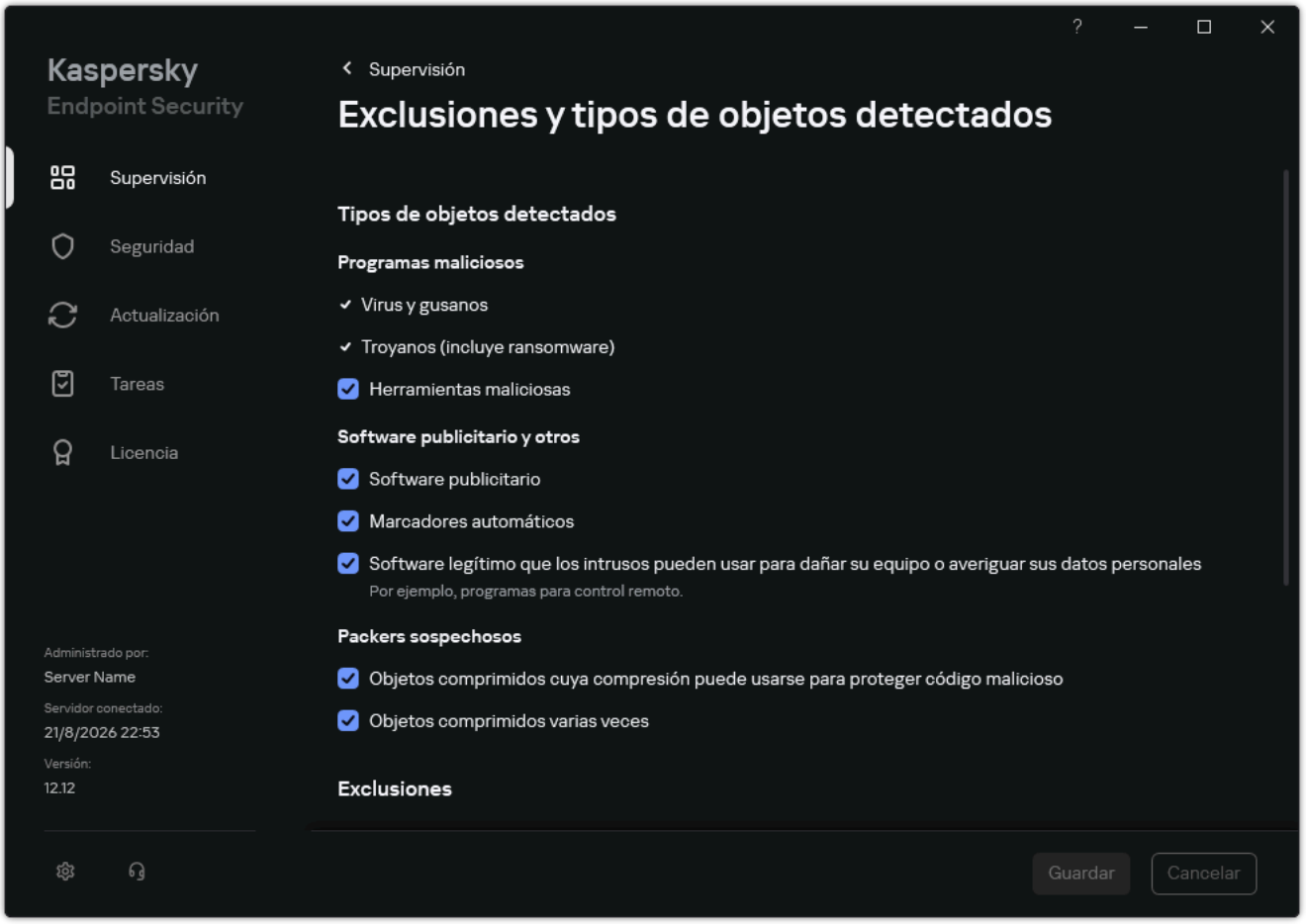
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Configuración de detección**.
5. En el bloque **Detección de otros tipos de objetos**, seleccione las casillas de verificación de los tipos de objetos que desea que Kaspersky Endpoint Security detecte.
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo seleccionar tipos de objetos detectables en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.

3. En el bloque **Tipos de objetos detectados**, seleccione las casillas de verificación de los tipos de objetos que desea que Kaspersky Endpoint Security detecte.

4. Guarde los cambios.



Tipos de objetos detectables

Edición de la lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de red y archivos (incluida la actividad maliciosa), así como el acceso al registro del sistema, no supervisa Kaspersky Endpoint Security. De forma predeterminada, Kaspersky Endpoint Security supervisa los objetos que el proceso de cualquier aplicación abre, ejecuta o guarda, y controla la actividad de todas las aplicaciones y el tráfico de red que generan. Una vez que se agrega una aplicación a la lista de aplicaciones de confianza, Kaspersky Endpoint Security deja de supervisar la actividad de la aplicación.

La diferencia entre las exclusiones de análisis y las aplicaciones de confianza es que, para las exclusiones, Kaspersky Endpoint Security no analiza los archivos, mientras que para las aplicaciones de confianza no controla los procesos iniciados. Si una aplicación de confianza crea un archivo malicioso en una carpeta que no está incluida en las exclusiones de análisis, Kaspersky Endpoint Security detectará el archivo y eliminará la amenaza. Si la carpeta se añade a las exclusiones, Kaspersky Endpoint Security omitirá este archivo.

Por ejemplo, si considera que los objetos que emplea el Bloc de notas estándar de Microsoft Windows son seguros, lo que significa que confía en esta aplicación, puede añadir el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza para que los objetos que use dicha aplicación no se supervisen. Esto aumentará el rendimiento del equipo, lo que resulta especialmente importante cuando se usan aplicaciones de servidor.

Además, algunas acciones que Kaspersky Endpoint Security clasifica como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de diferentes aplicaciones. Por ejemplo, la interceptación de texto que se escribe mediante el teclado es un proceso rutinario para intercambiadores de disposición del teclado automáticos (como Punto Switcher). Para tener en cuenta los detalles de este tipo de aplicaciones y excluir su actividad del proceso de análisis, le recomendamos que las agregue a la lista de aplicaciones de confianza.

Las aplicaciones de confianza ayudan a evitar problemas de compatibilidad entre Kaspersky Endpoint Security y otras aplicaciones (por ejemplo, el problema del análisis doble del tráfico de red de un equipo de terceros por parte de Kaspersky Endpoint Security y de otra aplicación antivirus).

Al mismo tiempo, el archivo ejecutable y el proceso de la aplicación de confianza sí que se analizan en busca de virus y otro software malicioso (malware). Puede excluirse completamente una aplicación del análisis de Kaspersky Endpoint Security gracias a las exclusiones del análisis.

Cómo añadir una aplicación a la lista de confianza en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
5. En el bloque **Exclusiones de análisis y aplicaciones de confianza → Aplicaciones de confianza**, haga clic en el botón **Configuración**.

   Esto abre una ventana que contiene una lista de aplicaciones de confianza.
6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de aplicaciones de confianza para todos los equipos de la empresa. Se fusionarán las listas de aplicaciones de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las aplicaciones de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar aplicaciones de confianza de la directiva principal.
7. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla de verificación está desactivada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Además, si se desmarca esta casilla, Kaspersky Endpoint Security ocultará la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación.
8. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una aplicación de confianza a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva aplicación de confianza a la raíz de la lista.

- **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *aplicaciones de confianza predefinidas*. También se han añadido aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar aplicaciones de confianza predefinidas según el propósito del servidor protegido.

- **Nueva exclusión en la categoría seleccionada**. Para añadir una nueva aplicación de confianza a una categoría específica, seleccione una categoría.

9. Seleccione los criterios de confianza:

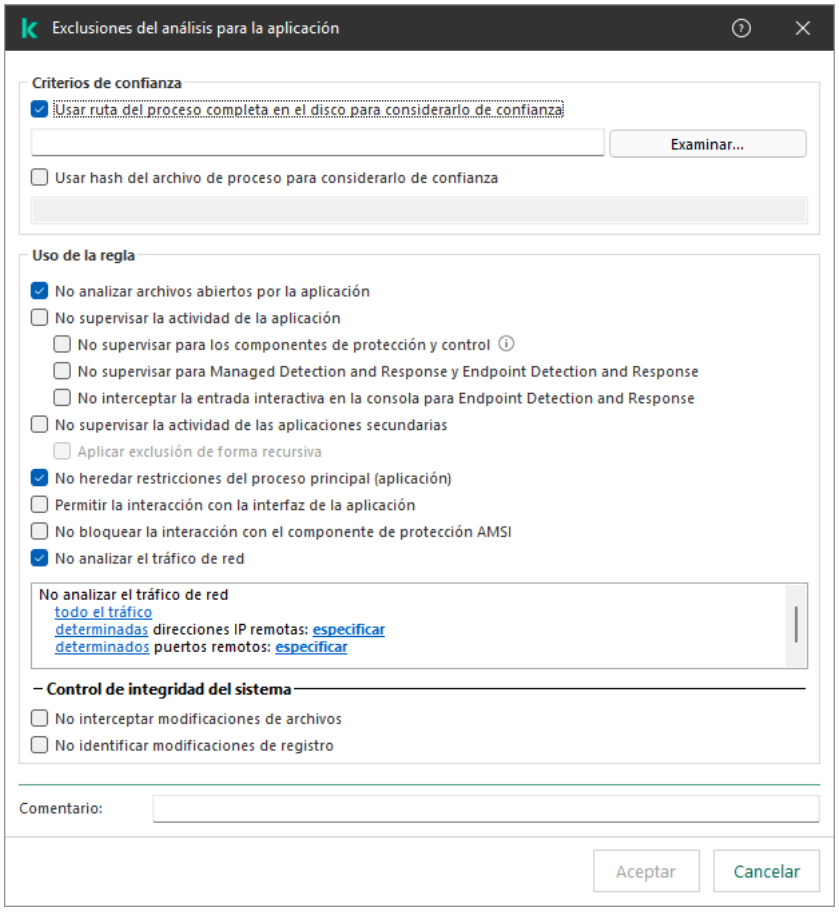
- **Usar ruta del proceso completa en el disco para considerarlo de confianza**. Introduzca la ruta al archivo ejecutable de la aplicación de confianza.

  Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

  Kaspersky Endpoint Security trata el nombre de archivo de una aplicación de confianza como sensible a mayúsculas y minúsculas. Si el nombre de archivo que introduzca presenta errores de mayúsculas y minúsculas, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

- **Usar hash del archivo de proceso para considerarlo de confianza**.

Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.



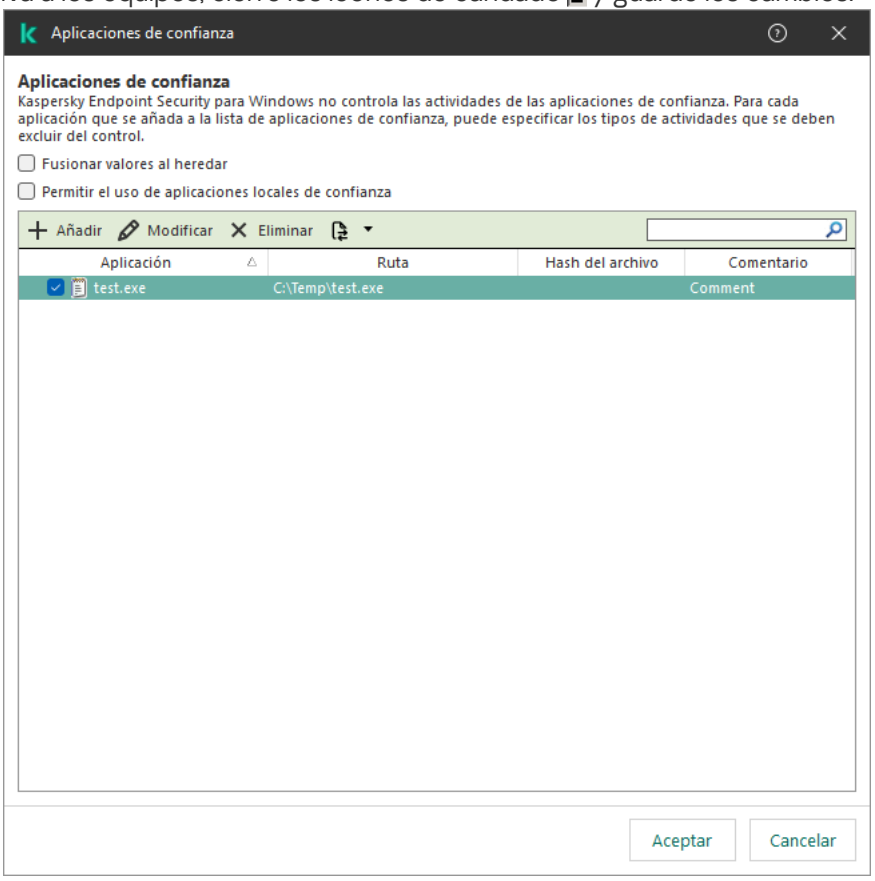
Configuración de la aplicación de confianza

10. Establezca la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).

11. Haga clic en **Aceptar**.

    La nueva aplicación de confianza se añadirá a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación situada junto al objeto.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.



Lista de aplicaciones de confianza

Cómo añadir una aplicación a la lista de confianza en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Zona de confianza**.
5. En la ventana que se abre, haga clic en el vínculo **Aplicaciones**.

   Esto abre una ventana que contiene una lista de aplicaciones de confianza.
6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de aplicaciones de confianza para todos los equipos de la empresa. Se fusionarán las listas de aplicaciones de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las aplicaciones de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar aplicaciones de confianza de la directiva principal.

7. Seleccione la casilla de verificación **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla de verificación está desactivada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Además, si se desmarca esta casilla, Kaspersky Endpoint Security ocultará la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación.

8. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una aplicación de confianza a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva aplicación de confianza a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *aplicaciones de confianza predefinidas*. También se han añadido aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar aplicaciones de confianza predefinidas según el propósito del servidor protegido.

   Para añadir una nueva aplicación de confianza a una categoría específica, active la casilla de verificación situada junto a esa categoría y seleccione la opción **Nueva exclusión**.

9. Seleccione los criterios de confianza:

   - **Ruta al archivo o carpeta**. Introduzca la ruta al archivo ejecutable de la aplicación de confianza.

     Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

     Kaspersky Endpoint Security trata el nombre de archivo de una aplicación de confianza como sensible a mayúsculas y minúsculas. Si el nombre de archivo que introduzca presenta errores de mayúsculas y minúsculas, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

   - **Hash de la aplicación**.

   Kaspersky Endpoint Security no admite la variable de entorno %userprofile% al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

10. Establezca la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).

11. Haga clic en **Aceptar**.

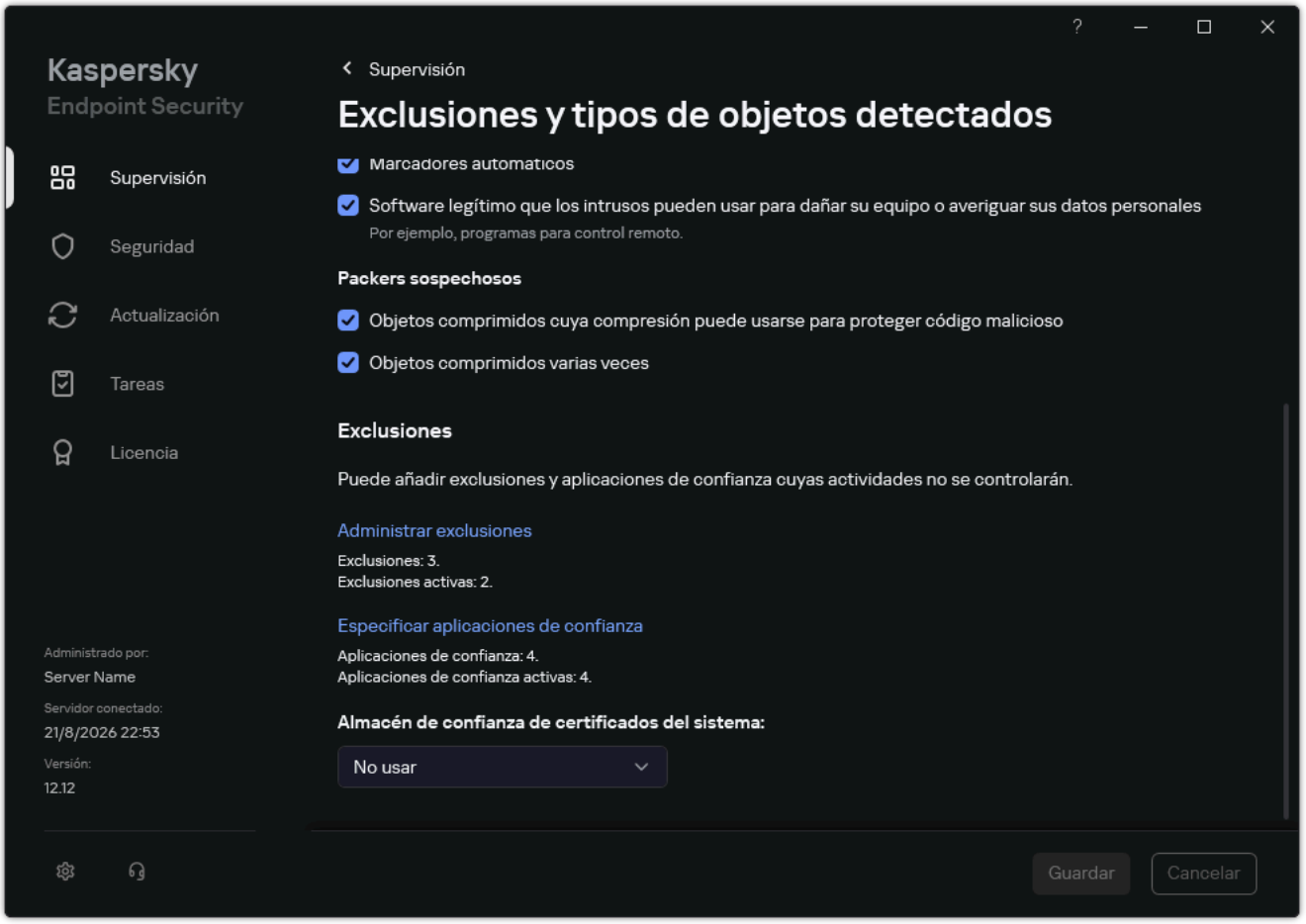
    La nueva aplicación de confianza se añadirá a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo añadir una aplicación a la lista de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.

Kaspersky Endpoint Security oculta la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las aplicaciones de confianza en la consola (símbolo de "candado cerrado") y las aplicaciones de confianza locales están prohibidas (la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** se encuentra desactivada).



Configuración de exclusiones

4. Haga clic en **Añadir** y seleccione una acción:

- **Categoría**. Puede agrupar las aplicaciones de confianza en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una aplicación de confianza a la misma.
- **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva aplicación de confianza a la raíz de la lista.
- **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *aplicaciones de confianza predefinidas*. También se han añadido aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar aplicaciones de confianza predefinidas según el propósito del servidor protegido.

Para añadir una nueva aplicación de confianza a una categoría específica, active la casilla de verificación situada junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Seleccione los criterios de confianza:

   - **Usar ruta del proceso completa en el disco para considerarlo de confianza**. Introduzca la ruta al archivo ejecutable de la aplicación de confianza.

     Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

     Kaspersky Endpoint Security trata el nombre de archivo de una aplicación de confianza como sensible a mayúsculas y minúsculas. Si el nombre de archivo que introduzca presenta errores de mayúsculas y minúsculas, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

   - **Usar hash del archivo de proceso para considerarlo de confianza**.

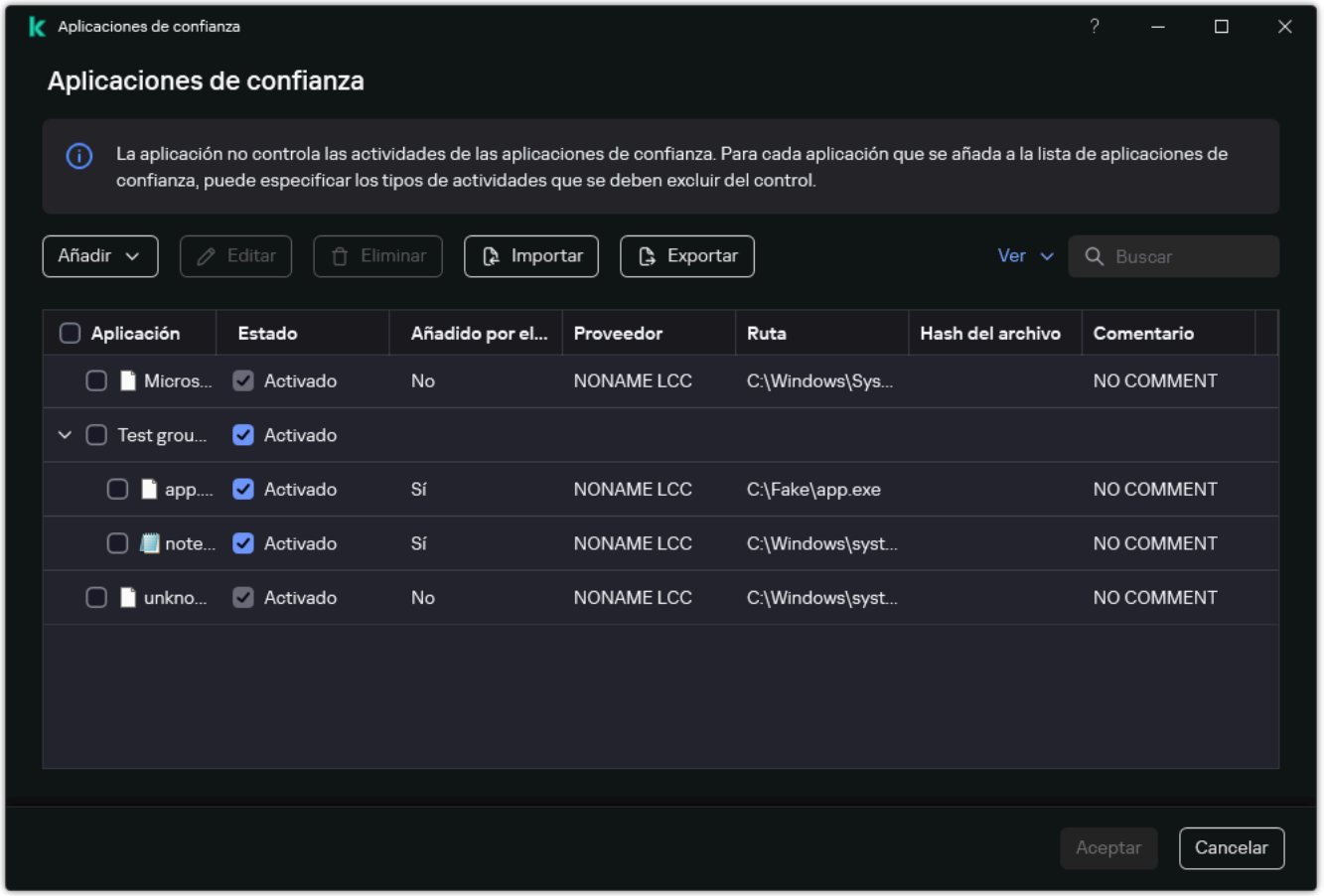
   Kaspersky Endpoint Security es compatible con variables de entorno y convierte la ruta en la interfaz local de la aplicación. En otras palabras, si introduce la ruta de archivo `%userprofile%\Documents\File.exe`, se añade un registro `C:\Users\Fred123\Documents\File.exe` en la interfaz local de la aplicación para el usuario Fred123. En consecuencia, Kaspersky Endpoint Security ignora el programa de confianza `File.exe` para otros usuarios. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, establezca la configuración avanzada.

7. Haga clic en **Aceptar**.

   La nueva aplicación de confianza se añadirá a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

8. Guarde los cambios.



Lista de aplicaciones de confianza

Configuración de la aplicación de confianza

Parámetro	Descripción
No analizar archivos abiertos por la aplicación	Todos los archivos abiertos por la aplicación quedan excluidos de los análisis de Kaspersky Endpoint Security. Por ejemplo, si utiliza aplicaciones para realizar copias de seguridad de archivos, esta función ayuda a reducir el consumo de recursos de Kaspersky Endpoint Security.
No supervisar la actividad de la aplicación	Kaspersky Endpoint Security no supervisará la actividad de red y archivos de la aplicación en el sistema operativo. Puede configurar la supervisión de la actividad de la aplicación en diferentes componentes de Kaspersky Endpoint Security: • **No supervisar para los componentes de protección y control**. La actividad de la aplicación se supervisa a través de los siguientes componentes: Detección de comportamiento, Prevención de exploits, Prevención de intrusiones en el host, Motor de reparación y Firewall. • **No supervisar para Managed Detection and Response ni Endpoint Detection and Response**. La actividad de la aplicación es supervisada por el agente MDR integrado y el agente EDR integrado (KATA). • **No interceptar la entrada interactiva en la consola para Endpoint Detection and Response**. Kaspersky Endpoint Security no envía datos de telemetría sobre la administración de la aplicación en la consola. Kaspersky Anti Targeted Attack Platform (EDR) utiliza los datos de telemetría.
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Endpoint Security no supervisará la actividad de archivos ni redes de las aplicaciones iniciadas por esta aplicación. Puede aplicar la exclusión de forma recursiva. De este modo, la aplicación no supervisa la actividad de toda la cadena de aplicaciones secundarias.
No heredar restricciones del proceso principal (aplicación)	Kaspersky Endpoint Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal se inicia a través de una aplicación para la que se configuran los derechos de aplicación (Prevención de intrusiones en el host) y las reglas de red de la aplicación (Firewall).
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Endpoint Security no supervisará la actividad de archivos ni redes de las aplicaciones iniciadas por esta aplicación. Puede aplicar la exclusión de forma recursiva. De este modo, la aplicación no supervisa la actividad de toda la cadena de aplicaciones secundarias.
Permitir la interacción con la interfaz de la aplicación	Autoprotección de Kaspersky Endpoint Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona la casilla de verificación, la aplicación de acceso remoto tiene autorización para administrar la configuración de Kaspersky Endpoint Security mediante la interfaz de Kaspersky Endpoint Security.

Parámetro	Descripción
No bloquear la interacción con el componente de protección AMSI	Kaspersky Endpoint Security no supervisará las solicitudes de la aplicación de confianza para que el componente de protección AMSI analice objetos.
No analizar el tráfico de red	El tráfico de red iniciado por la aplicación se excluirá de los análisis de Kaspersky Endpoint Security. Puede excluir todo el tráfico o solo el tráfico cifrado de los análisis. También puede excluir direcciones IP individuales y números de puerto de los análisis. Kaspersky Endpoint Security versión 14.0 o anterior no admite la exclusión del tráfico de red si se especifica un hash para una aplicación de confianza en lugar de una ruta.
No interceptar modificaciones de archivos *(disponible solo en la Consola de Kaspersky Security Center)*	Kaspersky Endpoint Security no supervisa los cambios en los archivos de la cobertura de supervisión Control de integridad del sistema. La aplicación aplica la exclusión a todos los modos de Control de integridad del sistema: Control de integridad del sistema en tiempo y Comprobación de integridad del sistema a demanda.
No identificar modificaciones de registro *(disponible solo en la Consola de Kaspersky Security Center)*	Kaspersky Endpoint Security no supervisa los cambios en las claves de registro de la cobertura de supervisión Control de integridad del sistema. La aplicación aplica la exclusión a todos los modos de Control de integridad del sistema: Control de integridad del sistema en tiempo y Comprobación de integridad del sistema a demanda.
Comentario	Si es necesario, puede proporcionar un breve comentario para la aplicación de confianza. Los comentarios ayudan a simplificar las búsquedas y la clasificación de aplicaciones de confianza.
Estado	Estado de la aplicación de confianza: • El estado **Activo** significa que la aplicación se encuentra en la zona de confianza. • El estado **Inactivo** significa que la aplicación está excluida de la zona de confianza.

Creación de una zona de confianza local

Ahora, el usuario puede crear su propia zona de confianza local par un equipo específico. De esta forma, el usuario puede crear sus propias listas locales de exclusiones de análisis y aplicaciones de confianza, además de la zona de confianza general en una directiva. Un administrador puede permitir o bloquear el uso de exclusiones locales o aplicaciones de confianza locales en la configuración de la directiva. Para ello, utilice las casillas **Permitir el uso de exclusiones locales** y **Permitir el uso de aplicaciones locales de confianza** de la sección **Exclusiones** de la directiva.

Si un administrador permite la creación de una zona de confianza local, el usuario puede añadir sus propias exclusiones de análisis y aplicaciones de confianza en la interfaz de usuario de la aplicación. Al mismo tiempo, el usuario no tiene permisos para modificar o eliminar objetos de la zona de confianza configurada en la directiva. El administrador también puede ver, añadir, modificar o eliminar elementos de la lista en la consola de Kaspersky Security Center si es necesario añadir exclusiones para un equipo individual.

Kaspersky Endpoint Security oculta las listas de exclusiones del análisis y aplicaciones de confianza en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de la zona de confianza en la consola (símbolo de "candado cerrado") y las exclusiones del análisis y aplicaciones de confianza locales están prohibidas.

Cómo añadir un objeto a la zona de confianza local en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.

4. Haga doble clic para abrir la ventana de propiedades del equipo.

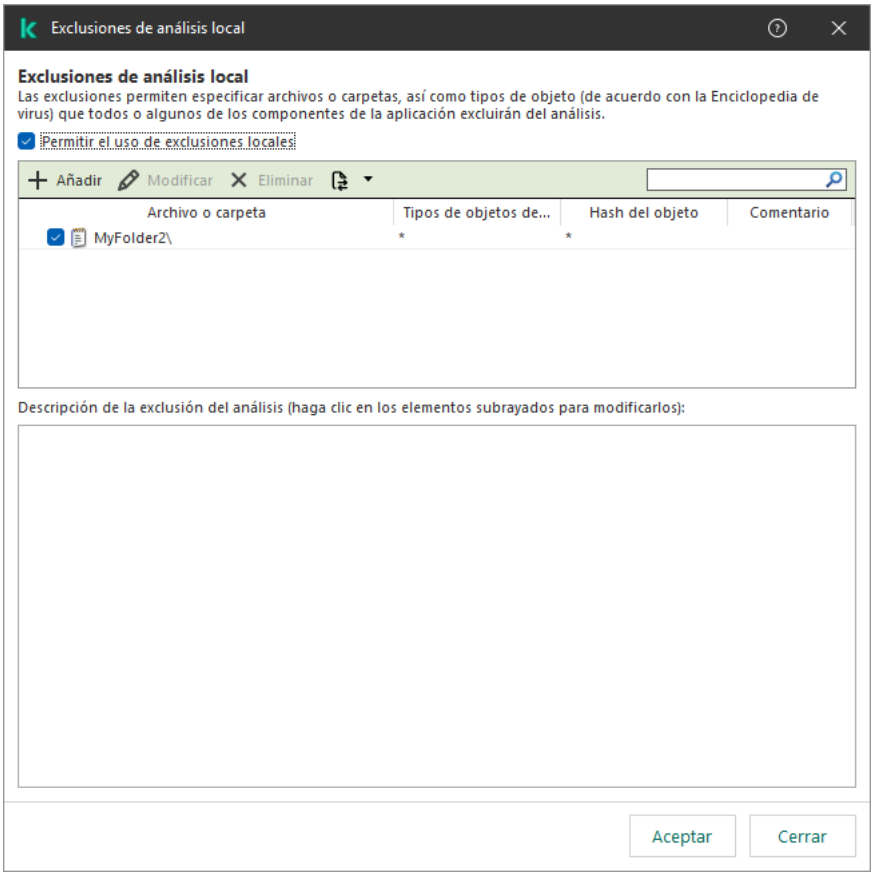
5. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.

6. En la lista de aplicaciones de Kaspersky que están instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.2)** y haga doble clic para abrir las propiedades de la aplicación.

7. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Exclusiones y tipos de objeto**.

8. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Exclusiones de análisis local**, haga clic en el botón **Configuración**.

   Se abre una ventana que contiene una lista de exclusiones locales.



Configuración de la zona de confianza

9. Haga una lista de exclusiones de análisis local.

   Las reglas para crear exclusiones de análisis local son las mismas que para las exclusiones generales. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

10. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Aplicaciones locales de confianza**, haga clic en el botón **Configuración**.

    Esto abre una ventana que contiene una lista de aplicaciones locales de confianza.

11. Haga una lista de aplicaciones locales de confianza.

    Las reglas para añadir aplicaciones a la lista de aplicaciones locales de confianza son las mismas que las reglas para añadirlas a la lista general. Kaspersky Endpoint Security admite variables de entorno y los caracteres * y ? al introducir una máscara.

12. Guarde los cambios.

Cómo añadir un objeto a la zona de confianza local en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Haga clic en el nombre del equipo en el que quiere permitir que un usuario realice una acción bloqueada.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.

5. Seleccione la pestaña **Configuración de la aplicación**.
6. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.
7. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el enlace **Exclusiones de análisis local**.
8. Haga una lista de exclusiones de análisis local.

   Las reglas para crear exclusiones locales son las mismas que las reglas para crear exclusiones generales. Kaspersky Endpoint Security admite variables de entorno y los caracteres * y ? al introducir una máscara.

9. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el enlace **Aplicaciones locales de confianza**.
10. Haga una lista de aplicaciones locales de confianza.

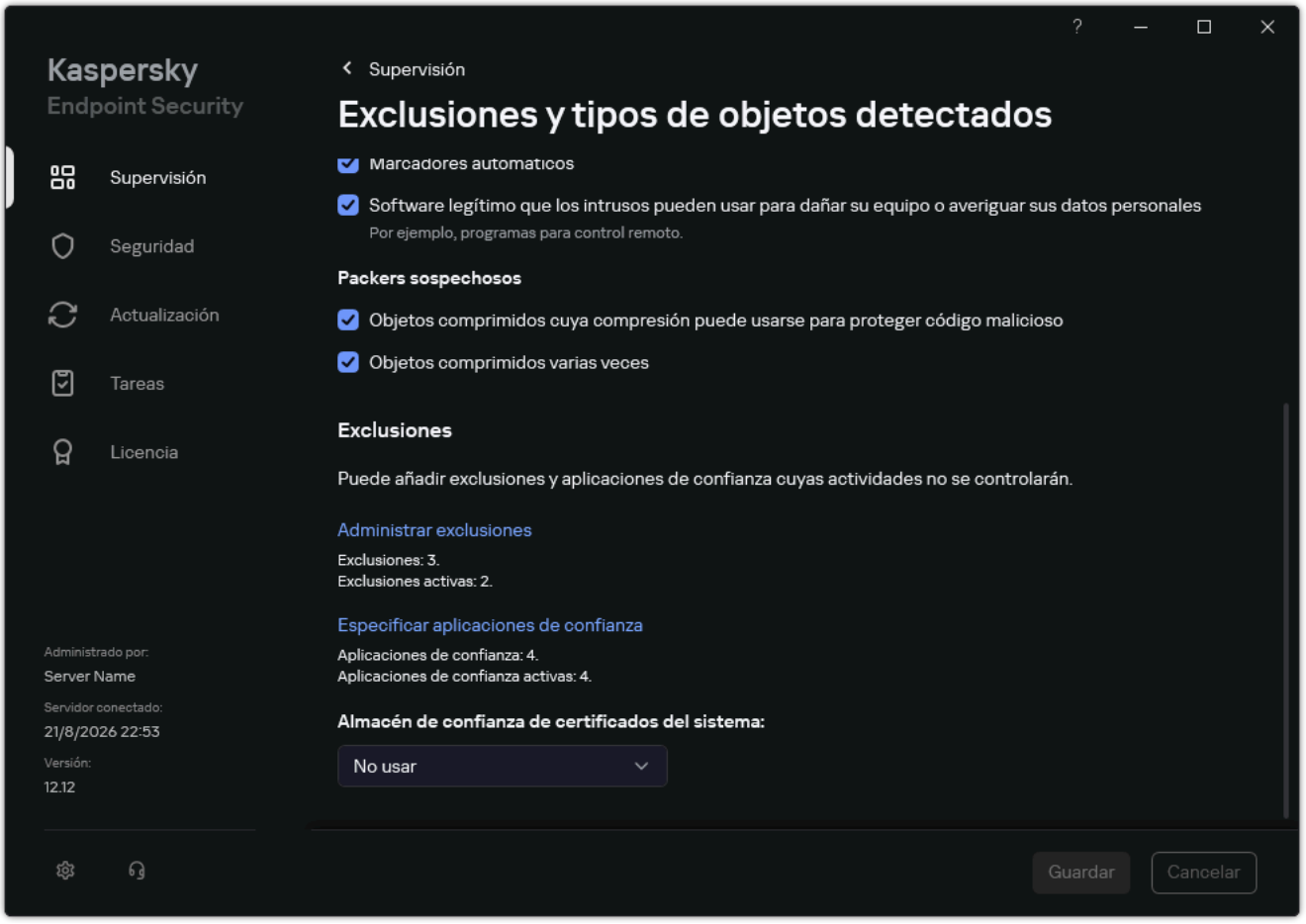
    Las reglas para añadir aplicaciones a la lista de aplicaciones locales de confianza son las mismas que las reglas para añadirlas a la lista general. Kaspersky Endpoint Security admite variables de entorno y los caracteres * y ? al introducir una máscara.

11. Guarde los cambios.

Cómo crear una exclusión del análisis local en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.

Kaspersky Endpoint Security oculta la lista de exclusiones del análisis en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las exclusiones del análisis en la consola (símbolo de "candado cerrado") y las exclusiones del análisis locales están prohibidas (la casilla de verificación **Permitir el uso de exclusiones locales** se encuentra desactivada).



Configuración de exclusiones

4. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una exclusión del análisis a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva exclusión de análisis a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *exclusiones de análisis predefinidas*. También se han añadido exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar exclusiones del análisis predefinidas según el propósito del servidor protegido.

   Para añadir una nueva exclusión de análisis a una categoría específica, active la casilla de verificación situada junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Si desea excluir un archivo o carpeta de los análisis, seleccione el archivo o carpeta haciendo clic en el botón **Examinar**.

También puede ingresar la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

  Puede utilizar máscaras al principio de la ruta del archivo, en el medio o al final. Por ejemplo, si desea agregar una carpeta para todos los usuarios en las exclusiones, ingrese la máscara `?:\Users\*\Folder\`.

  Puede excluir carpetas de red. Para hacer esto, introduzca la ruta a la carpeta de red manualmente (por ejemplo, `\\Network Share\*`).

6. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Tipos de objetos detectados**, introduzca el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

7. Si desea excluir un archivo individual de los análisis, introduzca el hash del archivo en el campo **Hash de objeto**.

   Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.

8. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión del análisis.

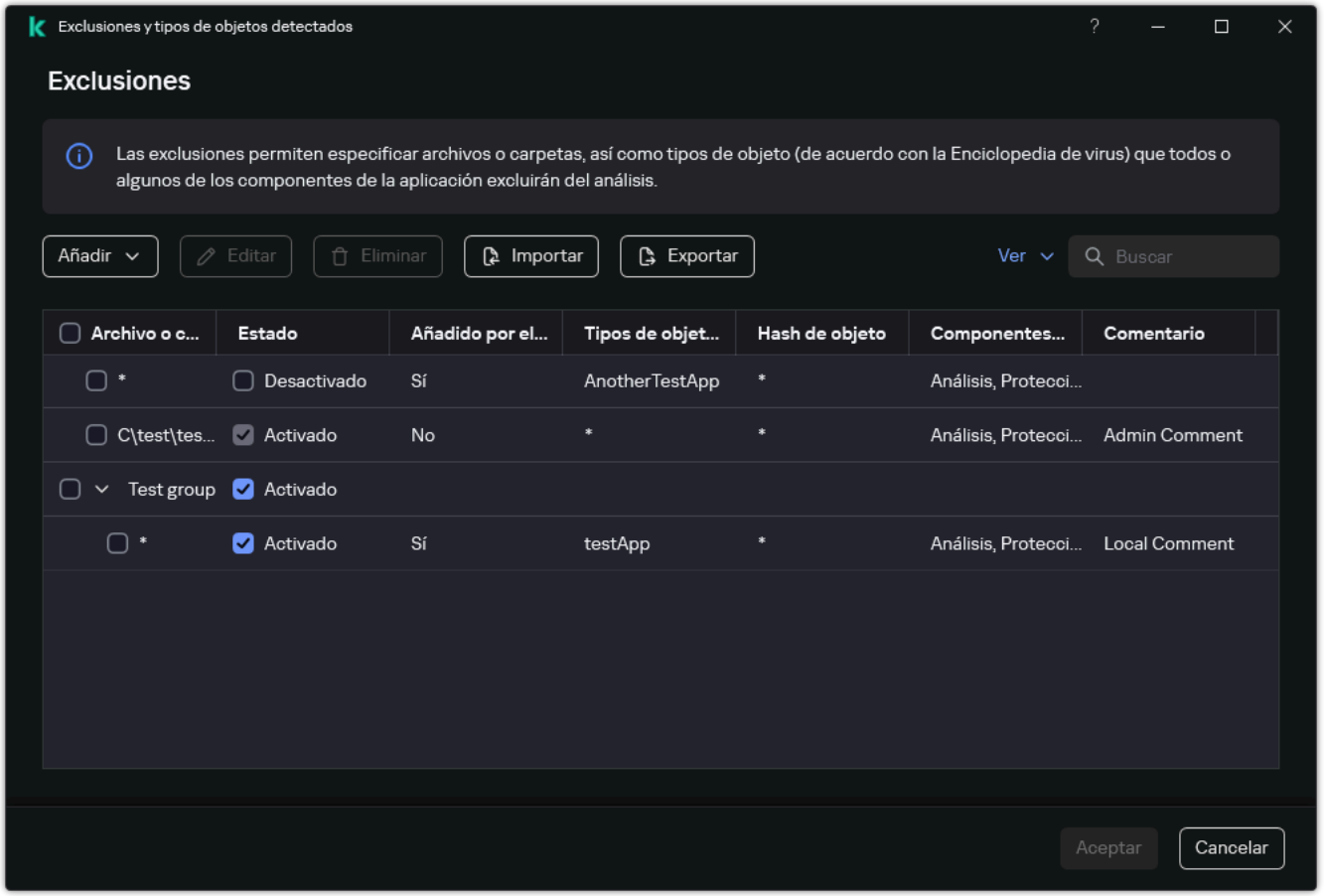
9. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

10. Seleccione el estado **Activo** para la exclusión.

11. Haga clic en **Añadir**.

    La nueva exclusión se añadirá a la lista. Puede desactivar la exclusión en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

12. Guarde los cambios.



Lista de exclusiones

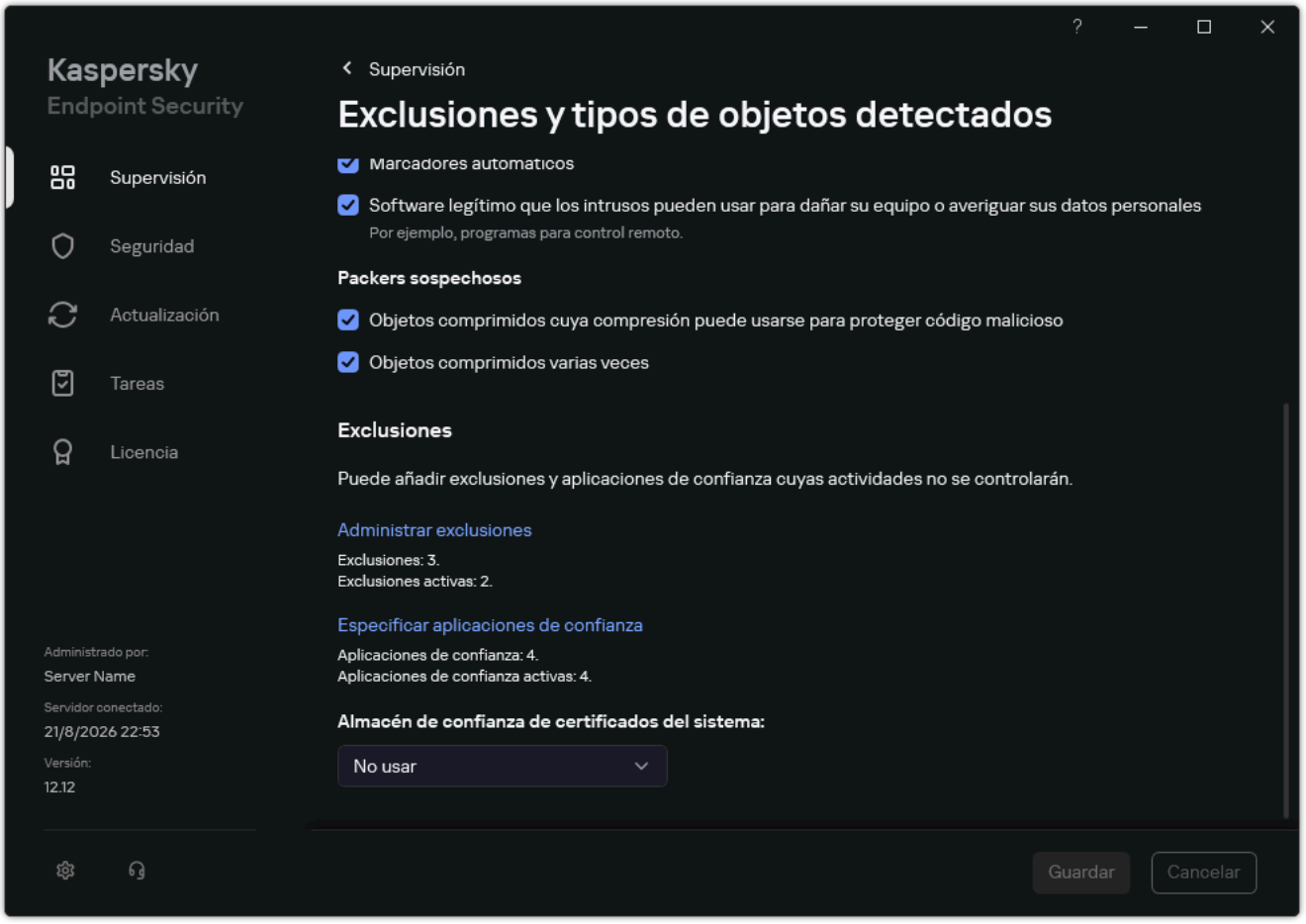
Cómo añadir una aplicación a la lista de aplicaciones locales de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.

3. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.

Kaspersky Endpoint Security oculta la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las aplicaciones de confianza en la consola (símbolo de "candado cerrado") y las aplicaciones de confianza locales están prohibidas (la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** se encuentra desactivada).



Configuración de exclusiones

4. Haga clic en **Añadir** y seleccione una acción:

   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías independientes. Para crear una nueva categoría, ingrese el nombre de la categoría y añada al menos una aplicación de confianza a la misma.
   - **Nueva exclusión**. Kaspersky Endpoint Security añade una nueva aplicación de confianza a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager, la aplicación incluye *aplicaciones de confianza predefinidas*. También se han añadido aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar aplicaciones de confianza predefinidas según el propósito del servidor protegido.

   Para añadir una nueva aplicación de confianza a una categoría específica, active la casilla de verificación situada junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Seleccione los criterios de confianza:

   - **Usar ruta del proceso completa en el disco para considerarlo de confianza**. Introduzca la ruta al archivo ejecutable de la aplicación de confianza.

     Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

Kaspersky Endpoint Security trata el nombre de archivo de una aplicación de confianza como sensible a mayúsculas y minúsculas. Si el nombre de archivo que introduzca presenta errores de mayúsculas y minúsculas, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

- **Usar hash del archivo de proceso para considerarlo de confianza**.

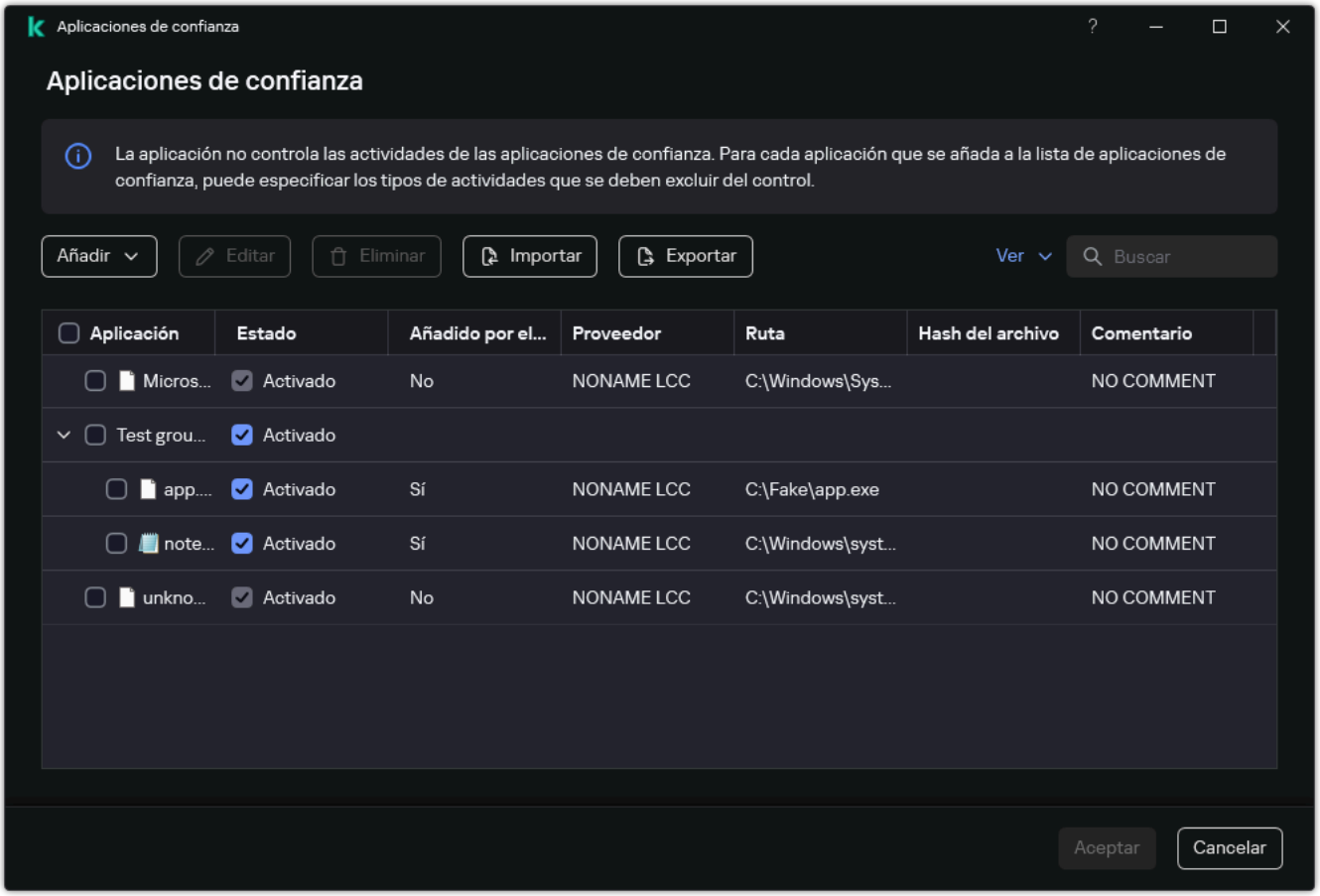
Kaspersky Endpoint Security es compatible con variables de entorno y convierte la ruta en la interfaz local de la aplicación. En otras palabras, si introduce la ruta de archivo `%userprofile%\Documents\File.exe`, se añade un registro `C:\Users\Fred123\Documents\File.exe` en la interfaz local de la aplicación para el usuario Fred123. En consecuencia, Kaspersky Endpoint Security ignora el programa de confianza `File.exe` para otros usuarios. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, establezca la configuración avanzada.

7. Haga clic en **Aceptar**.

   La nueva aplicación de confianza se añadirá a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

8. Guarde los cambios.



Lista de aplicaciones de confianza

Exportación e importación de la zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo. La zona de confianza consta de las siguientes listas: *exclusiones de análisis* y *aplicaciones de confianza*. Puede exportar estas listas a archivos XML y otros formatos. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de exclusiones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones y de la lista de aplicaciones de confianza, o para migrar la lista a un servidor diferente.

La aplicación utiliza los siguientes formatos para exportar e importar la *lista de exclusiones*:

- XML está disponible en la Consola de administración (MMC), Web Console y Cloud Console.
- DAT está disponible solo para importar en la Consola de administración (MMC). El propósito de este formato es mantener la compatibilidad con versiones anteriores de la aplicación. Puede convertir un archivo DAT a XML en la Consola de administración (MMC) para migrar las listas de exclusión a la Consola web.
- CSV solo está disponible en la interfaz local de la aplicación.

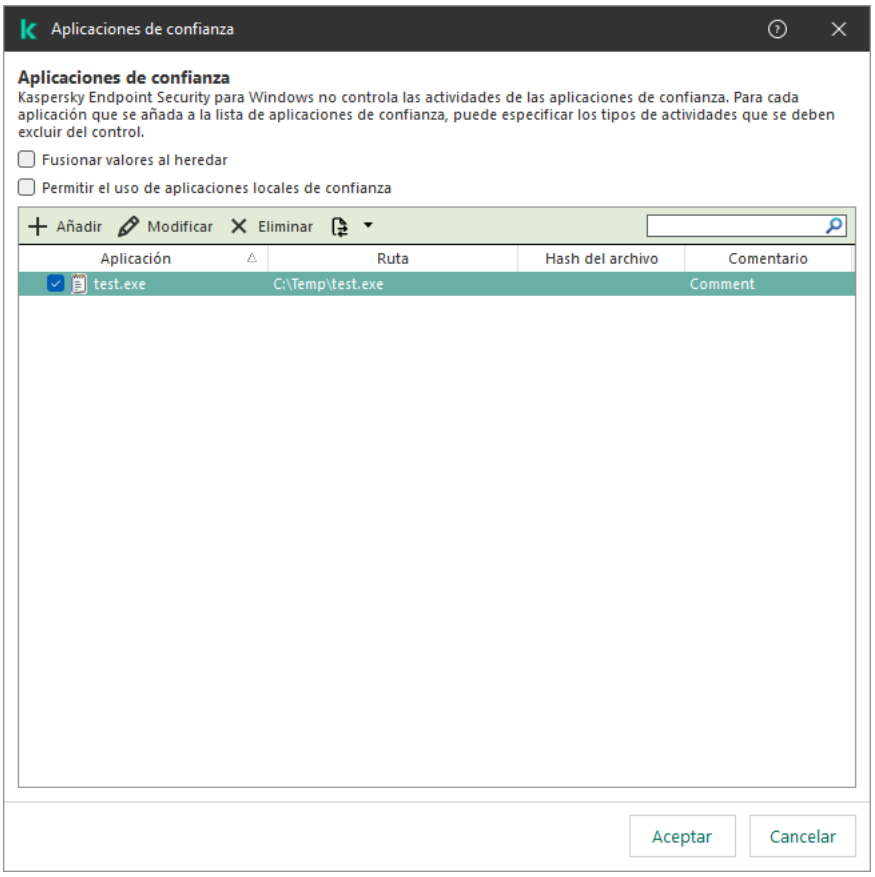
Kaspersky Endpoint Security utiliza el formato XML para exportar e importar la *lista de aplicaciones de confianza*.

Cómo exportar e importar la zona de confianza en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones y tipos de objeto**.
4. En **Exclusiones de análisis y aplicaciones de confianza**, seleccione el componente de la zona de confianza que desea exportar o importar: **Exclusiones del análisis** o **Aplicaciones de confianza**.
5. Haga clic en **Configuración**.
6. Para exportar la lista de reglas:
   a. Seleccione las exclusiones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna exclusión, Kaspersky Endpoint Security exportará todas las exclusiones.
   b. Haga clic en el botón → **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.

d. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML. Kaspersky Endpoint Security también admite la exportación de la lista de exclusiones a un archivo DAT.



Lista de aplicaciones de confianza

7. Para importar la lista de exclusiones:

a. Haga clic en el botón → **Importar**.

b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.

c. Abra el archivo.

Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML. Kaspersky Endpoint Security también admite la importación de una lista de exclusiones desde un archivo DAT.

8. Guarde los cambios.

Cómo exportar e importar la zona de confianza en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Zona de confianza**.

5. Para exportar la lista de reglas:

   a. Haga clic en el enlace **Exclusiones del análisis antimalware**.

   b. Seleccione las exclusiones que desea exportar.

   c. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de exclusiones a un archivo JSON en la carpeta de descargas predeterminada.

6. Para exportar la lista de aplicaciones de confianza:

   a. Seleccione las aplicaciones de confianza que desee exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de aplicaciones de confianza a un archivo JSON en la carpeta de descargas predeterminada.

7. Para importar la lista de exclusiones:

   a. Haga clic en el enlace **Exclusiones del análisis antimalware**.

   b. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que importar la lista de exclusiones.

   c. Abra el archivo.

      Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

8. Para importar la lista de aplicaciones de confianza:

   a. Haga clic en el enlace **Aplicaciones**.

   b. Haga clic en el botón → **Importar**.

      Se abre una ventana; en ella, seleccione el archivo JSON desde el que desea importar la lista de aplicaciones de confianza.

   c. Abra el archivo.

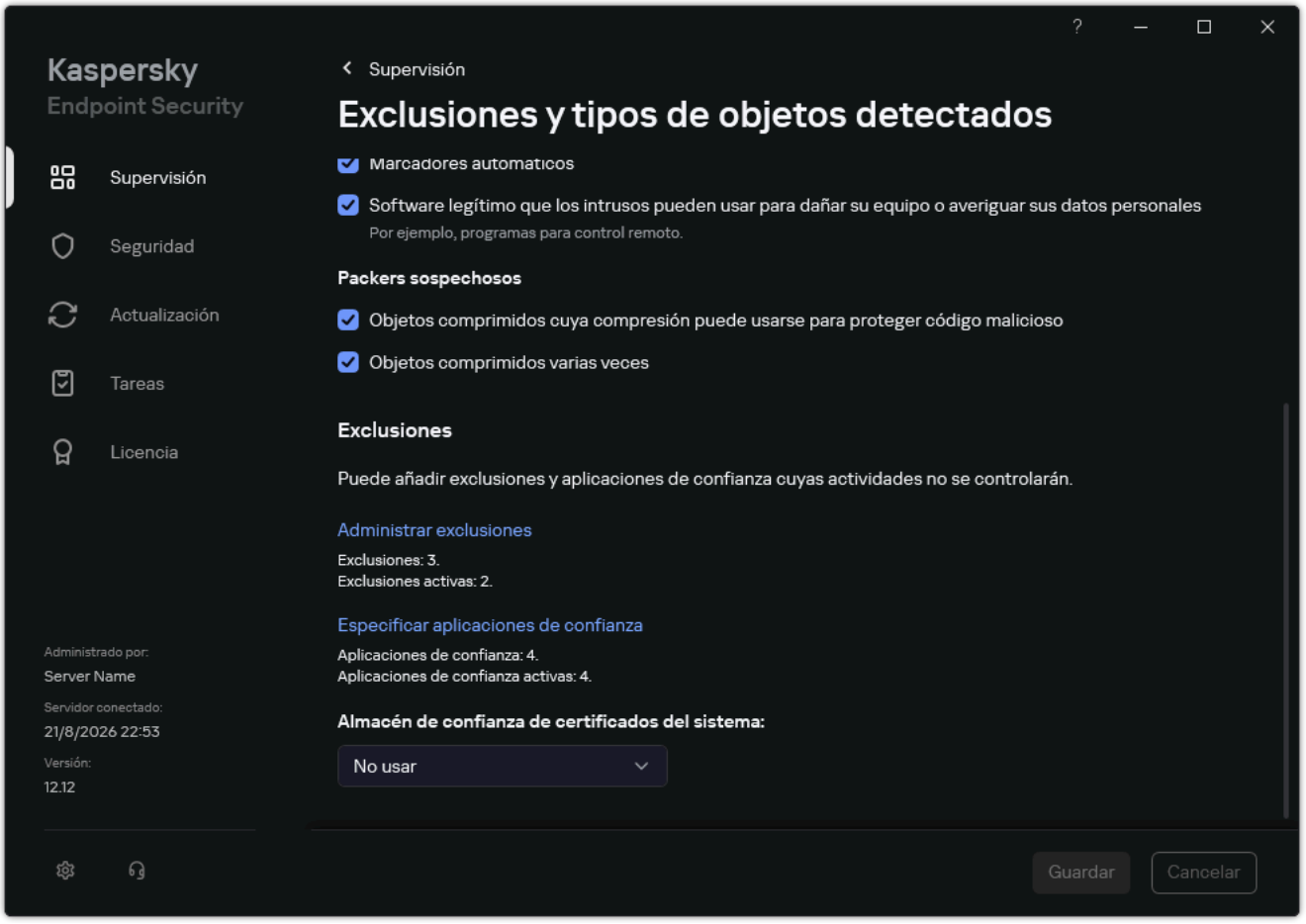
      Si el equipo ya tiene una lista de aplicaciones de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

9. Guarde los cambios.

Cómo exportar o importar la zona de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Exclusiones y tipos de objetos detectados**.



Configuración de exclusiones

3. Para exportar la lista de reglas:

   a. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.

   b. Seleccione las exclusiones que desea exportar.

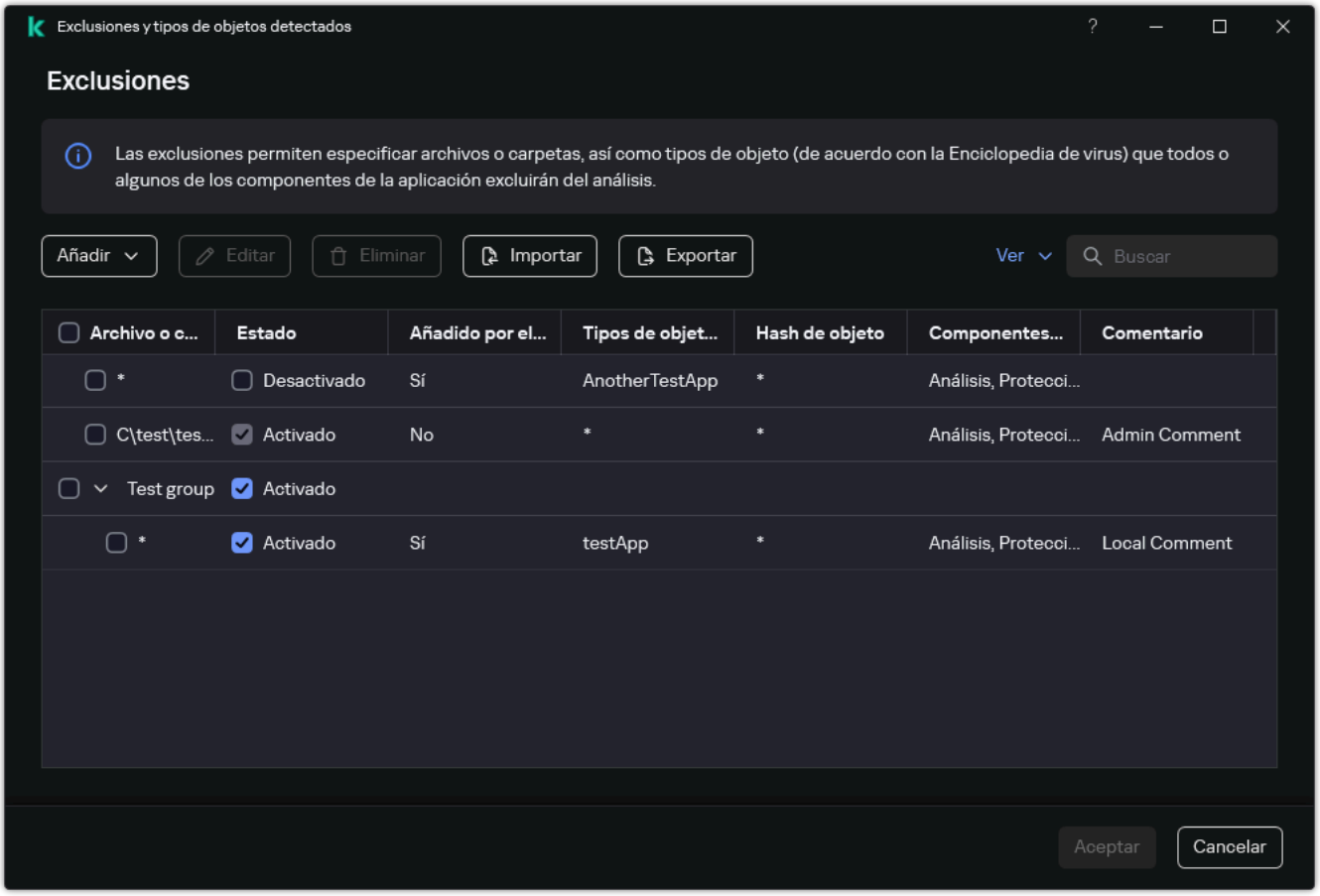
   c. Haga clic en **Exportar**.

   d. Confirme que desea exportar solo las exclusiones seleccionadas o exportar la lista completa de exclusiones.

   e. En la ventana que se abre, especifique el nombre del archivo CSV al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.

f. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo CSV.



Lista de exclusiones

4. Para exportar la lista de aplicaciones de confianza:

   a. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.

   b. Seleccione las aplicaciones de confianza que desee exportar.

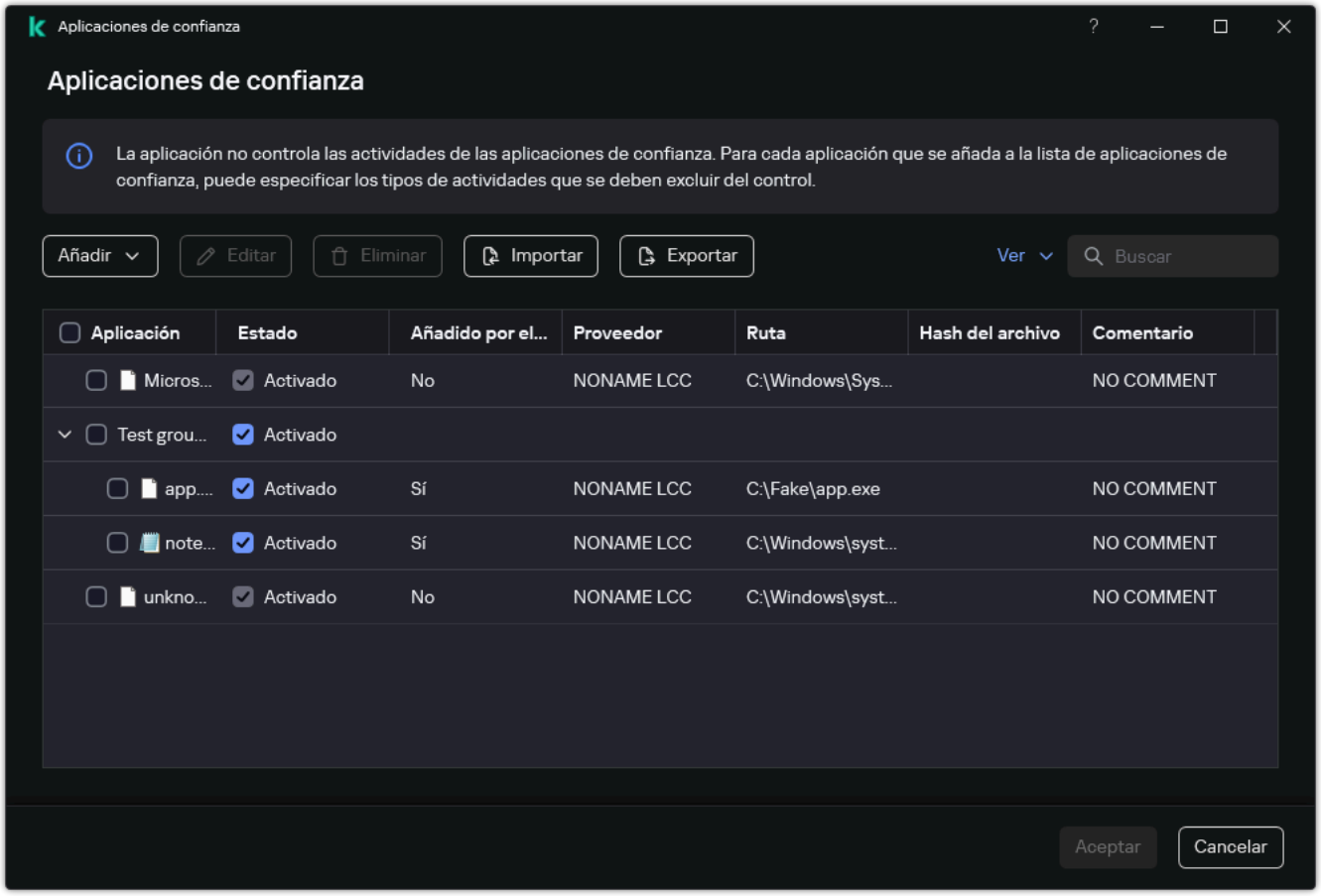
   c. Haga clic en **Exportar**.

   d. Confirme que desea exportar solo las aplicaciones de confianza seleccionadas o exportar la lista completa.

   e. Esto abre una ventana; en ella, introduzca el nombre del archivo XML al que desea exportar la lista de aplicaciones de confianza, y seleccione la carpeta en la que desea guardar este archivo.

f. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de aplicaciones de confianza al archivo XML.



Lista de aplicaciones de confianza

5. Para importar la lista de exclusiones:

a. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.

b. Haga clic en **Importar**.

c. En la ventana que se abre, seleccione el archivo CSV del que importar la lista de exclusiones.

d. Abra el archivo.

Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo CSV.

6. Para importar la lista de aplicaciones de confianza:

a. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.

b. Haga clic en **Importar**.

c. Se abre una ventana; en ella, seleccione el archivo XML desde el que desea importar la lista de aplicaciones de confianza.

d. Abra el archivo.

Si el equipo ya tiene una lista de aplicaciones de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

7. Guarde los cambios.

Manejo de aplicaciones con una firma digital confiable

El uso del almacén de certificados del sistema le permite excluir aplicaciones firmadas por una firma digital de confianza del análisis antivirus. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al Grupo de *De confianza*.

Cómo iniciar el uso de un almacenamiento de certificados del sistema de confianza en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
4. En el bloque **Almacén de confianza de certificados del sistema**, seleccione la casilla de verificación **Usar almacén de confianza de certificados del sistema**.
5. En la lista desplegable, seleccione el almacén del sistema en el que debe confiar Kaspersky Endpoint Security.
6. Guarde los cambios.

Cómo iniciar el uso de un almacenamiento de certificados del sistema de confianza en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Zona de confianza**.
5. En la ventana que se abre, haga clic en el vínculo **Certificados raíz**.
6. En la ventana que se abre, active la casilla **Usar almacén de confianza de certificados del sistema**.
7. Seleccione qué tienda del sistema debe considerar de confianza Kaspersky Endpoint Security.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo iniciar el uso de un almacenamiento de certificados del sistema de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Exclusiones y tipos de objetos detectados**.
3. En la lista desplegable **Almacén de confianza de certificados del sistema**, seleccione el almacén del sistema en el que debe confiar Kaspersky Endpoint Security.
4. Guarde los cambios.

Apéndice. Exclusiones de análisis predefinidas y aplicaciones de confianza.

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. A partir de Kaspersky Endpoint Security 12.8 para Windows, puede instalar la aplicación en modo Light Agent para proteger los entornos virtuales. Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware.

Puede seleccionar exclusiones predefinidas y aplicaciones de confianza de las siguientes formas:

- Instalar la aplicación.
  - Instalación de la aplicación de manera local mediante el Asistente de instalación
  - Propiedades del paquete de instalación
- Establecer la directiva.
  - Asistente de nueva directiva
  - Propiedades de la directiva: exclusiones de análisis y aplicaciones de confianza

Microsoft SQL Server

Al instalar Kaspersky Endpoint Security en un servidor SQL, debe crear una zona de confianza a partir de exclusiones y aplicaciones de confianza predefinidas para asegurarse de que no se interfiera con el funcionamiento del servidor.

Exclusiones de análisis predefinidas

Ruta	Versión de SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

Al instalar Kaspersky Endpoint Security en un servidor de Microsoft Exchange, debe crear una zona de confianza a partir de exclusiones y aplicaciones de confianza predefinidas para asegurarse de que no se interfiera con el funcionamiento del servidor.

Exclusiones de análisis predefinidas

Ruta	Versión de Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Ruta	Versión de Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Aplicaciones de confianza predefinidas

Ruta	Versión de Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Si Microsoft System Center Configuration Manager está instalado en el sistema operativo del equipo protegido, debe añadir una exclusión predefinida a la lista de exclusiones de análisis para garantizar el funcionamiento estable de la solución.

Exclusiones de análisis predefinidas

Ruta	Versión de System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Al instalar Kaspersky Endpoint Security en un entorno virtual Citrix, debe crear una zona de confianza a partir de exclusiones y aplicaciones de confianza predefinidas para asegurarse de que no se interfiera con el funcionamiento del servidor.

Ruta
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache

Ruta	
vdiskdif.vhdx	
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb	

Aplicaciones de confianza predefinidas

Ruta	Solución Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Aplicaciones y escritorios virtuales
%SystemRoot%\System32\drivers\CVhdFilter.sys	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Aplicaciones y escritorios virtuales
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Aplicaciones y escritorios virtuales

Ruta	Solución Citrix
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Aplicaciones y escritorios virtuales
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Aplicación Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Aplicación Workspace
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning

Ruta	Solución Citrix
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Al instalar Kaspersky Endpoint Security en un entorno virtual de VMware, debe crear una zona de confianza a partir de aplicaciones de confianza predefinidas para asegurarse de que no se interfiera con el funcionamiento del servidor.

Aplicaciones de confianza predefinidas

Ruta	Solución VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon

Ruta	Solución VMware
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Desduplicación de datos en Microsoft Windows Server

Si la desduplicación de datos está habilitada en el sistema operativo Microsoft Windows Server en el que está instalado Kaspersky Endpoint Security, debe añadir una aplicación de confianza predefinida a la lista de aplicaciones de confianza para optimizar Kaspersky Endpoint Security y reducir la carga de la CPU.

Aplicaciones de confianza predefinidas

Ruta	Versión de Microsoft Windows Server
%SystemRoot%\system32\fsdmhost.exe	Todas las versiones compatibles

Gestión de Copia de seguridad

Copias de seguridad almacena copias de seguridad de los archivos que se modificaron o eliminaron durante la desinfección. Una *copia de seguridad* es una copia del archivo creada antes de que el archivo se desinfectara o se eliminara. Las copias de seguridad de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. El usuario cuya cuenta se usó para instalar la Kaspersky Endpoint Security tiene derechos de acceso limitado a esta carpeta.

Kaspersky Endpoint Security no ofrece la posibilidad de configurar permisos de acceso de usuario a copias de seguridad de los archivos.

En ocasiones no se puede mantener la integridad de los archivos durante la desinfección. Si, después de la desinfección, pierde parcial o completamente el acceso a información importante de un archivo desinfectado, puede intentar restaurarlo a su carpeta original a partir de su copia de seguridad.

Si Kaspersky Endpoint Security funciona mediante la gestión de Kaspersky Security Center, las copias de seguridad de los archivos se pueden transmitir al Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la gestión de copias de seguridad de archivos en Kaspersky Security Center, consulte el sistema de Ayuda de Kaspersky Security Center.

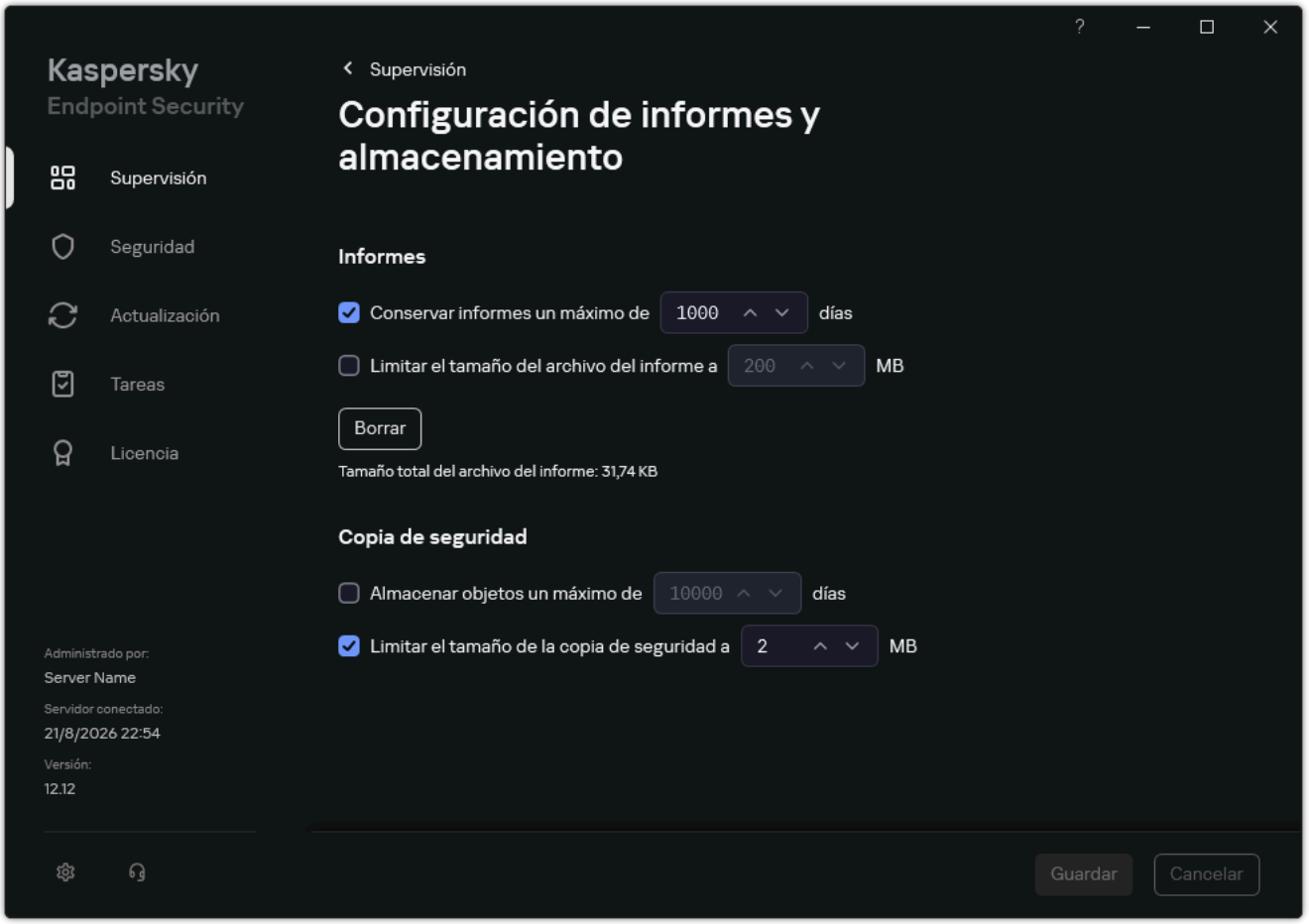
Configuración del período de almacenamiento máximo de archivos en Copia de seguridad

De forma predeterminada, el período de almacenamiento máximo de copias de archivos en Copia de seguridad es de 30 días. Cuando venza el período máximo de almacenamiento, Kaspersky Endpoint Security eliminará los archivos más antiguos de Copia de seguridad.

Para configurar el período de almacenamiento máximo para archivos en Copia de seguridad:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el mosaico **Informes y almacenamiento**.



Configuración de la copia de seguridad

3. Si desea limitar el período de almacenamiento para copias de archivos en Copia de seguridad, seleccione la casilla de verificación **Almacenar objetos un máximo de N días** en el bloque **Copia de seguridad**. Escriba la duración máxima de almacenamiento de las copias de los archivos en Copia de seguridad.

4. Guarde los cambios.

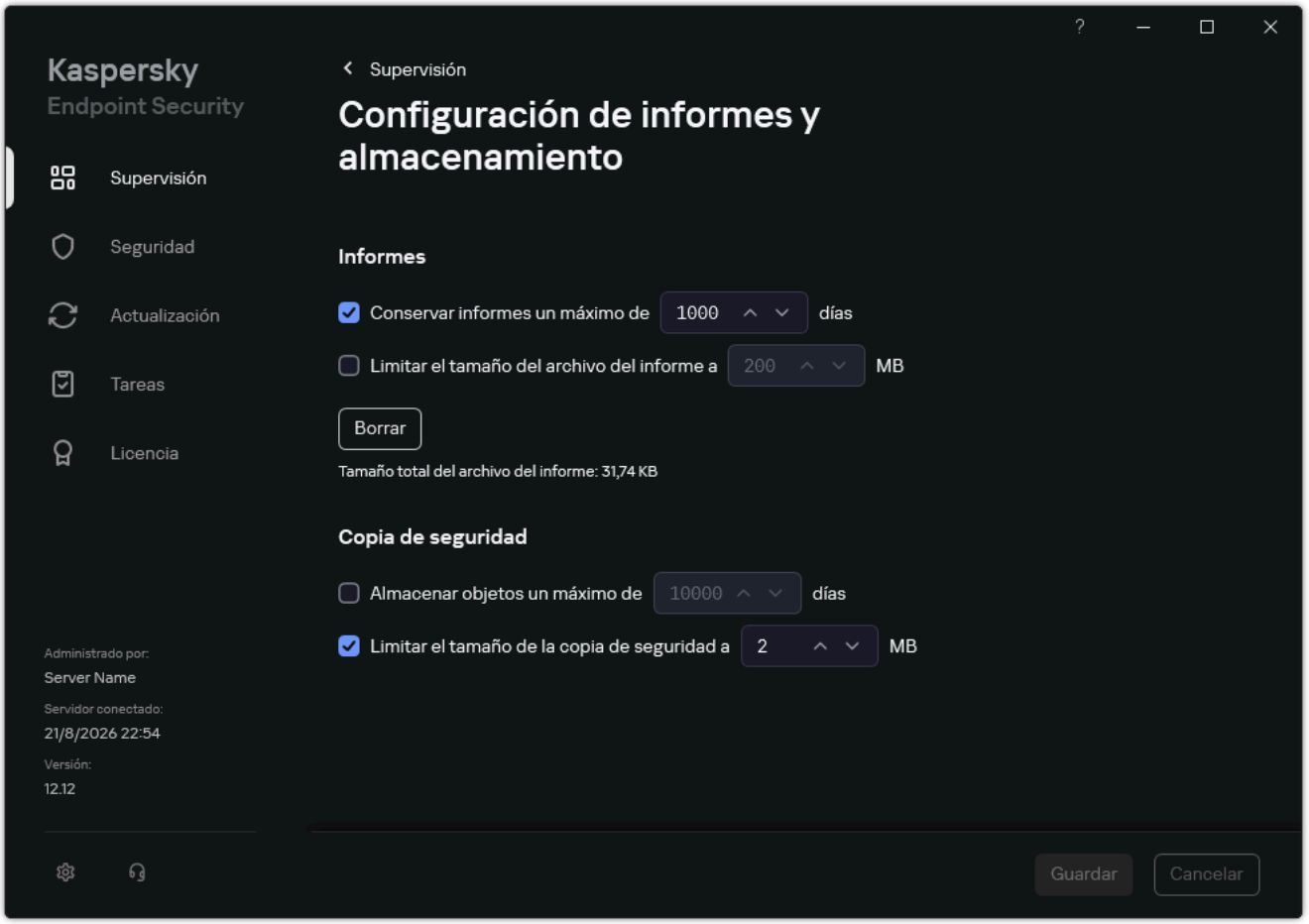
Configuración del tamaño máximo de Copia de seguridad

Puede especificar el tamaño máximo de Copia de seguridad. El tamaño de Copia de seguridad es ilimitado de forma predeterminada. Cuando se alcanza el límite máximo de almacenamiento, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos de Copia de seguridad.

Para configurar el tamaño máximo de Copia de seguridad:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el mosaico **Informes y almacenamiento**.



Configuración de la copia de seguridad

3. En el bloque **Copia de seguridad**, seleccione la casilla de verificación **Limitar el tamaño de la copia de seguridad a N MB**. Si la casilla de verificación está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Cuando se alcanza el valor definido, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos para evitar que el límite se exceda.

4. Guarde los cambios.

Restauración de archivos de Copia de seguridad

Si se detecta código malicioso en un archivo, Kaspersky Endpoint Security lo bloquea, le asigna el estado *No desinfectado*, coloca una copia en Copia de seguridad e intenta desinfectarlo. Si se realiza la desinfección del archivo correctamente, el estado de la copia de seguridad del archivo pasará a *Desinfectado*. El archivo está disponible en su carpeta original. Si un archivo no se puede desinfectar, Kaspersky Endpoint Security lo elimina de su carpeta original. Puede restaurar el archivo de su copia de seguridad a su carpeta original.

Los archivos con el estado *Se eliminará al reiniciar el equipo* no se pueden restaurar. Reinicie el equipo y el estado del archivo cambiará a *Desinfectado* o *Eliminado*. También puede restaurar el archivo de su copia de seguridad a su carpeta original.

Al detectar código malicioso en un archivo que forma parte de la aplicación Tienda Windows, Kaspersky Endpoint Security elimina de inmediato el archivo sin que se mueva una copia del archivo a Copia de seguridad. Puede restaurar la integridad de la aplicación de la Tienda Windows por medio de las herramientas adecuadas del sistema operativo (consulte los archivos de ayuda de Microsoft Windows para obtener información detallada sobre la restauración de una aplicación de la Tienda Windows).

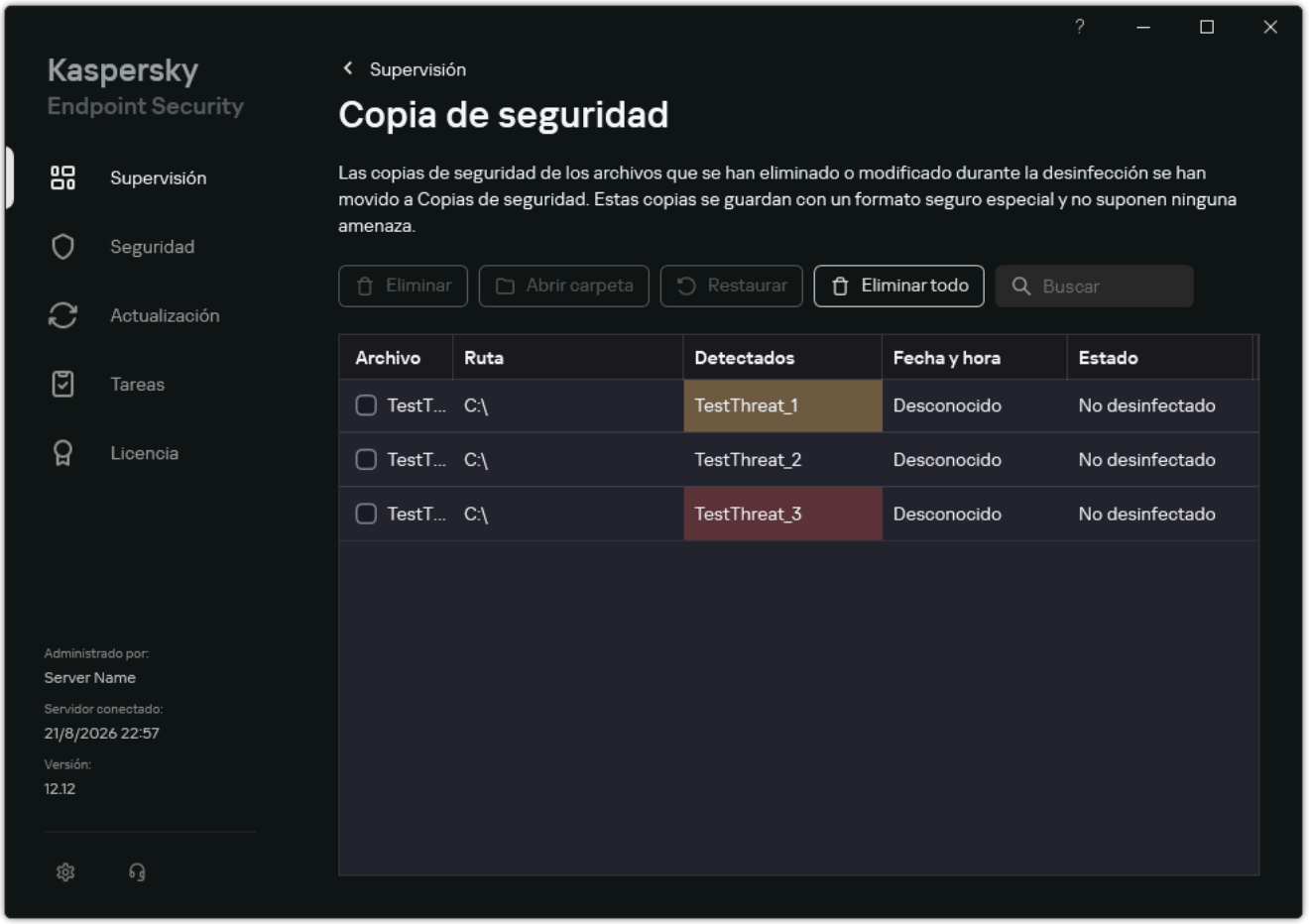
El conjunto de las copias de seguridad de los archivos se presenta como una tabla. Para una copia de seguridad de un archivo, se muestra la ruta a la carpeta original del archivo. La ruta a la carpeta original del archivo puede contener datos personales.

Si varios archivos con nombres idénticos y contenido diferente ubicados en la misma carpeta se mueven a Copia de seguridad, solo se podrá restaurar el archivo que se llevó allí en último lugar.

Para restaurar los archivos de Copia de seguridad, haga lo siguiente:

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Copia de seguridad**.
2. Esto abre la lista de archivos en Copia de seguridad; en esa lista, seleccione los archivos que desea restaurar y haga clic en **Restaurar**.

Kaspersky Endpoint Security restaura los archivos a partir de las copias de seguridad seleccionadas en las carpetas originales.



Copia de seguridad

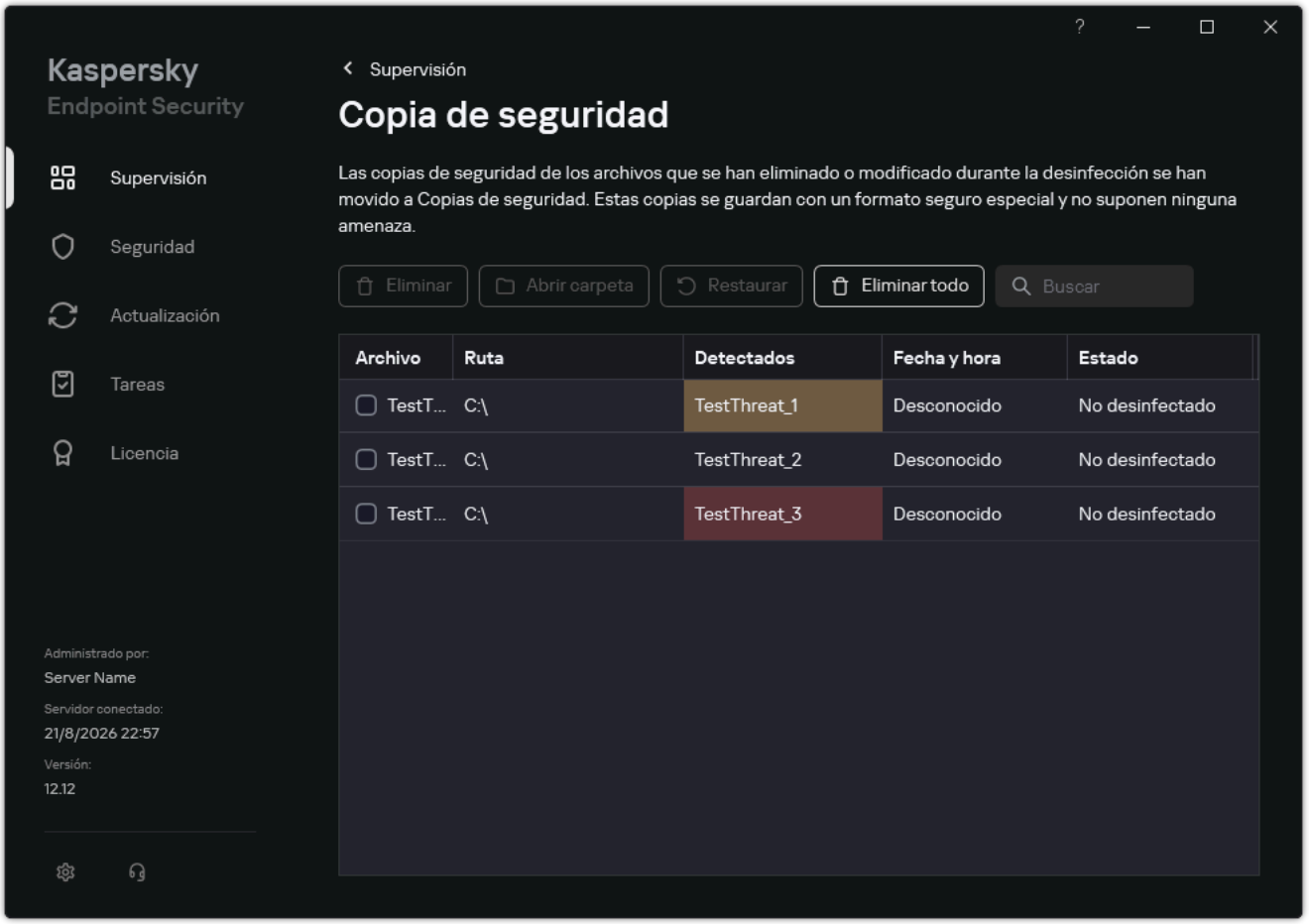
Eliminación de las copias de seguridad de los archivos de Copia de seguridad

Kaspersky Endpoint Security elimina automáticamente las copias de seguridad de los archivos de Copia de seguridad (independientemente de su estado) una vez que ha vencido el período de almacenamiento establecido en la configuración de la aplicación. También puede eliminar manualmente cualquier copia de un archivo desde Copia de seguridad.

Para eliminar las copias de seguridad de los archivos de Copia de seguridad:

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Copia de seguridad**.
2. Esto abre la lista de archivos en Copia de seguridad; en esta lista, seleccione los archivos que desea eliminar de la copia de seguridad y haga clic en **Eliminar**.

Kaspersky Endpoint Security elimina las copias de seguridad seleccionadas de los archivos de Copia de seguridad.



Copia de seguridad

Servicio de notificaciones

Toda clase de eventos se producen durante el funcionamiento de Kaspersky Endpoint Security. Pueden ser puramente informativos o críticos. Por ejemplo, las notificaciones pueden informar de una actualización de base de datos y de módulos de aplicación exitosa o registrar errores de componentes que se necesitan remediar.

Kaspersky Endpoint Security admite el registro de información sobre eventos en el funcionamiento del registro de aplicaciones de Microsoft Windows y/o del registro de sucesos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security envía notificaciones de las siguientes formas:

- mediante notificaciones emergentes en el área de notificación de la barra de tareas de Microsoft Windows;
- por correo electrónico.

Puede configurar el envío de notificaciones de eventos. El método de envío de notificaciones se configura para cada tipo de evento.

Al usar la tabla de eventos para configurar el servicio de notificaciones, puede realizar las siguientes acciones:

- Filtre los eventos del servicio de notificaciones por valores de columnas o por condiciones de filtro personalizadas.
- Utilice la función de búsqueda para los eventos del servicio de notificaciones.
- Ordene los eventos del servicio de notificaciones.
- Cambie el orden y el conjunto de columnas que aparecen en la lista de eventos del servicio de notificaciones.

Configuración de los parámetros de registro de eventos

Para configurar los parámetros del registro de eventos:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En el bloque **Notificaciones**, haga clic en el botón **Configurar notificaciones**.

   Los componentes y tareas de Kaspersky Endpoint Security aparecen en la parte izquierda de la ventana. En la parte derecha de la ventana figuran los eventos generados del componente o tarea seleccionados.

   Los eventos pueden contener siguientes datos de usuario:

   - Rutas a archivos analizadas por Kaspersky Endpoint Security.
   - Rutas a claves del registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
   - Nombre de usuario de Microsoft Windows.
   - Direcciones de páginas web abiertas por el usuario.

4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los que desee configurar los parámetros del registro de eventos.

5. Seleccione las casillas de verificación de los eventos relevantes de las columnas **Guardar en informe local** y **Guardar en Registro de eventos de Windows**.

   Los eventos cuyas casillas están seleccionadas en la columna **Guardar en informe local** se muestran en los Registros de aplicación. Los eventos cuyas casillas están seleccionadas en la columna **Guardar en Registro de eventos de Windows** se muestran en los registros de Windows en el canal `Application`.

6. Guarde los cambios.

Configuración de la visualización y entrega de notificaciones

Para configurar la visualización y entrega de notificaciones:

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.

3. En el bloque **Notificaciones**, haga clic en el botón **Configurar notificaciones**.

   Los componentes y tareas de Kaspersky Endpoint Security aparecen en la parte izquierda de la ventana. En la parte derecha de la ventana figuran los eventos generados del componente o tarea seleccionados.

   Los eventos pueden contener siguientes datos de usuario:

   - Rutas a archivos analizadas por Kaspersky Endpoint Security.
   - Rutas a claves del registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
   - Nombre de usuario de Microsoft Windows.
   - Direcciones de páginas web abiertas por el usuario.

4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los que desee configurar el envío de notificaciones.

5. En la columna **Notificar en pantalla**, seleccione las casillas situadas junto a los eventos relevantes.

   La información sobre los eventos seleccionados aparece en mensajes emergentes en pantalla en el área de notificación de la barra de tareas de Microsoft Windows.

6. En la columna **Notificar por correo electrónico**, seleccione las casillas situadas junto a los eventos relevantes.

   La información sobre los eventos seleccionados se entrega por correo electrónico si se configuran los ajustes de entrega de notificaciones del correo.

7. Haga clic en **Aceptar**.

8. Si activó las notificaciones por correo electrónico, establezca la configuración para la entrega de correo electrónico:

   a. Haga clic en **Configurar notificaciones de correo**.

   b. Seleccione la casilla de verificación **Notificar acerca de eventos** para activar el envío de notificaciones sobre los eventos de Kaspersky Endpoint Security que se seleccionan en la columna **Notificar por correo electrónico**.

   c. Especifique la configuración del envío de notificaciones por correo electrónico.

   d. Haga clic en **Aceptar**.

9. Guarde los cambios.

Configuración de la visualización de advertencias sobre el estado de la aplicación en el área de notificaciones

Para configurar la visualización de advertencias de estado de la aplicación en el área de notificaciones:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En el bloque **Mostrar el estado de la aplicación en el área de notificaciones**, seleccione las casillas de verificación que hay junto a esas categorías de eventos sobre los cuales desea ver notificaciones en el área de notificaciones de Microsoft Windows.
4. Guarde los cambios.

Cuando tienen lugar eventos asociados con las categorías seleccionadas, el icono de la aplicación del área de notificaciones cambiará a o a según la seriedad de la advertencia.

Mensajes entre los usuarios y el administrador

Los componentes de Control de aplicaciones, Control de dispositivos, Control Web y Control de anomalías adaptativo permiten que los usuarios de una red LAN con equipos que tienen Kaspersky Endpoint Security instalado envíen mensajes al administrador.

Es posible que un usuario deba enviar un mensaje al administrador de la red corporativa local en los casos siguientes:

- Control de dispositivos bloqueó el acceso al dispositivo.

  La plantilla del mensaje para una solicitud de acceso a un dispositivo bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección Control de dispositivos.

- Control de aplicaciones bloqueó el inicio de una aplicación.

  La plantilla del mensaje para solicitar permiso para el inicio de una aplicación bloqueada está disponible en la interfaz de Kaspersky Endpoint Security en la sección Control de aplicaciones.

- Control Web bloqueó el acceso a un recurso web.

  La plantilla del mensaje para solicitar acceso a un recurso web bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección Control Web.

El método usado para enviar mensajes y la plantilla utilizada dependen de si hay una directiva activa de Kaspersky Security Center que se ejecuta en el equipo que tiene Kaspersky Endpoint Security instalado, y si hay alguna conexión con el servidor de administración de Kaspersky Security Center. Son posibles las siguientes situaciones:

- Si una directiva de Kaspersky Security Center no se está ejecutando en el equipo donde se ha instalado Kaspersky Endpoint Security, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

  Los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la interfaz local de Kaspersky Endpoint Security.

- Si una directiva de Kaspersky Security Center se está ejecutando en el equipo donde se ha instalado Kaspersky Endpoint Security, el mensaje estándar se envía al servidor de administración de Kaspersky Security Center.

  En este caso, los mensajes del usuario se pueden ver en el almacén de eventos de Kaspersky Security Center (consulte las instrucciones más abajo). Los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

- Si la directiva para casos en los que el equipo está fuera de la oficina de Kaspersky Security Center está ejecutándose en el equipo donde se ha instalado Kaspersky Endpoint Security, el método usado para enviar mensajes depende de si existe una conexión con Kaspersky Security Center.

  - Si se establece una conexión con Kaspersky Security Center, Kaspersky Endpoint Security envía el mensaje estándar al servidor de administración de Kaspersky Security Center.

  - Si falta una conexión con Kaspersky Security Center, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

  En ambos casos, los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

Para ver el mensaje de un usuario en el almacén de eventos de Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.

   El espacio de trabajo de Kaspersky Security Center muestra todos los eventos que se producen durante el funcionamiento de Kaspersky Endpoint Security, incluidos los mensajes al administrador que se reciben de los usuarios de la red de área local.

3. Para configurar el filtro del evento, en la lista desplegable **Selecciones de eventos**, seleccione **Solicitudes de los usuarios**.

4. Seleccione el mensaje enviado al administrador.

5. Haga clic en el botón **Abrir ventana de propiedades del evento** en la parte derecha del espacio de trabajo de la consola de administración.

Gestión de informes

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la ejecución de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se registra en informes.

Los informes se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Los informes pueden contener siguientes datos de usuario:

- Rutas a archivos analizadas por Kaspersky Endpoint Security.
- Rutas a claves del registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
- Nombre de usuario de Microsoft Windows.
- Direcciones de páginas web abiertas por el usuario.

Los datos del informe se presentan en forma de tabla. Cada fila de la tabla contiene información sobre un evento independiente. Los atributos de eventos se encuentran en las columnas de la tabla. Algunas de las columnas son compuestas, que contienen columnas anidadas con atributos adicionales. Para ver atributos adicionales, haga clic en el botón ⊞ situado junto al nombre de la columna. Los eventos que se registran durante el funcionamiento de los diversos componentes o durante el rendimiento de las distintas tareas cuentan con distintos grupos de atributos.

Están disponibles los siguientes informes:

- Informe **Auditoría del sistema**. Contiene información acerca de los eventos producidos durante la interacción entre el usuario y la aplicación, y durante el funcionamiento de la aplicación en general, que no está relacionado con ningún componente o tarea de Kaspersky Endpoint Security en particular.
- Informes sobre el funcionamiento de componentes de Kaspersky Endpoint Security.
- Informes de tarea de Kaspersky Endpoint Security.
- Informe **Cifrado de datos**. Contiene información sobre eventos que tienen lugar durante el cifrado y el descifrado de datos.

Los informes usan los siguientes niveles de importancia de eventos:

ⓘ **Mensajes de información**. Eventos de referencia que, por lo general, no contienen información importante.

⚠ **Advertencias**. Eventos a los que se debe prestar atención porque reflejan situaciones importantes en el funcionamiento de Kaspersky Endpoint Security.

⓪ **Eventos críticos**. Eventos de importancia fundamental que indican problemas en el funcionamiento de Kaspersky Endpoint Security o vulnerabilidades en la protección del equipo del usuario.

Para un procesamiento apropiado de los informes, puede modificar la presentación de los datos en la pantalla de los modos siguientes:

- Filtrado de la lista de eventos por diversos criterios.
- Uso de la función de búsqueda para buscar un determinado evento.
- Visualización del evento seleccionado en una sección independiente.
- Orden de las listas de eventos por cada columna del informe.
- Muestre y oculte eventos agrupados por el filtro de eventos con el botón ⊞.
- Cambio del orden y la disposición de las columnas que se muestran en el informe.

Puede guardar un informe generado en un archivo de texto, si es necesario. También puede eliminar información de informes sobre las tareas y los componentes de Kaspersky Endpoint Security que se combinan en grupos.

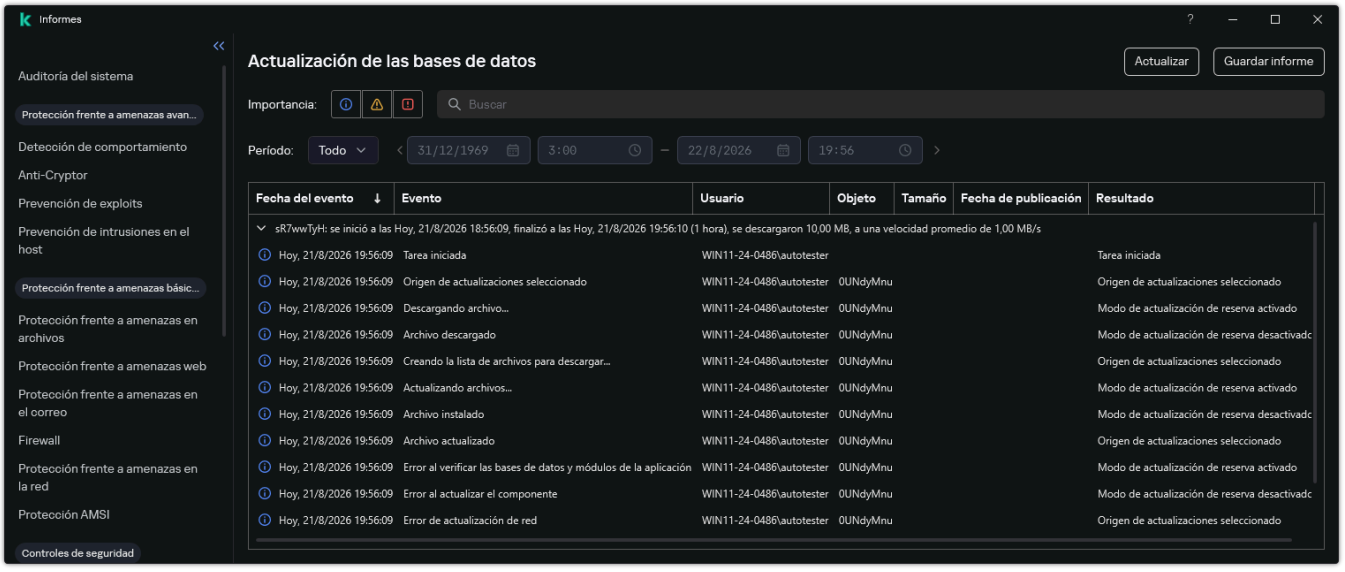
Si Kaspersky Endpoint Security funciona mediante la gestión de Kaspersky Security Center, la información sobre los eventos se puede transmitir al Servidor de administración de Kaspersky Security Center (para obtener más información, consulte la Ayuda de Kaspersky Security Center).

Ver informes

Si un usuario puede ver informes, el usuario también puede ver todos los eventos reflejados en los informes.

Para visualizar informes:

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Informes**.



Informes

2. En la lista de componentes y tareas, seleccione un componente o una tarea.

   En la parte derecha de la ventana se muestra un informe que contiene una lista de eventos provenientes del funcionamiento del componente o la tarea seleccionados de Kaspersky Endpoint Security. Puede clasificar eventos en el informe según los valores de las celdas de una de las columnas.

3. Para ver información detallada de un evento, seleccione el evento en el informe.

En la parte inferior de la ventana se muestra un bloque con el resumen de eventos.

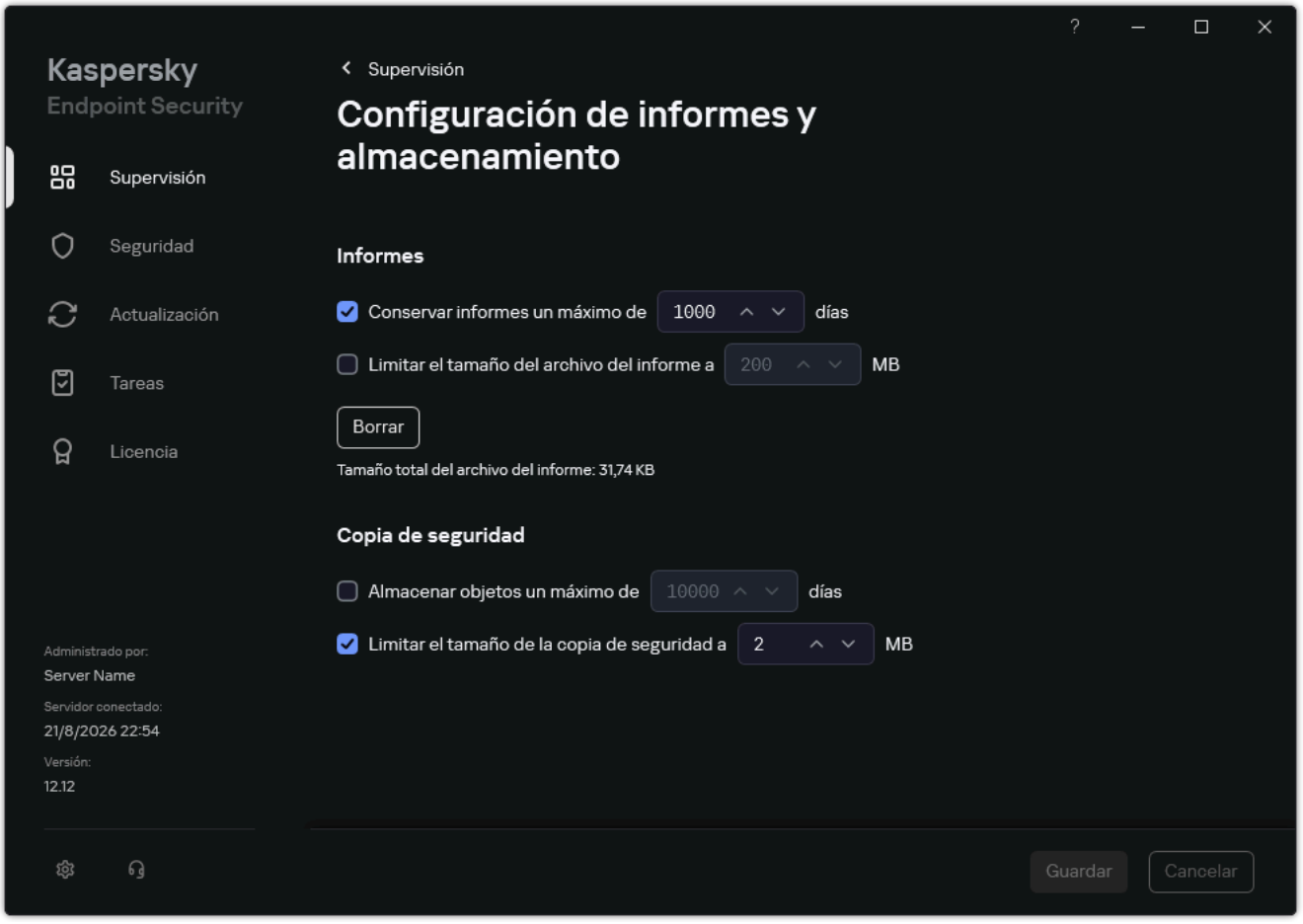
Configuración del período máximo de almacenamiento del informe

El período de almacenamiento máximo predeterminado de los informes sobre eventos registrados por Kaspersky Endpoint Security es de 30 días. Después de dicho período de tiempo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.

Para modificar el plazo máximo de almacenamiento de informes:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el mosaico **Informes y almacenamiento**.



Configuración de informe

3. Si desea limitar el período de almacenamiento del informe, seleccione la casilla **Conservar informes un máximo de N días** en el bloque **Informes**. Definir el período máximo de almacenamiento del informe

4. Guarde los cambios.

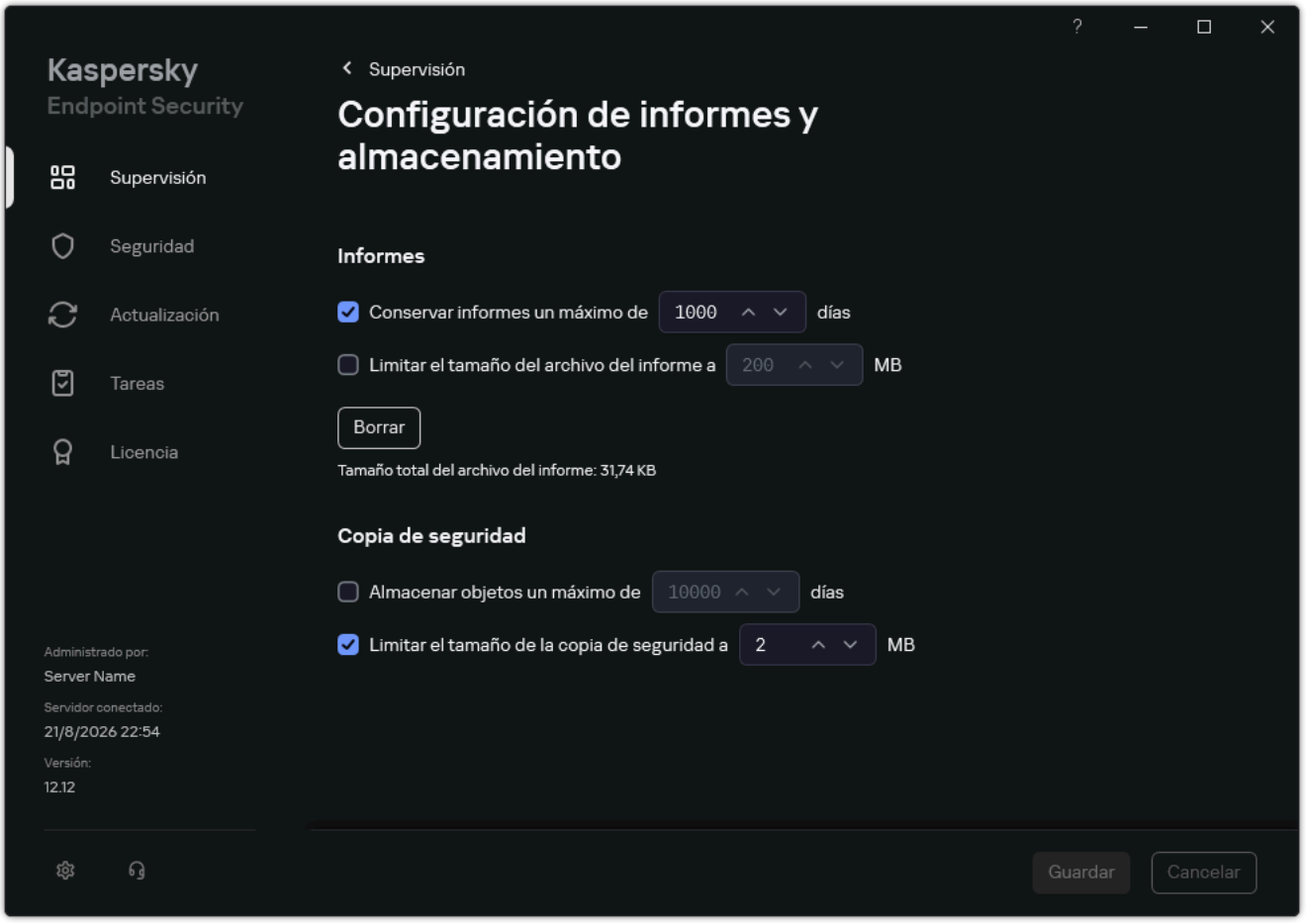
Configuración del tamaño máximo del archivo del informe

Puede especificar el tamaño máximo del archivo que contiene el informe. De forma predeterminada, el tamaño máximo de archivo del informe es de 1024 MB. Para evitar superar el tamaño máximo de archivo de informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo de informe cuando se alcance el tamaño máximo en el archivo de informe.

Para configurar el tamaño máximo del archivo del informe, haga lo siguiente:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el mosaico **Informes y almacenamiento**.



Configuración de informe

3. En el bloque **Informes**, seleccione la casilla **Limitar el tamaño del archivo del informe a N MB** si desea limitar el tamaño de un archivo del informe. Definir el tamaño máximo del archivo del informe

4. Guarde los cambios.

Almacenamiento de informes en archivos

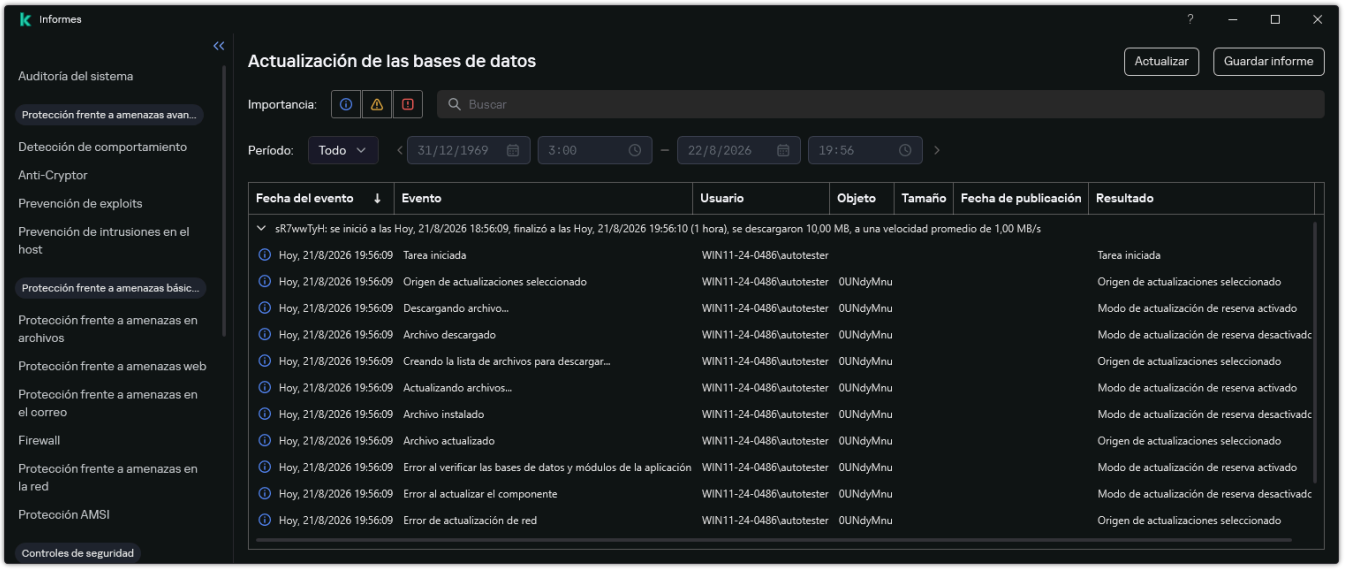
El usuario es personalmente responsable de garantizar la seguridad de información desde un informe guardado al archivo y, en particular, para controlar y restringir el acceso a esta información.

Puede guardar el informe que se genera en un archivo en formato de texto (TXT) o un archivo CSV.

Kaspersky Endpoint Security registra eventos en el informe tal y como se muestran en la pantalla, es decir, con el mismo conjunto y secuencia de atributos de eventos.

Para guardar el informe en un archivo:

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Informes**.



Informes

2. Esto abre una ventana donde debe seleccionar el componente o la tarea.

   En la parte derecha de la ventana, se muestra un informe que contiene una lista de eventos en el funcionamiento del componente o tarea seleccionado de Kaspersky Endpoint Security.

3. Si fuera necesario, puede modificar la presentación de los datos en el informe haciendo lo siguiente:

   - Filtrando eventos
   - Realizando una búsqueda de eventos
   - Reorganizando columnas
   - Ordenando eventos

4. Haga clic en el botón **Guardar informe** en la parte superior derecha de la ventana.

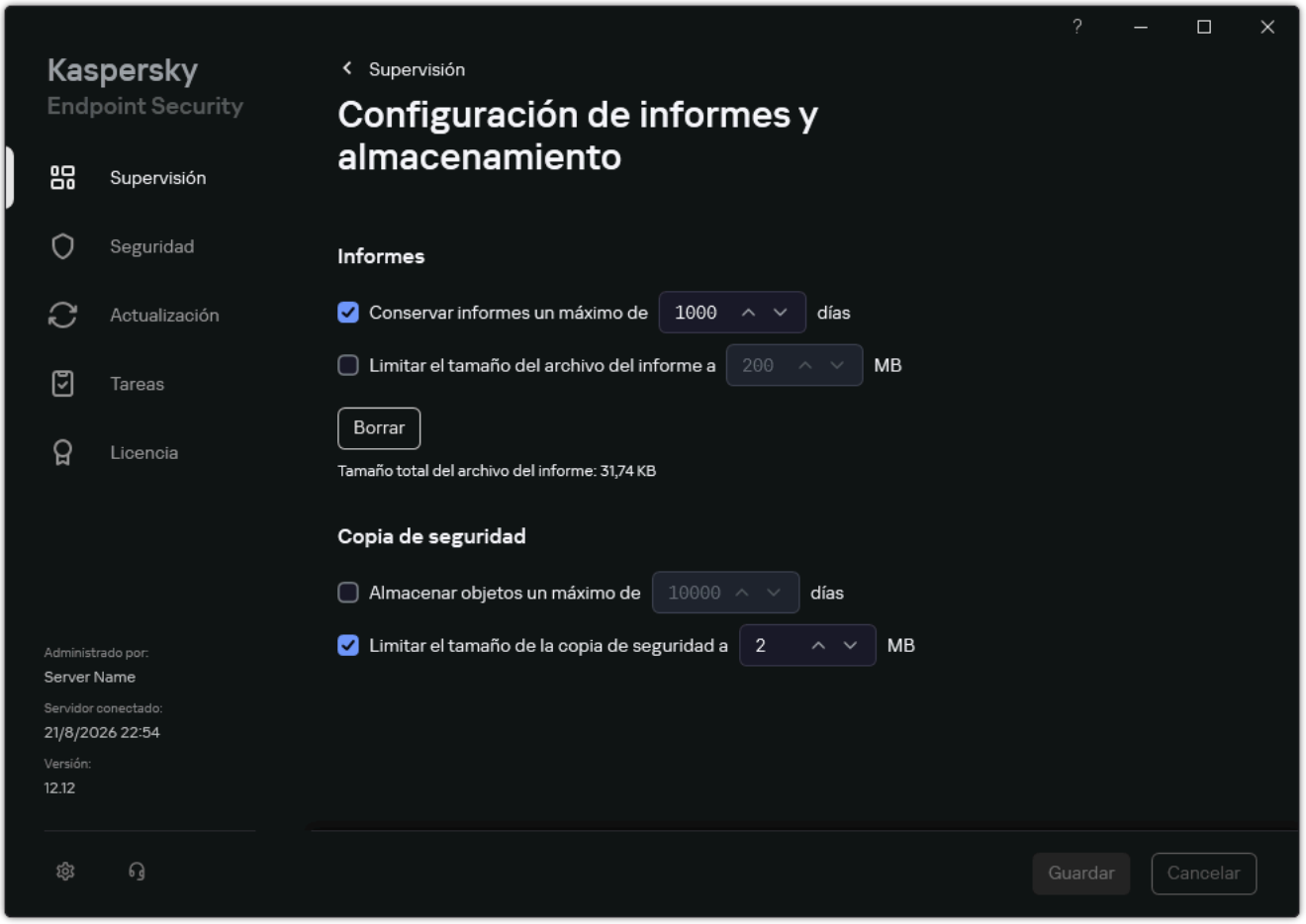
5. En la ventana que se abre, especifique la carpeta de destino para el archivo del informe.

6. Escriba el nombre del archivo del informe.
7. Elija el formato de archivo de informe necesario: TXT o CSV.
8. Guarde los cambios.

Limpieza de informes

Para quitar información de los informes:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el mosaico **Informes y almacenamiento**.



Configuración de informe

3. En el bloque **Informes**, haga clic en el botón **Borrar**.
4. Si la Protección con contraseña está activada, Kaspersky Endpoint Security puede solicitarle las credenciales de la cuenta de usuario. La aplicación solicita las credenciales de la cuenta si el usuario no tiene el permiso necesario.

Kaspersky Endpoint Security eliminará todos los informes de todos los componentes y tareas de la aplicación.

Autoprotección de Kaspersky Endpoint Security

Autoprotección evita que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de Kaspersky Endpoint Security y, por ejemplo, eliminar Kaspersky Endpoint Security del equipo. El conjunto de tecnologías de Autoprotección disponibles para Kaspersky Endpoint Security depende de si el sistema operativo es de 32 o 64 bits (consulte la tabla a continuación). La autodefensa también incluye Protección con contraseña y Protección de conexión al Servidor de administración.

Protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).

Protección de la conexión del Servidor de administración evita la reconexión no autorizada del equipo a un servidor que no es de confianza.

Tecnologías de Autoprotección de Kaspersky Endpoint Security

Tecnología	Descripción	Equipo x86	Equipo x64
Mecanismo de Autoprotección	La tecnología bloquea el acceso a los siguientes componentes de la aplicación: • archivos en la carpeta de instalación de Kaspersky Endpoint Security y otros archivos de la aplicación; • claves de registro con informes pertenecientes a la aplicación; • procesos que la aplicación ejecuta.	✓	✓
AM-PPL (Antimalware Protected Process Light)	La tecnología protege los procesos de Kaspersky Endpoint Security frente a acciones maliciosas. Para obtener más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019.	✓	✓
Mecanismo de protección de gestión externa	Esta tecnología evita que otras aplicaciones (por ejemplo, TeamViewer o RemotelyAnywhere) obtengan acceso a Kaspersky Endpoint Security.	✓	– (excepto para Windows 7)

Activación y desactivación de Autoprotección

Kaspersky Endpoint Security impide la modificación o eliminación de los archivos de la aplicación en el disco duro, los procesos de memoria y las entradas en el Registro del sistema.

La tecnología bloquea el acceso a los siguientes componentes de la aplicación:

- archivos en la carpeta de instalación de Kaspersky Endpoint Security y otros archivos de la aplicación;
- claves de registro con informes pertenecientes a la aplicación;
- procesos que la aplicación ejecuta.

Los mecanismos de Autodefensa no se aplican a los procesos de Kaspersky Endpoint Security iniciados por procesos principales que no son de confianza.

El mecanismo de autoprotección de Kaspersky Endpoint Security está activado de forma predeterminada.

Cómo activar o desactivar la autoprotección en la Consola de administración (MMC)

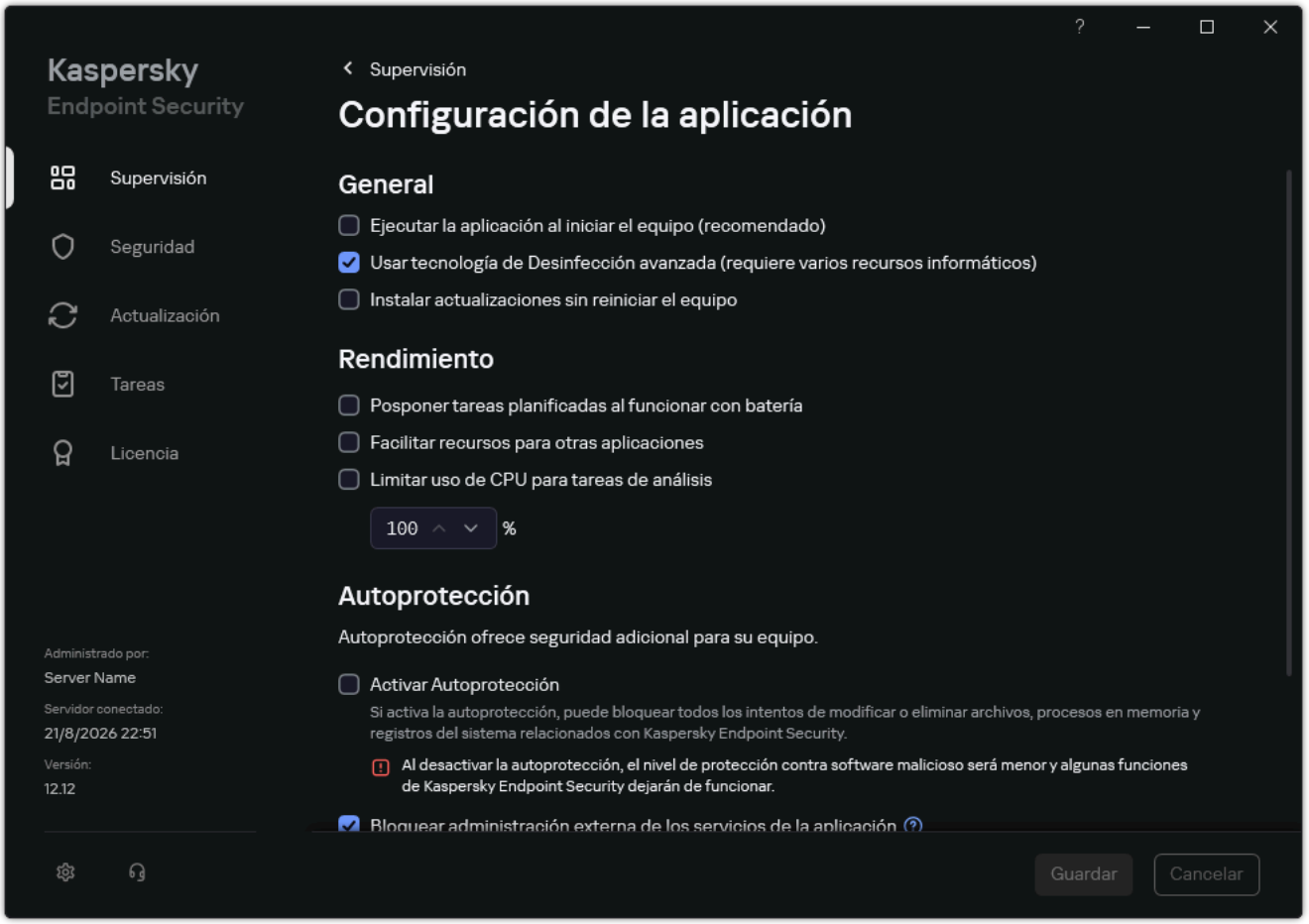
1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.
4. Utilice la casilla de verificación **Activar la autoprotección** para activar o desactivar el mecanismo Autoprotección.
5. Guarde los cambios.

Cómo activar o desactivar la autoprotección en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Autoprotección**.
5. Utilice el interruptor **Autoprotección ACTIVADA** para activar o desactivar el mecanismo Autoprotección.
6. Guarde los cambios.

Cómo activar o desactivar la autoprotección en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. Utilice la casilla de verificación **Activar Autoprotección** para activar o desactivar el mecanismo Autoprotección.
4. Guarde los cambios.

Activación y desactivación de la compatibilidad con AM-PPL

Kaspersky Endpoint Security es compatible con la tecnología Antimalware Protected Process Light (en adelante también llamada "AM-PPL") de Microsoft. AM-PPL protege los procesos de Kaspersky Endpoint Security frente a acciones maliciosas (por ejemplo, la finalización de la aplicación). AM-PPL solo permite la ejecución de procesos de confianza. Los procesos de Kaspersky Endpoint Security se firman de acuerdo con los requisitos de seguridad de Windows y, por lo tanto, son de confianza. Para obtener más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está activada de forma predeterminada.

Kaspersky Endpoint Security también tiene mecanismos integrados para proteger los procesos de las aplicaciones. La compatibilidad con AM-PPL le permite delegar funciones de seguridad de procesos al sistema operativo. De este modo, puede aumentar la velocidad de la aplicación y reducir el consumo de recursos informáticos.

Utilice la tecnología AM-PPL de forma continua. AM-PPL es un componente importante de la protección del sistema operativo. Desactivar la compatibilidad con AM-PPL puede hacer que algunas funciones de Kaspersky Endpoint Security fallen (por ejemplo, la integración de la aplicación con Windows Security Center). La desactivación de la compatibilidad con AM-PPL solo se permite en un entorno de prueba independiente con fines de resolución de problemas.

La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019.

Para activar o desactivar la tecnología AM-PPL:

1. Desactive el mecanismo Autoprotección de la aplicación.

   El mecanismo Autoprotección evita la modificación y eliminación de procesos de la aplicación en la memoria del equipo, incluido el cambio del estado de AM-PPL.

2. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.

3. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

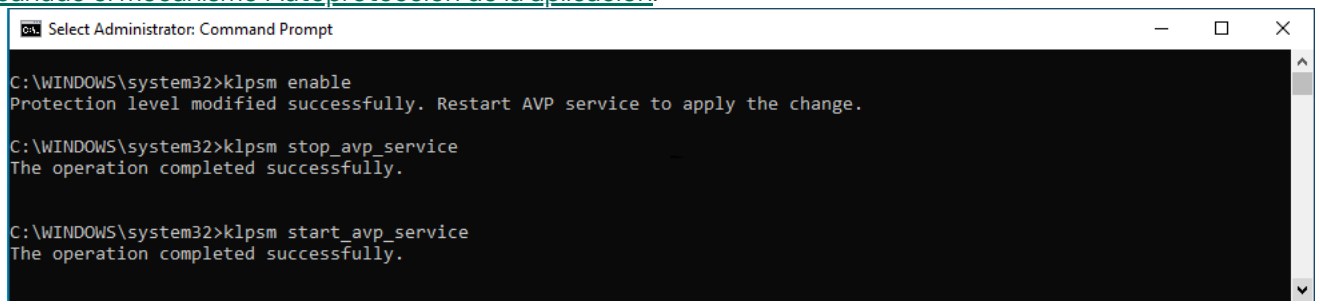
   Puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% durante la instalación de la aplicación.

4. Introduzca lo siguiente en la línea de comandos:

   - `klpsm.exe enable`. Active la compatibilidad con la tecnología AM-PPL (vea la imagen más abajo).
   - `klpsm.exe disable` – Desactive la compatibilidad con la tecnología AM-PPL.

5. Reinicie Kaspersky Endpoint Security.

6. Reanude el mecanismo Autoprotección de la aplicación.



Activación de la compatibilidad con la tecnología AM-PPL

Protección de los servicios de la aplicación contra gestión externa

La protección de los servicios de la aplicación contra gestión externa bloquea los intentos de los usuarios y de otras aplicaciones de detener los servicios de Kaspersky Endpoint Security Service. La protección garantiza el funcionamiento de los siguientes servicios:

- Kaspersky Endpoint Security Service (AVP.KES.14.2)
- Servicio Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

Para salir de la aplicación desde la línea de comandos, desactive la protección de los servicios de Kaspersky Endpoint Security contra la gestión externa.

Puede permitir la administración externa de los servicios de la aplicación solo en equipos que no admitan la tecnología AM-PPL o en equipos que tengan la tecnología desactivada.

Cómo activar o desactivar la Protección de los servicios de la aplicación contra la administración externa en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.
4. Utilice la casilla de verificación **Bloquear administración externa de los servicios de la aplicación** para activar o desactivar la protección de los servicios de Kaspersky Endpoint Security contra la gestión externa.
5. Guarde los cambios.

Cómo activar o desactivar la Protección de los servicios de la aplicación contra la administración externa en Web Console y Cloud Console

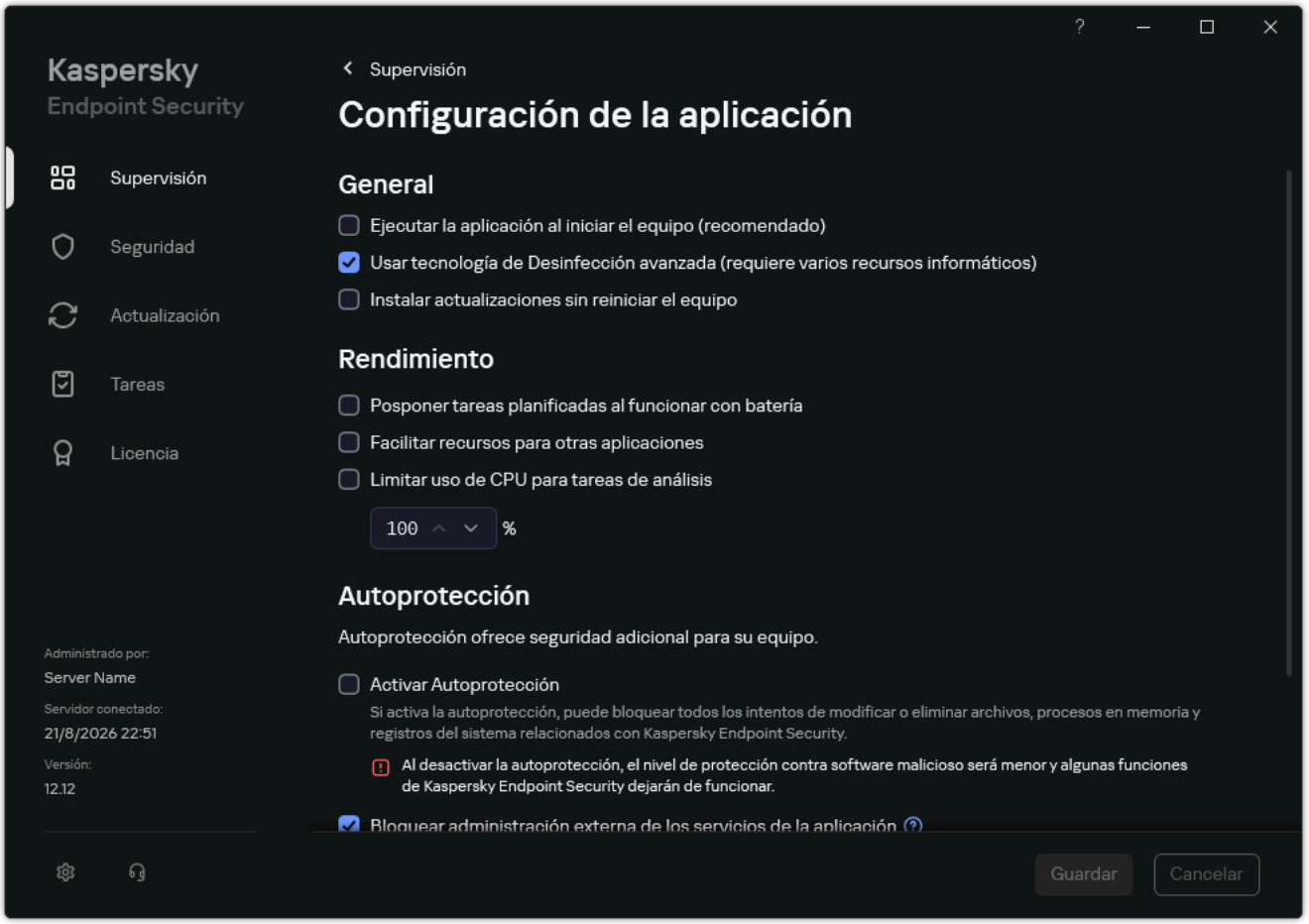
1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Autoprotección**.
5. Utilice la casilla de verificación **Bloquear la administración externa de los servicios de la aplicación** para activar o desactivar la protección de los servicios de Kaspersky Endpoint Security contra la gestión externa.
6. Guarde los cambios.

Cómo activar o desactivar la Protección de los servicios de la aplicación contra la administración externa en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Configuración general → Configuración de la aplicación**.

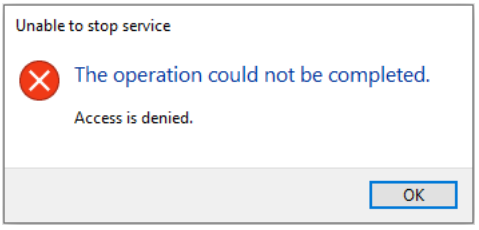


Configuración de Kaspersky Endpoint Security para Windows

3. Utilice la casilla de verificación **Bloquear administración externa de los servicios de la aplicación** para activar o desactivar la protección de los servicios de Kaspersky Endpoint Security contra la gestión externa.

4. Guarde los cambios.

Como resultado, cuando un usuario intenta detener los servicios de la aplicación, aparece una ventana del sistema con un mensaje de error. El usuario solo puede gestionar los servicios de la aplicación desde la interfaz de Kaspersky Endpoint Security.



Error de acceso a los servicios de la aplicación

Soporte de las aplicaciones de administración remota

Puede que alguna que otra vez necesite usar una aplicación de administración remota mientras está activada la protección de gestión externa.

Para activar el funcionamiento de las aplicaciones de administración remota:

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Exclusiones y tipos de objetos detectados**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. Seleccione el archivo ejecutable de la aplicación de administración remota.

   También puede ingresar la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.
6. Seleccione la casilla **Permitir interacción con la interfaz de Kaspersky Endpoint Security**.
7. Guarde los cambios.

Protección con contraseña

Varios usuarios con distintos niveles de conocimientos informáticos pueden usar un solo equipo. Si los usuarios cuentan con acceso ilimitado a Kaspersky Endpoint Security y su configuración, el nivel general de protección del equipo puede verse reducido. La protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).

Si el usuario que ha iniciado sesión en Windows (el *usuario de la sesión*) tiene el permiso necesario para realizar una acción, Kaspersky Endpoint Security no le solicita un nombre de usuario y contraseña o una contraseña temporal. El usuario obtiene acceso a Kaspersky Endpoint Security de conformidad con los permisos que tiene asignados.

Si el usuario de la sesión no tiene permitido realizar una acción, tiene las siguientes alternativas para obtener acceso a la aplicación:

- Introduzca un nombre de usuario y contraseña.

  Este método es conveniente para las operaciones cotidianas. Para realizar una acción protegida con contraseña, se introducen las credenciales de una cuenta de dominio perteneciente a un usuario con el permiso necesario. En este caso, el equipo debe estar en ese dominio. Si el equipo no está en el dominio, puede usar la cuenta de KLAdmin o una cuenta añadida manualmente.

- Introduzca una contraseña temporal.

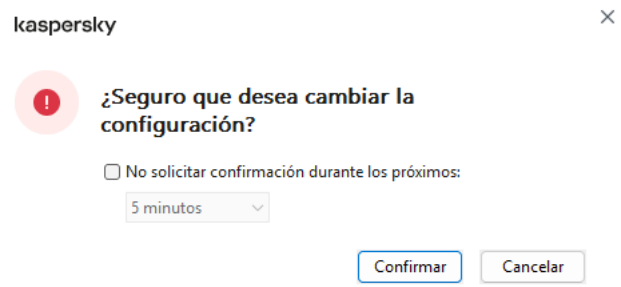
  Este método es conveniente para otorgar permisos temporales para realizar acciones bloqueadas (por ejemplo, salir de la aplicación) a usuarios fuera de la red corporativa. Cuando expira una contraseña temporal o se cierra una sesión, Kaspersky Endpoint Security revierte su configuración a su estado anterior.

- Token.

  Este método es adecuado para usuarios con privilegios (como el personal de soporte técnico). La autenticación mediante token permite usar el modo de inicio de sesión con tarjeta inteligente en Active Directory. Esto mejora la seguridad de la infraestructura de la organización.

Cuando un usuario intenta realizar una acción protegida con contraseña, Kaspersky Endpoint Security le solicita un nombre de usuario y una contraseña, la contraseña del token o una contraseña temporal (consulte la siguiente figura).

En la ventana de ingreso de contraseña, puede cambiar de idioma solo pulsando **ALT+SHIFT**. El uso de otros accesos directos, incluso si están configurados en el sistema operativo, no funcionan para cambiar de idioma.



Solicitud de contraseña de acceso a Kaspersky Endpoint Security

Nombre de usuario y contraseña

Para acceder a Kaspersky Endpoint Security, debe introducir las credenciales de la cuenta. La protección con contraseña admite las siguientes cuentas:

- **KLAdmin**. Una cuenta de administrado con acceso ilimitado a Kaspersky Endpoint Security. La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña. No se pueden revocar los permisos de la cuenta KLAdmin. Cuando habilita la protección con contraseña, Kaspersky Endpoint Security le solicita que configure una contraseña para la cuenta KLAdmin.

- **Cuenta añadida manualmente**. Una cuenta externa al dominio de Active Directory. Puede usar esta cuenta de servicio en lugar de KLAdmin si no desea compartir la contraseña de administrador. Puede establecer cualquier nombre de usuario y contraseña, y configurar permisos individuales.

- **El grupo Todos**. Un grupo integrado de Windows que incluye a todos los usuarios dentro de la red corporativa. Los usuarios del grupo Todos pueden acceder a la aplicación según los permisos que se le otorgan.

- **Usuarios o grupos individuales**. Las cuentas de usuario para las que puede configurar permisos individuales. Por ejemplo, si se bloquea una acción para el grupo Todos, puede autorizar esta acción para un usuario o un grupo individual.

- **Usuario de sesión**. La cuenta de usuario que inició la sesión de Windows. Puede cambiar a otro usuario de sesión cuando se solicite una contraseña (la casilla **Guardar contraseña para esta sesión**). En este caso, Kaspersky Endpoint Security considera usuario de la sesión al usuario cuyas credenciales de la cuenta se introdujeron, en lugar del usuario que inició la sesión de Windows.

Contraseña temporal

Se puede utilizar una contraseña temporal para otorgar acceso temporal a Kaspersky Endpoint Security a un equipo particular fuera de la red corporativa. El Administrador genera una contraseña temporal para un equipo particular en las propiedades del equipo de Kaspersky Security Center. El Administrador selecciona las acciones que se protegerán con la contraseña temporal y especifica el período de validez de la contraseña temporal.

Token

Para acceder a las funciones de Kaspersky Endpoint Security, debe seleccionar el certificado de usuario correspondiente en la lista de certificados almacenados en el token conectado e introducir su PIN. La autenticación mediante token solo está disponible para los usuarios del dominio de Active Directory. El administrador puede configurar permisos para un usuario concreto o un grupo. Para que funcione la autenticación mediante token, debe implementar una infraestructura de PKI de confianza e instalar software especial para administrar el token.

Activar la protección con contraseña

La protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).

Cómo activar la protección con contraseña en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Interfaz**.
4. En el bloque **Protección con contraseña**, haga clic en el botón **Configuración**.
   Esto abre una ventana con la configuración de Protección de contraseña.
5. Utilice la casilla de verificación **Activar la protección con contraseña** para activar o desactivar el componente.
6. En **Permisos**, seleccione la cuenta KLAdmin.
7. Esto abre una ventana; en ella, haga clic en **Contraseña** y establezca una contraseña para la cuenta KLAdmin.
   La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña.

   > Si olvidó la contraseña de su cuenta KLAdmin, puede restablecer la contraseña en las propiedades de la directiva.

8. Vuelva a la lista de cuentas.

9. Configure los permisos para todos los usuarios dentro de la red corporativa:

    a. En **Permisos**, seleccione el grupo "Todos".

    El grupo Todos es un grupo integrado de Windows que incluye a todos los usuarios dentro de la red corporativa.

    b. Si la ventana se abrió, seleccione las casillas ubicadas junto a las acciones que los usuarios podrán realizar sin introducir la contraseña.

    Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un usuario individual que tiene el permiso requerido, o si introduce una contraseña temporal.

    > Los permisos de la protección con contraseña tienen algunos aspectos importantes que se deben tener en cuenta. Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.

10. Guarde los cambios.

Cómo activar la Protección con contraseña en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

    Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.
5. En **Protección con contraseña**, use el interruptor **Protección con contraseña ACTIVADA** para activar o desactivar el componente.
6. Especifique la contraseña para la cuenta de KLAdmin y confírmela.

    La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña.

    > Si olvidó la contraseña de su cuenta KLAdmin, puede restablecer la contraseña en las propiedades de la directiva.

7. Vuelva a la lista de cuentas.
8. Configure los permisos para todos los usuarios dentro de la red corporativa:

    a. En la tabla de cuentas, seleccione el grupo "Todos".

    El grupo Todos es un grupo integrado de Windows que incluye a todos los usuarios dentro de la red corporativa.

    b. Si la ventana se abrió, seleccione las casillas ubicadas junto a las acciones que los usuarios podrán realizar sin introducir la contraseña.

Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un usuario individual que tiene el permiso requerido, o si introduce una contraseña temporal.

Los permisos de la protección con contraseña tienen algunos aspectos importantes que se deben tener en cuenta. Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.

9. Guarde los cambios.

Cómo activar la Protección con contraseña en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. Utilice interruptor **Protección con contraseña** para activar o desactivar el componente.
4. Especifique la contraseña para la cuenta de KLAdmin y confírmela.

   La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña.

   Si un equipo se está ejecutando bajo una directiva, el Administrador puede restablecer la contraseña para la cuenta de KLAdmin en las propiedades de la directiva. Si el equipo no está conectado a Kaspersky Security Center y ha olvidado la contraseña de la cuenta de KLAdmin, no es posible recuperar la contraseña.

5. Configure los permisos para todos los usuarios dentro de la red corporativa:

   a. En la tabla de la cuenta, haga clic en el botón **Editar** para abrir la lista de permisos para el grupo Todos.

   El grupo Todos es un grupo integrado de Windows que incluye a todos los usuarios dentro de la red corporativa.

   b. Seleccione las casillas ubicadas junto a las acciones que los usuarios podrán realizar sin introducir la contraseña.

   Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un usuario individual que tiene el permiso requerido, o si introduce una contraseña temporal.

   Los permisos de la protección con contraseña tienen algunos aspectos importantes que se deben tener en cuenta. Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.

6. Guarde los cambios.

Cuando se active la protección con contraseña, la aplicación restringirá el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron al grupo Todos. Solo puede realizar las acciones que están bloqueadas para el grupo Todos si utiliza la cuenta de KLAdmin, otra cuenta que tenga los permisos requeridos, o si introduce una contraseña temporal.

Para desactivar la protección con contraseña, deberá iniciar sesión con el usuario KLAdmin. La protección con contraseña no puede desactivarse cuando se está usando una contraseña temporal o cualquier otra cuenta.

Durante la comprobación de contraseña, puede seleccionar la casilla **Guardar contraseña para esta sesión**. En este caso, Kaspersky Endpoint Security no solicitará una contraseña cuando un usuario intente realizar otra acción protegida con contraseña durante la sesión.

Otorgarle permisos a usuarios o grupos individuales

La protección de contraseñas permite otorgar acceso a Kaspersky Endpoint Security a cuentas de usuario de Active Directory individuales y cuentas de usuario añadidas manualmente.

Cuentas de usuario de Active Directory

Puede otorgar a Kaspersky Endpoint Security acceso a usuario individuales o grupos en el dominio de Active Directory. Por ejemplo, si salir de la aplicación está bloqueado para el grupo Todos, puede otorgar el permiso para **Salir de la aplicación** a un usuario particular. Por lo tanto, solo puede salir de la aplicación si ha iniciado sesión como ese usuario o como KLAdmin.

Puede usar las credenciales de la cuenta para acceder a la aplicación solo si el equipo está en el dominio. Si el equipo no está en el dominio, puede usar la cuenta de KLAdmin o una contraseña temporal.

Cuentas de usuario añadidas manualmente

Puede crear una cuenta de usuario que no esté presente en Active Directory y asignar permisos individuales a dicha cuenta de usuario. Es decir, puede crear una *cuenta de usuario de servicios* y usarla en lugar de KLAdmin. De esta forma, no necesita compartir su contraseña de administrador de KLAdmin con otros usuarios o crear nuevas cuentas de usuario de Active Directory. Puede especificar cualquier nombre de usuario y contraseña. Por ejemplo, puede otorgar el **Ver informes** permiso a la cuenta de usuario del servicio. Como resultado, si visualizar informe se prohíbe al grupo "Todo", puede abrir los informes con la cuenta de usuario del servicio o la cuenta de usuario de KLAdmin.

Otorgarle permisos a usuarios o grupos individuales

Cómo otorgar permisos a usuarios individuales o grupos en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Interfaz**.
4. En el bloque **Protección con contraseña**, haga clic en el botón **Configuración**.

   Esto abre una ventana con la configuración de Protección de contraseña.
5. En la tabla de la cuenta, haga clic en **Añadir**.
6. Seleccione el tipo de cuenta de usuario que desea añadir:

   - **Seleccionar un usuario/grupo del directorio activo**: Cuentas de usuario de Active Directory.

     Para seleccionar una cuenta, haga clic en **Seleccionar**. Seleccione un usuario o un grupo de Active Directory y confirme su selección.

   - **Añadir manualmente un usuario o grupo de usuarios** para una cuenta de usuario de servicio añadida manualmente.

     Para añadir una cuenta de usuario del servicio, introduzca un nombre de usuario y una contraseña (por ejemplo, SecureAdmin).

     > Puede restablecer una contraseña de cuenta de usuario de servicio en la configuración de la directiva. La contraseña de la cuenta de usuario del servicio debe restablecerse de la misma forma que la contraseña de KLAdmin. Si se permite editar la configuración de Protección con contraseña (el "candado" está abierto) o no se aplica ninguna directiva en el equipo, puede restablecer la contraseña de la cuenta de usuario del servicio en la interfaz de la aplicación. Para ello, confirme los cambios en la información de la cuenta de usuario del servicio usando la contraseña de KLAdmin.
7. En la lista **Permisos**, seleccione las casillas que se encuentran junto a las acciones que el usuario o el grupo seleccionados podrán realizar sin que se les solicite una contraseña.

   Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un usuario individual que tiene el permiso requerido, o si introduce una contraseña temporal.

   > Los permisos de la protección con contraseña tienen algunos aspectos importantes que se deben tener en cuenta. Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.
8. Guarde los cambios.

Cómo otorgar permisos a usuarios individuales o grupos en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.
5. En el bloque **Protección con contraseña**, haga clic en el enlace **Permisos de usuario**.

   Esto abre el formulario para otorgar permisos de activación de contraseña.
6. Haga clic en **Añadir**.
7. Seleccione el tipo de cuenta de usuario que desea añadir:

   - **Seleccionar desde Active Directory**: Cuentas de usuario de Active Directory.

     Para seleccionar una cuenta, haga clic en **Modificar**. Seleccione un usuario o un grupo de Active Directory y confirme su selección.
   - **Añadir manualmente** para una cuenta de usuario de servicio añadida manualmente.

     Para añadir una cuenta de usuario del servicio, introduzca un nombre de usuario y una contraseña (por ejemplo, SecureAdmin).

     > Puede restablecer una contraseña de cuenta de usuario de servicio en la configuración de la directiva. La contraseña de la cuenta de usuario del servicio debe restablecerse de la misma forma que la contraseña de KLAdmin. Si se permite editar la configuración de Protección con contraseña (el "candado" está abierto) o no se aplica ninguna directiva en el equipo, puede restablecer la contraseña de la cuenta de usuario del servicio en la interfaz de la aplicación. Para ello, confirme los cambios en la información de la cuenta de usuario del servicio usando la contraseña de KLAdmin.
8. En la lista **Permisos**, seleccione las casillas que se encuentran junto a las acciones que el usuario o el grupo seleccionados podrán realizar sin que se les solicite una contraseña.

   Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un usuario individual que tiene el permiso requerido, o si introduce una contraseña temporal.

   > Los permisos de la protección con contraseña tienen algunos aspectos importantes que se deben tener en cuenta. Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.
9. Haga clic en **Añadir**.
10. Guarde los cambios.

Cómo otorgar permisos a usuarios individuales o grupos en la interfaz de usuario de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.

3. En la tabla de la cuenta, haga clic en **Añadir**.

4. Seleccione el tipo de cuenta de usuario que desea añadir:

   - **Seleccionar un usuario/grupo del directorio activo**: Cuentas de usuario de Active Directory.

     Para seleccionar una cuenta, haga clic en **Seleccionar usuario o grupo**. Seleccione un usuario o un grupo de Active Directory y confirme su selección.

   - **Añadir un usuario manualmente** para una cuenta de usuario de servicio añadida manualmente.

     Para añadir una cuenta de usuario del servicio, introduzca un nombre de usuario y una contraseña (por ejemplo, SecureAdmin).

     Puede restablecer una contraseña de cuenta de usuario de servicio en la configuración de la directiva. La contraseña de la cuenta de usuario del servicio debe restablecerse de la misma forma que la contraseña de KLAdmin. Si se permite editar la configuración de Protección con contraseña (el "candado" está abierto) o no se aplica ninguna directiva en el equipo, puede restablecer la contraseña de la cuenta de usuario del servicio en la interfaz de la aplicación. Para ello, confirme los cambios en la información de la cuenta de usuario del servicio usando la contraseña de KLAdmin.

5. En la lista **Permisos**, seleccione las casillas que se encuentran junto a las acciones que el usuario o el grupo seleccionados podrán realizar sin que se les solicite una contraseña.

   Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un usuario individual que tiene el permiso requerido, o si introduce una contraseña temporal.

   Los permisos de la protección con contraseña tienen algunos aspectos importantes que se deben tener en cuenta. Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.

6. Guarde los cambios.

Por lo tanto, si está restringido el acceso a la aplicación para el grupo Todos, los usuarios recibirán permisos para acceder a Kaspersky Endpoint Security según los permisos individuales de los usuarios.

Utilizar una contraseña temporal para otorgar permisos

Se puede utilizar una contraseña temporal para otorgar acceso temporal a Kaspersky Endpoint Security a un equipo particular fuera de la red corporativa. Esto es necesario para permitir que el usuario realice una acción bloqueada sin obtener las credenciales de la cuenta KLAdmin. Para utilizar una contraseña temporal, se debe añadir el equipo a Kaspersky Security Center.

Cómo permitir que un usuario realice una acción bloqueada con una contraseña temporal a través de la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.

4. Haga doble clic para abrir la ventana de propiedades del equipo.

5. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky que están instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.2)** y haga doble clic para abrir las propiedades de la aplicación.
7. En la ventana de configuración de la aplicación, seleccione **Configuración general → Interfaz**.
8. En el bloque **Protección con contraseña**, haga clic en el botón **Configuración**.
9. En la ventana que se abre, en el bloque **Contraseña temporal**, haga clic en el botón **Lista de contraseñas temporales**.

   La ventana Administración de contraseñas temporales se abre.
10. Haga clic en **Añadir**.
11. En el campo **Fecha de caducidad**, especifique la fecha de caducidad en la que expirará la contraseña temporal.
12. En la tabla **Cobertura de la contraseña temporal**, seleccione las casillas que se encuentran junto a las acciones que estarán disponibles para el usuario después de introducir la contraseña temporal.
13. Haga clic en **Generar**.

    Se abrirá una ventana que contiene la contraseña temporal (consulte la siguiente figura).
14. Copie la contraseña y proporciónesela al usuario.

Cómo permitir que un usuario realice una acción bloqueada con una contraseña temporal a través de Web Console y Cloud Console

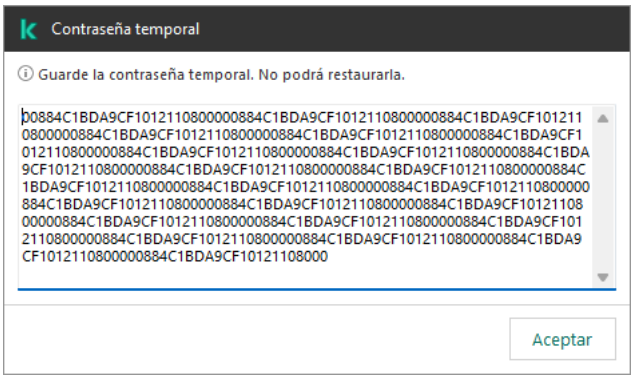
1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Haga clic en el nombre del equipo en el que quiere permitir que un usuario realice una acción bloqueada.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. En la ventana de configuración de la aplicación, seleccione **Configuración general → Interfaz**.
7. En el bloque **Contraseñas temporales**, haga clic en el botón **Añadir**.
8. En el campo **Fecha de caducidad**, especifique la fecha de caducidad en la que expirará la contraseña temporal.
9. En la tabla **Cobertura de la contraseña temporal**, seleccione las casillas que se encuentran junto a las acciones que estarán disponibles para el usuario después de introducir la contraseña temporal.

10. Haga clic en **Generar**.

    Se abre una ventana con la contraseña temporal.

11. Copie la contraseña y proporciónesela al usuario.

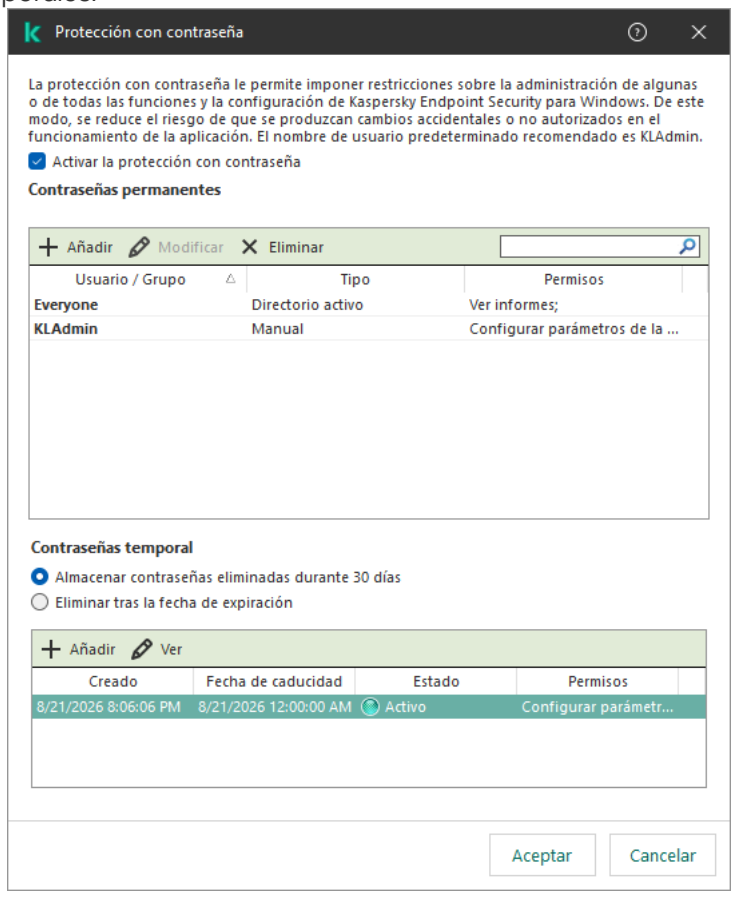


Contraseña temporal

Revocación de contraseña temporal

A partir de la versión 12.9, Kaspersky Endpoint Security para Windows incluye la función de *administración de contraseñas temporales*. La administración de contraseñas temporales le permite realizar las siguientes acciones:

- Guardar el historial de contraseñas (hasta 30 días).
- Supervisar el estado de la contraseña temporal: *Activo*, *Caducado*, *Revocado*.
- Revocar contraseñas temporales.



Administración de contraseñas temporales

La administración de contraseñas temporales actualiza el estado de la contraseña y la revoca solo después de sincronizar el equipo con Kaspersky Security Center.

Cómo revocar la contraseña temporal usando la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Haga doble clic para abrir la ventana de propiedades del equipo.
5. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky que están instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.2)** y haga doble clic para abrir las propiedades de la aplicación.
7. En la ventana de configuración de la aplicación, seleccione **Configuración general → Interfaz**.
8. En el bloque **Protección con contraseña**, haga clic en el botón **Configuración**.
9. Esto abre una ventana; en ella, bajo **Contraseña temporal**, configure el parámetro de almacenamiento para las contraseñas caducadas.
10. Haga clic en **Lista de contraseñas temporales**.

    La ventana Administración de contraseñas temporales se abre. La administración de contraseñas temporales muestra la fecha de caducidad de la contraseña, el estado de la contraseña y la lista de permisos.
11. Seleccione la contraseña temporal activa que desea revocar y haga doble clic en la contraseña para abrir sus propiedades.
12. En la ventana que se abre, haga clic en el botón **Revocar**.
13. Guarde los cambios. Para aplicar la directiva en equipos, cierre los candados .

Cómo revocar una contraseña temporal usando Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Haga clic en el nombre del equipo en el que quiere permitir que un usuario realice una acción bloqueada.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.

    Se abre la configuración local de la aplicación.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. En la ventana de configuración de la aplicación, seleccione **Configuración general → Interfaz**.
7. En **Contraseñas temporales**, configure el almacenamiento de contraseñas caducadas.

8. Haga clic en el enlace **Contraseña temporal**.

   La ventana Administración de contraseñas temporales se abre. La administración de contraseñas temporales muestra la fecha de caducidad de la contraseña, el estado de la contraseña y la lista de permisos.

9. Seleccione la contraseña temporal activa que desea revocar.

10. En la ventana que se abre, haga clic en el botón **Revocar contraseña**.

11. Guarde los cambios. Para aplicar la directiva en equipos, cierre los candados .

Como resultado, la Administración de contraseñas temporales establece el estado de la contraseña en *Revocando (sincronizando con un host)*. Después de sincronizar el equipo con Kaspersky Security Center, la aplicación revoca la contraseña temporal y bloquea los permisos otorgados inmediatamente.

Aspectos especiales de los permisos de la protección con contraseña

Los permisos de la protección con contraseña tienen algunos aspectos y limitaciones importantes que se deben tener en cuenta.

Configurar parámetros de la aplicación

Si el equipo de un usuario se está ejecutando bajo una directiva, asegúrese que toda las configuraciones requeridas de la directiva puedan modificarse (los atributos estén abiertos).

Salir de la aplicación

No hay consideraciones ni limitaciones especiales.

Desactivar componentes de protección

- No se puede otorgar el permiso para desactivar los componentes de protección para el grupo "Todos". Para permitir que otros usuarios además de KLAdmin desactiven los componentes de control, añada un usuario o un grupo que tenga permiso de **Desactivar componentes de protección** en la configuración de la protección con contraseña.
- Si el equipo de un usuario se está ejecutando bajo una directiva, asegúrese que toda las configuraciones requeridas de la directiva puedan modificarse (los atributos estén abiertos).
- Para desactivar los componentes de protección en la configuración de la aplicación, un usuario debe tener el permiso **Configurar parámetros de la aplicación**.
- Para desactivar los componentes de protección a través del menú contextual (usando el elemento de menú **Pausar la protección**), el usuario debe tener el permiso **Desactivar componentes de protección** además del permiso **Desactivar componentes de control**.

Desactivar componentes de control

- No se puede otorgar el permiso para desactivar los componentes de control para el grupo "Todos". Para permitir que otros usuarios además de KLAdmin desactiven los componentes de control, añada un usuario o un grupo que tenga permiso de **Desactivar componentes de control** en la configuración de la protección con contraseña.
- Si el equipo de un usuario se está ejecutando bajo una directiva, asegúrese que toda las configuraciones requeridas de la directiva puedan modificarse (los atributos estén abiertos).
- Para desactivar los componentes de control en la configuración de la aplicación, un usuario debe tener el permiso **Configurar parámetros de la aplicación**.
- Para desactivar los componentes de control desde el menú contextual (usando el elemento del menú **Pausar la protección**), el usuario debe tener el permiso **Desactivar componentes de control** además del permiso **Desactivar componentes de protección**.

Desactivar la directiva de Kaspersky Security Center

No es posible asignar al grupo "Everyone" el permiso para deshabilitar la directiva de Kaspersky Security Center. Para que KLAdmin no sea el único usuario autorizado a desactivar la directiva, añada un usuario o grupo que tenga el permiso **Desactivar la directiva de Kaspersky Security Center** en la configuración de la protección con contraseña.

Eliminar clave

No hay consideraciones ni limitaciones especiales.

Eliminar/modificar/restaurar la aplicación

Si ha permitido eliminar, modificar y restaurar la aplicación para el grupo "Todos", Kaspersky Endpoint Security no solicita una contraseña cuando el usuario intenta llevar a cabo estas operaciones. Por lo tanto, cualquier usuario, incluidos aquellos usuarios fuera del dominio, puede instalar, modificar o restaurar la aplicación.

Restaurar el acceso a los datos en los dispositivos cifrados

Solo puede restaurar el acceso a los datos y a las unidades cifradas si ha iniciado sesión como KLAdmin. No se le puede otorgar a ningún otro usuario el permiso para realizar esta acción.

Ver informes

No hay consideraciones ni limitaciones especiales.

Restaurar desde copia de seguridad

No hay consideraciones ni limitaciones especiales.

Exportar configuración

De forma predeterminada, se deniega la exportación de la configuración de la aplicación al grupo "Todos". Puede exportar la configuración de la aplicación mediante la cuenta de usuario de KLAdmin. Exportar la configuración de la aplicación solo incluye la creación de un archivo de configuración con la configuración de Kaspersky Endpoint Security en la interfaz de la aplicación. El permiso no restringe la exportación de listas de exclusiones de análisis, direcciones web de confianza, dispositivos de confianza u otras listas mantenidas por los componentes de la aplicación.

Restablecimiento de la contraseña de KLAdmin

Si olvidó la contraseña de su cuenta KLAdmin, puede restablecer la contraseña en las propiedades de la directiva. No puede restablecer la contraseña en la interfaz de la aplicación.

Puede realizar acciones protegidas con contraseña mediante una contraseña temporal. En este caso, no es necesario que introduzca las credenciales de KLAdmin.

Si el equipo no está conectado a Kaspersky Security Center y ha olvidado la contraseña de la cuenta de KLAdmin, no es posible recuperar la contraseña.

Cómo restablecer la contraseña de la cuenta KLAdmin mediante la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Interfaz**.
4. En el bloque **Protección con contraseña**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, desactive la casilla de verificación **Activar la protección con contraseña**.
6. Guarde los cambios.
7. Vuelva a seleccionar la casilla de verificación **Activar la protección con contraseña**.

8. Haga clic en **Aceptar**.
   Esto abre la ventana de la contraseña del administrador.
9. Especifique la contraseña nueva para la cuenta de KLAdmin y confírmela.
10. Guarde los cambios.

Cómo restablecer la contraseña de la cuenta KLAdmin en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.
2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.
   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows 14.2**.
   Se abre la configuración local de la aplicación.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Vaya a **Configuración general** → **Autoprotección**.
7. En **Protección con contraseña**, desactive el conmutador **Protección con contraseña**.
8. Guarde los cambios.
9. Vuelva a encender el interruptor **Protección con contraseña**.
10. Especifique la contraseña nueva para la cuenta de KLAdmin y confírmela.
11. Guarde los cambios.

Como resultado, la contraseña de su cuenta KLAdmin se actualiza después de aplicar la directiva.

Protección de conexión al Servidor de administración

La conexión del equipo al servidor de administración se realiza mediante el componente *Agente de red* de Kaspersky Security Center. Si un intruso tiene derechos suficientes para modificar la configuración de conexión del servidor, existe el riesgo de que el equipo se conecte a un servidor no fiable. Esto permitiría que el intruso aplicara sus propias directivas de grupo y, por ejemplo, desactivase la autoprotección de la aplicación. Kaspersky Endpoint Security puede evitar la reconexión no autorizada de un equipo a un servidor distinto. Para proteger la conexión del servidor, la aplicación sugiere establecer una contraseña y usar la Password-Based key Derivation Function (PBKDF2). Como resultado, resulta imposible acceder a la aplicación sin contraseña.

Para asegurar una protección completa de Kaspersky Endpoint Security y el Agente de red ante accesos no autorizados, recomendamos activar la protección adicional. Para la seguridad de Kaspersky Endpoint Security, recomendamos activar la Protección con contraseña. Para proteger el Agente de red, recomendamos establecer una contraseña de desinstalación. Para obtener información sobre la protección del Agente de red ante eliminaciones, consulte la Ayuda de Kaspersky Security Center.

La administración de la conexión del equipo al servidor de administración se realiza mediante la tarea *Protección de la conexión al servidor de administración*. La tarea le permite realizar las siguientes acciones:

- Establecer una contraseña para proteger la conexión del servidor.
- Cambiar la contraseña.
- Reconectar el equipo a un servidor distinto.
- Desactivar la protección de conexión del servidor.

Autenticar el equipo al conectar al servidor de administración

Tras establecer una contraseña, la aplicación crea una matriz de datos usando la transformación PBKDF2 de la contraseña. A continuación, la aplicación cifra esta matriz de datos mediante la clave del Agente de red. La aplicación usa la matriz de datos cifrada para comprobar los derechos y privilegios del servidor de administración en las conexiones posteriores.

Por tanto, siempre que se intenta reconectar el equipo al servidor de administración, la aplicación descifra la matriz de datos con la clave del Agente de red y la compara con la copia local. Si no coinciden, el acceso a la aplicación se restringe.

Protección de conexión al Servidor de administración

Cómo establecer una contraseña para proteger la conexión al servidor en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2) → Protección de la conexión al servidor de administración**.

Paso 2. Proteger la conexión al servidor de administración

Establezca una contraseña para proteger la conexión del servidor:

1. En **Protección de la conexión al servidor de administración**, seleccione **Proteger con contraseña**.
2. En la lista desplegable **Servidor de administración**, seleccione **Nuevo servidor**.
3. En el campo **Contraseña de conexión al servidor de administración**, establezca una contraseña para la conexión al servidor de administración y confírmela.

   Si olvida la contraseña, puede cambiarla usando una tarea.
4. Si tiene Kaspersky Endpoint Security 12.7 o una versión anterior de la aplicación implementada, seleccione la casilla **Activar compatibilidad de cifrado mediante contraseña para versiones anteriores de la aplicación (12.7 e inferiores)**.

   A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si ha implementado Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desactive esta casilla y utilice el cifrado de contraseña más seguro. Las versiones anteriores de la aplicación no admiten el cifrado de contraseña seguro. Para ejecutar la tarea, debe seleccionar la casilla de verificación.

Paso 3. Selección de la cuenta para ejecutar la tarea

Seleccione **Cuenta preconfigurada**. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

Paso 4. Configurar una planificación de inicio de tarea

En **Inicio programado**, seleccione **Manualmente**.

Paso 5. Definir el nombre de la tarea

Introduzca un nombre para la tarea; por ejemplo, *Contraseña de conexión al servidor principal*.

Paso 6. Conclusión de la creación de tareas

Finalice el asistente. Seleccione la casilla **Ejecutar la tarea después de que finalice el asistente** o ejecute la tarea manualmente. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo establecer una contraseña para proteger la conexión al servidor en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Protección de la conexión al servidor de administración**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve; por ejemplo, *Contraseña de conexión al servidor principal*.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta de usuario predeterminada. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Seleccione la tarea **Protección de la conexión al servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. En **Protección de la conexión al servidor de administración**, seleccione **Proteger con contraseña**.

10. En la lista desplegable **Conexión al servidor de administración**, seleccione **Nueva contraseña**.

11. En el campo **Contraseña de conexión al servidor de administración**, establezca una contraseña para la conexión al servidor de administración y confírmela.

    Si olvida la contraseña, puede cambiarla usando una tarea.

12. Si tiene Kaspersky Endpoint Security 12.7 o una versión anterior de la aplicación implementada, seleccione la casilla **Activar compatibilidad de cifrado mediante contraseña para versiones anteriores de la aplicación (12.7 e inferiores)**.

    A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si ha implementado Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desactive esta casilla y utilice el cifrado de contraseña más seguro. Las versiones anteriores de la aplicación no admiten el cifrado de contraseña seguro. Para ejecutar la tarea, debe seleccionar la casilla de verificación.

13. Guarde los cambios.

14. Active la casilla ubicada junto a la tarea.

15. Haga clic en **Iniciar**.

Puede supervisar el estado de la tarea y el número de dispositivos en los que se completó correctamente o con errores.

Reconectar el equipo a un servidor de administración distinto

Para reconectar el equipo a un servidor de administración distinto hay que seguir estos pasos:

1. En la consola del servidor de `[KSC1]` actual, ejecute la tarea *Cambiar Servidor de administración* para el Agente de red.

   Tras ejecutar la tarea, el equipo se reconecta al nuevo servidor de `[KSC2]`.

   El equipo aparecerá en la consola del servidor `[KSC1]` con el estado *Crítico* . Configurar la aplicación mediante directivas o ejecutando tareas de forma remota en el equipo es imposible.

2. En la consola del nuevo servidor de `[KSC2]`, cree una nueva tarea *Protección de la conexión al servidor de administración* para Kaspersky Endpoint Security. En las propiedades de la tarea, introduzca la contraseña del servidor anterior y establezca una contraseña para el nuevo servidor.

   Cómo establecer una nueva contraseña para reconectar a un nuevo servidor en la Consola de administración (MMC)

   1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

      Se abre la lista de tareas.

   2. Haga clic en **Nueva tarea**.

   El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Protección de la conexión al servidor de administración**.

Paso 2. Proteger la conexión al servidor de administración

Establezca una contraseña para proteger la conexión al nuevo Servidor de administración:

1. En **Protección de la conexión al servidor de administración**, seleccione **Proteger con contraseña**.
2. En la lista desplegable **Servidor de administración**, seleccione **Reconectar desde otro servidor**.
3. En el campo **Contraseña actual**, introduzca la contraseña establecida para la conexión al servidor de confianza usado anteriormente.
4. En el campo **Nueva contraseña**, establezca una contraseña para la conexión al nuevo Servidor de administración y confírmela.

   Si olvida la contraseña, puede cambiarla usando una tarea.

5. Si tiene Kaspersky Endpoint Security 12.7 o una versión anterior de la aplicación implementada, seleccione la casilla **Activar compatibilidad de cifrado mediante contraseña para versiones anteriores de la aplicación (12.7 e inferiores)**.

   A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si ha implementado Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desactive esta casilla y utilice el cifrado de contraseña más seguro. Las versiones anteriores de la aplicación no admiten el cifrado de contraseña seguro. Para ejecutar la tarea, debe seleccionar la casilla de verificación.

Paso 3. Selección de la cuenta para ejecutar la tarea

Seleccione **Cuenta preconfigurada**. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

Paso 4. Configurar una planificación de inicio de tarea

En **Inicio programado**, seleccione **Manualmente**.

Paso 5. Definir el nombre de la tarea

Introduzca un nombre para la tarea; por ejemplo, *Contraseña de conexión al servidor principal*.

Paso 6. Conclusión de la creación de tareas

Finalice el asistente. Seleccione la casilla **Ejecutar la tarea después de que finalice el asistente** o ejecute la tarea manualmente. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo establecer una nueva contraseña para reconectar a un nuevo servidor en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Protección de la conexión al servidor de administración**.

c. En el campo **Nombre de la tarea**, escriba una descripción breve; por ejemplo, *Contraseña de conexión al servidor principal*.

d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Seleccione una cuenta de usuario predeterminada. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Seleccione la tarea **Protección de la conexión al servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. En **Protección de la conexión al servidor de administración**, seleccione **Proteger con contraseña**.

10. En la lista desplegable **Conexión al servidor de administración**, seleccione **Reconectar desde otro servidor**.

11. En el campo **Contraseña actual**, introduzca la contraseña establecida para la conexión al servidor de confianza usado anteriormente.

12. En el campo **Nueva contraseña**, establezca una contraseña para la conexión al nuevo Servidor de administración y confírmela.

    Si olvida la contraseña, puede cambiarla usando una tarea.

13. Si tiene Kaspersky Endpoint Security 12.7 o una versión anterior de la aplicación implementada, seleccione la casilla **Activar compatibilidad de cifrado mediante contraseña para versiones anteriores de la aplicación (12.7 e inferiores)**.

    A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si ha implementado Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desactive esta casilla y utilice el cifrado de contraseña más seguro. Las versiones anteriores de la aplicación no admiten el cifrado de contraseña seguro. Para ejecutar la tarea, debe seleccionar la casilla de verificación.

14. Guarde los cambios.

15. Active la casilla ubicada junto a la tarea.

16. Haga clic en **Iniciar**.

    Puede supervisar el estado de la tarea y el número de dispositivos en los que se completó correctamente o con errores.

Tras completar la tarea, asegúrese de que en la consola del nuevo servidor de `[KSC2]`, el estado del equipo es *Aceptar* . Pruebe si puede ejecutar tareas de forma remota y configurar la aplicación usando directivas.

Restablecer la contraseña de conexión al Servidor de administración

Si ha olvidado la contraseña de conexión al Servidor de administración o su seguridad se ha visto comprometida, puede restablecerla en las propiedades de la tarea. También puede restablecer la contraseña y establecer una nueva para un grupo de equipos con distintos estados de protección de conexión al Servidor de administración. Es decir, si algunos equipos tienen la protección activada y otros desactivada, la tarea establece una contraseña para todos.

Solo puede restablecer la contraseña de conexión al Servidor de administración en la consola del servidor de confianza al que está conectado el equipo.

Cómo restablecer la contraseña de conexión al Servidor de administración mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea **Protección de la conexión al servidor de administración** y haga doble clic para abrir las propiedades de la tarea.
4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
5. En **Protección de la conexión al servidor de administración**, seleccione **Proteger y cambiar la contraseña**.
6. En el campo **Contraseña de conexión al servidor de administración**, establezca una nueva contraseña para la conexión al nuevo servidor de confianza y confírmela.
7. Guarde los cambios.
8. Ejecute la tarea.

Cómo restablecer la contraseña de conexión al Servidor de administración en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Seleccione la tarea **Protección de la conexión al servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. En **Protección de la conexión al servidor de administración**, seleccione **Proteger y cambiar la contraseña**.
5. En el campo **Contraseña de conexión al servidor de administración**, establezca una nueva contraseña para la conexión al nuevo servidor de confianza y confírmela.
6. Guarde los cambios.
7. Active la casilla ubicada junto a la tarea.
8. Haga clic en **Iniciar**.

Como resultado, la contraseña de conexión al Servidor de administración se restablece cuando finaliza la tarea.

Desactivación de la protección de conexión al Servidor de administración

Solo puede desactivar de forma remota la protección de conexión al Servidor de administración en la consola del servidor de confianza al que está conectado el equipo. También puede desactivar la protección de forma local, mediante la línea de comandos.

Cómo desactivar la protección de conexión al servidor en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Tareas**.
3. Seleccione la tarea **Protección de la conexión al servidor de administración** y haga doble clic para abrir las propiedades de la tarea.
4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
5. En **Protección de la conexión al servidor de administración**, seleccione **No proteger**.
6. Guarde los cambios.
7. Ejecute la tarea.

   Puede supervisar el estado de la tarea y el número de dispositivos en los que se completó correctamente o con errores.

Cómo desactivar la protección de conexión al servidor en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Seleccione la tarea **Protección de la conexión al servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. En **Protección de la conexión al servidor de administración**, seleccione **No proteger con contraseña**.
5. Guarde los cambios.
6. Active la casilla ubicada junto a la tarea.
7. Haga clic en **Iniciar**.

   Puede supervisar el estado de la tarea y el número de dispositivos en los que se completó correctamente o con errores.

Cómo desactivar la protección de conexión al servidor en la línea de comandos

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   donde `<password>` es la contraseña de la cuenta de usuario KLAdmin o la contraseña de la tarea *Protección de la conexión al servidor de administración*. Si no se especifica el parámetro, Kaspersky Endpoint Security le pide que introduzca una contraseña en la siguiente línea.

   Para ejecutar este comando, es necesario que la protección con contraseña esté activada.

Ejemplo

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Cifrado de datos

Kaspersky Endpoint Security le permite cifrar las carpetas y los archivos almacenados en las unidades locales y extraíbles, o las unidades extraíbles y los discos duros por completo. El cifrado de datos minimiza el riesgo de filtraciones de información que se puede producir en caso de pérdida o robo del equipo portátil, unidad extraíble o disco duro, o cuando usuarios y aplicaciones no autorizados acceden a los datos. Kaspersky Endpoint Security utiliza el algoritmo de cifrado Advanced Encryption Standard (AES, "Advanced Encryption Standard").

Si la licencia ha caducado, la aplicación no cifra datos nuevos, y los datos cifrados antiguos permanecen cifrados y disponibles para su uso. En este caso, para cifrar nuevos datos se requiere activar la aplicación con una nueva licencia que permita el uso de cifrado.

Si Kaspersky Endpoint Security está instalado en un equipo basado en Arm, solo está disponible el Cifrado de unidad BitLocker. La aplicación no admite otros componentes de cifrado de datos.

Si la licencia ha caducado, si no se ha cumplido el Contrato de licencia de usuario final, si se ha eliminado la clave de licencia o los componentes de cifrado, o si se ha desinstalado Kaspersky Endpoint Security, no se garantiza que los archivos cifrados previamente se encuentren cifrados. La razón es que algunas aplicaciones, como Microsoft Office Word, crean una copia temporal de los archivos cuando se modifican. Cuando se guarda el archivo original, la copia temporal sustituye al archivo original. Por lo tanto, en un equipo que no disponga de funcionalidad de cifrado, o un equipo en la que esta funcionalidad no sea accesible, el archivo permanece sin cifrar.

Kaspersky Endpoint Security ofrece las siguientes características de protección de datos:

- **Cifrado de archivos en unidades locales del equipo**. Puede compilar listas de archivos por extensión o grupos de extensiones y listas de carpetas almacenadas en las unidades del equipo local, así como crear reglas para el cifrado de los archivos creados por aplicaciones específicas. Después de aplicar una directiva, Kaspersky Endpoint Security cifra y descifra los archivos siguientes:
  - archivos añadidos individualmente a listas para su cifrado y descifrado;
  - archivos almacenados en carpetas añadidos a listas para su cifrado y descifrado;
  - Archivos creados por aplicaciones separadas.
- **Cifrado de unidades extraíbles**. Puede especificar una regla de cifrado predeterminada para que la aplicación lleve a cabo la misma acción en todas las unidades extraíbles o especificar reglas de cifrado de unidades extraíbles particulares.

  La prioridad de la regla de cifrado predeterminada es más baja que la de las reglas de cifrado creadas para unidades extraíbles particulares. La prioridad de las reglas de cifrado creadas para las unidades extraíbles del modelo de dispositivo especificado es más baja que la de las reglas de cifrado creadas para las unidades extraíbles cuyo ID de dispositivo es el especificado.

Para seleccionar una regla de cifrado de los archivos de una unidad extraíble, Kaspersky Endpoint Security comprueba si se conocen el modelo de dispositivo y el ID. A continuación, la aplicación realiza una de las siguientes operaciones:

- Si se conoce el modelo de dispositivo únicamente, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles del modelo de dispositivo especificado.
- Si se conoce el ID de dispositivo únicamente, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles con el ID de dispositivo especificado.
- Si se conocen el modelo de dispositivo y el ID, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles con el ID de dispositivo especificado. Si no existe tal regla, pero sí una regla de cifrado creada para unidades extraíbles con el modelo de dispositivo específico, la aplicación aplica esta regla. Si no se especifica ninguna regla de cifrado para el ID de dispositivo específico del modelo de dispositivo concreto, la aplicación aplica la regla de cifrado predeterminada.
- Si no se conocen el modelo de dispositivo ni el ID de dispositivo, la aplicación utiliza la regla de cifrado predeterminada.

La aplicación le permite preparar una unidad extraíble para que pueda utilizar los datos cifrados que contiene en modo portátil. Una vez que active el modo portátil, puede acceder a los archivos cifrados de las unidades extraíbles conectadas al equipo sin la necesidad de disponer de la funcionalidad de cifrado.

- **Gestión de reglas de acceso de las aplicaciones a los archivos cifrados**. Para cualquier aplicación, puede crear una regla de acceso a archivos cifrados que bloquee el acceso a archivos de este tipo o lo permita solo como ciphertext, que es una secuencia de caracteres que se obtiene cuando se aplica el cifrado.
- **Creación de paquetes cifrados**. Puede crear archivos comprimidos cifrados y proteger el acceso a dichos archivos mediante una contraseña. Solo se puede acceder al contenido de los archivos comprimidos cifrados por medio de las contraseñas con las cuales se protegió el acceso a dichos archivos comprimidos. Dichos archivos comprimidos se pueden transmitir de forma segura a través de redes o por medio de unidades extraíbles.
- **Cifrado de disco completo**. Puede seleccionar una tecnología de cifrado: Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker (en adelante también llamado simplemente "BitLocker").

  BitLocker es una tecnología que forma parte del sistema operativo Windows. Si un equipo está dotado de un Trusted Platform Module, (TPM), BitLocker lo utiliza para almacenar claves de recuperación que proporcionan acceso a un disco duro cifrado. Cuando el equipo se inicia, BitLocker solicita las claves de recuperación del disco duro desde el módulo de plataforma segura y desbloquea la unidad. Puede configurar el uso de una contraseña y un código PIN para acceder a las claves de recuperación.

  Puede especificar la regla de cifrado de disco completo predeterminada y crear una lista de discos duros que se deben excluir del cifrado. Kaspersky Endpoint Security realiza un cifrado de disco completo sector por sector cuando se aplica la directiva de Kaspersky Security Center. La aplicación cifra todas las particiones lógicas de los discos duros de forma simultánea.

  Después de que se hayan cifrado los discos duros del sistema, en el siguiente inicio de sesión en el equipo, el usuario debe autenticarse en el Agente de autenticación antes de que se pueda acceder a los discos duros y cargar el sistema operativo. Esto requiere la introducción de la contraseña del token o la tarjeta inteligente conectada al equipo, o bien el nombre de usuario y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local que utilice la tarea *Administrar cuentas del Agente de autenticación*. Estas cuentas se basan en las cuentas de Microsoft Windows con las que los usuarios inician sesión en el sistema operativo. También puede usar la tecnología Single Sign-On, que le permite iniciar sesión automáticamente en el sistema operativo utilizando el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

Kaspersky Endpoint Security duplica las cuentas del Agente de autenticación si crea una copia de seguridad del equipo y cifra los datos de este, y, a continuación, restaura la copia de seguridad del equipo y vuelve a cifrar dichos datos. Para eliminar las cuentas duplicadas, debe usar la herramienta klmover con la clave `dupfix`. La utilidad klmover se incluye en la compilación de Kaspersky Security Center. Puede leer más sobre su funcionamiento en la ayuda de Kaspersky Security Center.

Solo se puede acceder a discos duros cifrados en los equipos en los que se haya instalado Kaspersky Endpoint Security con la funcionalidad de cifrado de disco completo. Esta precaución minimiza el riesgo de fuga de datos de un disco duro cifrado cuando se intenta acceder a él desde el exterior de la red de área local de la compañía.

Para cifrar discos duros y unidades extraíbles, puede utilizar la función Cifrar solo el espacio en disco utilizado. Se recomienda utilizar esta función solo para dispositivos nuevos que no se hayan utilizado anteriormente. Si va a aplicar cifrado a un dispositivo que ya está en uso, se recomienda que cifre el dispositivo completo. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable.

Antes comenzar el cifrado, Kaspersky Endpoint Security obtiene el mapa de los sectores del sistema de archivos. La primera oleada de cifrado incluye los sectores que están ocupados por archivos en el momento en que se inicia el cifrado. La segunda oleada de cifrado incluye los sectores que se escribieron después de que comenzara el cifrado. Una vez que el cifrado se ha completado, todos los sectores que contienen datos están cifrados.

Una vez que el cifrado se ha completado y un usuario elimina un archivo, los sectores que almacenaban el archivo eliminado vuelven a estar disponibles para almacenar nueva información a nivel del sistema de archivos, pero permanecen cifrados. Esto quiere decir que, después de un tiempo, todos los sectores de un dispositivo nuevo terminan por cifrarse, según se van guardando archivos en él, si este se cifra regularmente con la función **Cifrar solo el espacio en disco utilizado**.

El Servidor de administración de Kaspersky Security Center que haya controlado el equipo durante el cifrado proporciona los datos necesarios para descifrar archivos. Si el equipo con objetos cifrados estaba administrado por un Servidor de Administración diferente por algún motivo, puede obtener acceso a los datos cifrados de una de las siguientes maneras:

- Servidores de administración en la misma jerarquía:
  - No necesita realizar ninguna acción adicional. El usuario retendrá el acceso a los objetos cifrados. Las clave de cifrado se distribuyen a todos los Servidores de administración.
- Servidores de administración separados
  - Solicite acceso a los objetos cifrados al administrador de la red de área local.
  - Restaure los datos en los dispositivos cifrados por medio de la Utilidad de restauración.
  - Mediante una copia de seguridad, restaure la configuración del Servidor de administración de Kaspersky Security Center que haya controlado el equipo durante el cifrado y utilice esta configuración en el servidor de administración que ahora controla el equipo con los archivos cifrados.

Si no hay acceso a datos cifrados, siga las instrucciones especiales para trabajar con datos cifrados (Restaurar el acceso a archivos cifrados, Trabajar con dispositivos cifrados si no existe acceso a estos).

Limitaciones de funcionalidad del cifrado

El Cifrado de datos tiene las siguientes limitaciones:

- La aplicación crea archivos de servicio durante el cifrado. Se requiere alrededor de un 0,5 % del espacio libre no fragmentado en el disco duro para almacenarlos. Si no hay bastante espacio libre no fragmentado en el disco duro, el cifrado no comenzará hasta que se libere suficiente.
- Puede administrar todos los componentes de cifrado de datos en la Consola de administración de Kaspersky Security Center y en Kaspersky Security Center Web Console. En Kaspersky Security Center Cloud Console, solo puede administrar BitLocker.
- Cifrado de datos solo está disponible al utilizar Kaspersky Endpoint Security con el sistema de administración Kaspersky Security Center o con Kaspersky Security Center Cloud Console (solo para BitLocker). El Cifrado de datos cuando se usa Kaspersky Endpoint Security en modo sin conexión no es posible porque Kaspersky Endpoint Security almacena las claves de cifrado en Kaspersky Security Center.
- Si se instala Kaspersky Endpoint Security en un equipo en el que se ejecuta Microsoft Windows para servidores, solo está disponible el cifrado de disco completo mediante tecnología de Cifrado de unidad BitLocker. Si se instala Kaspersky Endpoint Security en un equipo en el que se ejecuta Windows para estaciones de trabajo, la funcionalidad de cifrado de datos está completamente disponible.
- Si Kaspersky Endpoint Security está instalado en un equipo basado en Arm, solo está disponible el cifrado de disco completo con tecnología de cifrado de unidades BitLocker; otros componentes de cifrado no son compatibles.

El Cifrado de disco completo con la tecnología Cifrado de disco de Kaspersky no está disponible para los discos duros que no cumplan los requisitos de software y hardware.

No hay respaldo para la compatibilidad entre la funcionalidad de cifrado de disco completo de Kaspersky Endpoint Security y Kaspersky Anti-Virus para UEFI. Kaspersky Anti-Virus for UEFI se inicia antes de que se cargue el sistema operativo. Cuando se usa la característica de cifrado de disco completo, la aplicación detecta que no hay un sistema operativo instalado en el equipo. Esto conduce a que Kaspersky Anti-Virus for UEFI se cierre con un error. El Cifrado de archivos (FLE) no afecta el funcionamiento de Kaspersky Anti-Virus para UEFI.

Kaspersky Endpoint Security admite la siguiente configuración:

- Unidades de disco duro, SSD y USB.

  La tecnología Kaspersky Disk Encryption (FDE) permite trabajar con SSD al tiempo que preserva el rendimiento y la vida útil de las unidades SSD.

- Unidades conectadas a través de bus: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.
- Unidades no extraíbles conectadas mediante bus SD o MMC.
- Unidades con sectores de 512 bytes.
- Unidades con sectores de 4096 bytes que emulan 512 bytes.
- Unidades con el siguiente tipo de particiones: GPT, MBR y VBR (unidades extraíbles).

- Software integrado del estándar UEFI 64 y BIOS heredado.
- Software integrado del estándar UEFI con soporte de Secure Boot.

  Secure Boot es una tecnología diseñada para verificar firmas digitales para aplicaciones y controladores de cargadores UEFI. Secure Boot bloquea el inicio de aplicaciones y controladores UEFI que no están firmados o que están firmados por editores desconocidos. Kaspersky Disk Encryption (FDE) es totalmente compatible con Secure Boot. El Agente de autenticación está firmado por un certificado de Editor de controladores UEFI de Microsoft Windows.

  En algunos dispositivos (por ejemplo, Microsoft Surface Pro y Microsoft Surface Pro 2), se puede instalar una lista desactualizada de certificados de verificación de firma digital de forma predeterminada. Antes de cifrar la unidad, debe actualizar la lista de certificados.
- Software integrado del estándar UEFI con soporte Fast Boot.

  Fast Boot es una tecnología que ayuda a que el equipo se inicie más rápido. Cuando la tecnología Fast Boot está activada, normalmente el equipo carga solo el conjunto mínimo de controladores UEFI necesarios para iniciar el sistema operativo. Cuando la tecnología Fast Boot está activada, es posible que los teclados USB, ratones, tokens USB, paneles táctiles y pantallas táctiles no funcionen mientras el Agente de autenticación se está ejecutando.

  Para utilizar el Cifrado de disco de Kaspersky (FDE), se recomienda desactivar la tecnología Fast Boot. Puede utilizar la Utilidad de prueba FDE para probar el funcionamiento del Cifrado de disco de Kaspersky (FDE).

Kaspersky Endpoint Security no admite las configuraciones siguientes:

- El cargador de arranque se ubica en una unidad mientras que el sistema operativo se halla en una unidad diferente.
- El sistema contiene el software integrado del estándar UEFI 32.
- El sistema cuenta con Intel® Rapid Start Technology y unidades que constan de una partición de hibernación, incluso cuando Intel® Rapid Start Technology está desactivada.
- Unidades de disco en formato MBR con más de 10 particiones ampliadas.
- El sistema tiene un archivo de intercambio ubicado en una unidad de disco que no pertenece al sistema.
- Sistema multiarranque con varios sistemas operativos instalados simultáneamente.
- Particiones dinámicas (solo se admiten las particiones principales).
- Unidades de disco con menos del 0,5% de espacio libre en disco no fragmentado.
- Unidades de disco con un tamaño del sector distinto de 512 bytes o 4096 bytes que emulan 512 bytes.
- Unidades híbridas.
- El sistema tiene cargadores de terceros.
- Unidades con directorios NTFS comprimidos.
- La tecnología de Cifrado de disco de Kaspersky (FDE) es incompatible con otras tecnologías de cifrado de disco completo (como BitLocker, McAfee Drive Encryption y WinMagic SecureDoc).

- La tecnología Cifrado de disco de Kaspersky (FDE) es incompatible con la tecnología ExpressCache.
- No se admite la creación, eliminación y modificación de particiones en una unidad cifrada. Podría perder datos.
- El formato del sistema de archivos no es compatible. Podría perder datos.

  Si necesita formatear una unidad que fue cifrada con la tecnología de Cifrado de disco de Kaspersky (FDE), formatee la unidad en un equipo que no tenga Kaspersky Endpoint Security para Windows y use solo el cifrado de disco completo.

  Una unidad cifrada formateada con la opción de formato rápido puede identificarse erróneamente como cifrada la próxima vez que se conecte a un equipo que tenga instalado Kaspersky Endpoint Security para Windows. Los datos del usuario no estarán disponibles.
- El agente de autenticación no admite más de 100 cuentas.
- La tecnología Single Sign-On es incompatible con otras tecnologías de desarrolladores externos.
- La tecnología de Cifrado de disco de Kaspersky (FDE) no es compatible con los siguientes modelos de dispositivos:
  - Dell Latitude E6410 (modo UEFI)
  - HP Compaq nc8430 (modo BIOS heredado)
  - Lenovo ThinkCentre 8811 (modo BIOS heredado)
- El Agente de autenticación no admite trabajar con tokens USB cuando la compatibilidad con USB heredado está activada. Solo la autenticación basada en contraseña será posible en el equipo.
- Al cifrar una unidad en modo BIOS heredado, se recomienda activar la compatibilidad con USB heredado en los siguientes modelos de dispositivos:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320

- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- HP Compaq dx2450 Microtower PC
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (placa base)

Cómo cambiar la longitud de la clave de cifrado (AES56 o AES256)

Kaspersky Endpoint Security utiliza el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard"). En Kaspersky Endpoint Security, la longitud de clave efectiva de AES algoritmo puede ser de 256 bits o de 56 bits. El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: están disponibles tanto la variante de *cifrado "fuerte" (AES256)* como la de *cifrado "ligero" (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

Cambiar la longitud de la clave de cifrado solo es posible en Kaspersky Endpoint Security 11.2.0 o posterior.

Para cambiar la longitud de la clave de cifrado, complete estos pasos:

1. Antes de cambiar la longitud de la clave de cifrado, descifre los objetos que Kaspersky Endpoint Security ya haya cifrado:

   a. Descifrar los discos duros.

   b. Descifre los archivos almacenados en los discos locales.

   c. Descifre las unidades extraíbles.

   Una vez que cambie la longitud de la clave de cifrado, los objetos que permanezcan cifrados dejarán de estar disponibles.

2. Elimine Kaspersky Endpoint Security.

3. Instale Kaspersky Endpoint Security con un paquete de distribución de Kaspersky Endpoint Security que contenga una biblioteca de cifrado diferente.

Otra alternativa para realizar el cambio de longitud consiste en actualizar la aplicación. Para que el cambio pueda hacerse de este modo, se deben cumplir las siguientes condiciones:

- La versión de Kaspersky Endpoint Security instalada en el equipo debe ser la 10 Service Pack 2 o posterior.
- Los componentes de cifrado de datos (Cifrado de archivos, Cifrado de disco completo) no deben estar instalados en el equipo.

  De manera predeterminada, Kaspersky Endpoint Security no incluye los componentes de cifrado de datos. El componente Administración de BitLocker no afecta al cambio en la longitud de la clave de cifrado.

Para cambiar la longitud de la clave de cifrado, ejecute el archivo kes_win.msi o setup_kes.exe del paquete de distribución que contenga la biblioteca de cifrado necesaria. Si necesita actualizar la aplicación en forma remota, utilice el paquete de instalación.

No se puede cambiar la longitud de la clave de cifrado utilizando el paquete de distribución de la misma versión de la aplicación que está instalada en su equipo sin desinstalar primero la aplicación.

Cifrado de disco de Kaspersky

Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.

El Cifrado de disco de Kaspersky está disponible solo para equipos con un sistema operativo Windows para estaciones de trabajo. Para los equipos con un sistema operativo Windows para servidores, use la tecnología Cifrado de unidad BitLocker.

La característica de cifrado de disco completo de Kaspersky Endpoint Security es compatible con los sistemas de archivos FAT32, NTFS y exFAT.

Antes de empezar el cifrado de disco completo, la aplicación ejecuta una serie de comprobaciones para determinar si el dispositivo se puede cifrar. Esto incluye la comprobación del disco duro del sistema para averiguar si es compatible con el Agente de autenticación o los componentes de cifrado de BitLocker. Para comprobar la compatibilidad, el equipo se debe reiniciar. Tras el reinicio, la aplicación llevará a cabo todas las comprobaciones necesarias automáticamente. Si se supera la comprobación de compatibilidad, la tarea de cifrado de disco completo comenzará después de que el sistema operativo se haya cargado y la aplicación se haya iniciado. Si se determina que el disco duro del sistema no es compatible con Agente de autenticación o con los componentes de cifrado de BitLocker, se deberá reiniciar el equipo pulsando el botón físico de reinicio. Kaspersky Endpoint Security registra información sobre la incompatibilidad. En función de esta información, la aplicación no comenzará el cifrado de disco completo cuando arranque el sistema operativo. La información sobre este evento se registra en informes de Kaspersky Security Center.

Si la configuración de hardware del equipo ha cambiado, se deberá eliminar la información de incompatibilidad registrada por la aplicación durante la comprobación anterior para averiguar la compatibilidad del disco duro del sistema con el Agente de autenticación y los componentes de cifrado de BitLocker. Para ello, escriba `avp pbatestreset` en la línea de comandos antes del cifrado de disco completo. Si el sistema operativo no se carga después de que se haya comprobado la compatibilidad del disco duro del sistema con Agente de autenticación, debe quitar los objetos y los datos que permanecen tras la operación de prueba del Agente de autenticación con la Utilidad de restauración. A continuación, inicie Kaspersky Endpoint Security y vuelva a ejecutar el comando `avp pbatestreset`.

Cuando comience el cifrado de disco completo, Kaspersky Endpoint Security cifra todos los datos escritos en los discos duros.

Si el usuario apaga o reinicia el equipo durante la tarea de cifrado de disco completo, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el Agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo cambia al modo de hibernación durante el cifrado de disco completo, el Agente de autenticación se carga cuando el sistema operativo vuelve al modo normal. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el Agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el cifrado de disco completo, Kaspersky Endpoint Security reanudará el proceso cuando el sistema operativo vuelva a encontrarse en el modo normal sin cargar el Agente de autenticación.

La autenticación de usuario en Agente de autenticación se puede realizar de dos maneras:

- Introduzca el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local con las herramientas de Kaspersky Security Center.
- Introduzca la contraseña de un token o una tarjeta inteligente conectados al equipo.

  El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraran usando el algoritmo de cifrado AES56, no se podrá agregar el archivo del certificado electrónico al comando.

El agente de autenticación admite las distribuciones del teclado para los siguientes idiomas:

- Inglés (Reino Unido)
- Inglés (EE. UU.)

- Árabe (Argelia, Marruecos, Túnez; diseño AZERTY)
- Español (América Latina)
- Italiano
- Alemán (Alemania y Austria)
- Alemán (Suiza)
- Portugués (Brasil; diseño ABNT2)
- Ruso (para teclados IBM de 105 teclas o teclados Windows con el diseño QWERTY)
- Turco (diseño QWERTY)
- Francés (Francia)
- Francés (Suiza)
- Francés (Bélgica, diseño AZERTY)
- Japonés (para teclados de 106 teclas con el diseño QWERTY)

Hay una distribución del teclado disponible en el Agente de autenticación si esta se ha añadido en el idioma y con la configuración regional estándar del sistema operativo, y aparece disponible en la pantalla de bienvenida de Microsoft Windows.

Si el nombre de la cuenta del Agente de autenticación contiene símbolos que no pueden introducirse mediante las distribuciones del teclado disponibles en el Agente de autenticación, solo es posible acceder a los discos duros cifrados después de su restauración mediante la Utilidad de restauración o después de que se restauren el nombre de la cuenta y la contraseña del Agente de autenticación.

Características especiales del cifrado de unidades SSD

La aplicación admite el cifrado de unidades SSD, unidades SSHD híbridas y unidades con la función Intel Smart Response. La aplicación no admite el cifrado de unidades con la función Intel Rapid Start. Desactive la función Intel Rapid Start antes de cifrar dicha unidad.

El cifrado de unidades SSD tiene las siguientes características especiales:

- Si una unidad SSD es nueva y no contiene datos confidenciales, habilite el cifrado solo del espacio ocupado. Esto le permite sobrescribir los sectores relevantes de la unidad.
- Si una unidad SSD está en uso y tiene datos confidenciales, seleccione una de las siguientes opciones:
  - Limpie completamente la unidad SSD (Secure Erase), instale el sistema operativo y ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado activada.
  - Ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado desactivada.

El cifrado de una unidad SSD requiere de 5 a 10 GB de espacio libre. Los requerimientos de espacio libre para almacenar datos de administración de cifrado se proporcionan en la siguiente tabla.

Requerimientos de espacio libre para almacenar datos de administración de cifrado

Tamaño de la unidad SSD (GB)	Espacio libre en la partición principal de la unidad SSD (MB)	Espacio libre en la partición secundaria de la unidad SSD (MB)
128	250	64
256	250	640
512	300	128

Comienzo del Cifrado de disco de Kaspersky

Antes de comenzar el cifrado de disco completo, es aconsejable asegurarse de que el equipo no esté infectado. Para ello, ejecute la tarea Análisis completo o Análisis de áreas críticas. Cifrar un disco completo en un equipo infectado con un rootkit puede provocar que el equipo se inutilice.

Antes de iniciar el cifrado de disco, debe verificar la configuración de las cuentas del Agente de autenticación. Se necesita un Agente de autenticación para trabajar con unidades protegidas con la tecnología Cifrado de disco de Kaspersky (FDE). Antes de que se cargue el sistema operativo, el usuario debe completar la autenticación con el Agente. Kaspersky Endpoint Security le permite crear automáticamente cuentas de Agente de autenticación antes de cifrar una unidad. Puede activar la creación automática de cuentas del Agente de autenticación en la configuración de la directiva de cifrado de disco completo (consulte las instrucciones, a continuación). También puede utilizar la tecnología de inicio de sesión único (SSO).

Kaspersky Endpoint Security le permite crear automáticamente cuentas de Agente de autenticación para los siguientes grupos de usuarios:

- **Todas las cuentas del equipo**. Todas las cuentas en el equipo que han estado activas en algún momento.
- **Todas las cuentas de dominio del equipo**. Todas las cuentas del equipo que pertenecen a algún dominio y que han estado activas en algún momento.
- **Todas las cuentas locales del equipo**. Todas las cuentas locales en el equipo que han estado activas en algún momento.
- **Cuenta de servicio con una contraseña única**. La cuenta de servicio es necesaria para acceder al equipo, por ejemplo, cuando el usuario olvida la contraseña. También puede utilizar la cuenta de servicio como cuenta de reserva. Debe introducir el nombre de la cuenta (por defecto, `ServiceAccount`). Kaspersky Endpoint Security crea una contraseña automáticamente. Puede encontrar la contraseña en la consola de Kaspersky Security Center.
- **Administrador local**. Kaspersky Endpoint Security crea una cuenta de usuario del Agente de autenticación para el administrador local del equipo.
- **Administrador del equipo**. Kaspersky Endpoint Security crea una cuenta de usuario del Agente de autenticación para la cuenta del administrador del equipo. Puede ver qué cuenta tiene la función de administrador del equipo en las propiedades del equipo en Active Directory. Por defecto, la función de administrador del equipo no está definida, es decir, no corresponde a ninguna cuenta.
- **Cuenta activa**. Kaspersky Endpoint Security crea automáticamente una cuenta de agente de autenticación para la cuenta que está activa en el momento del cifrado del disco.

La tarea *Administrar cuentas del Agente de autenticación* está diseñada para configurar los ajustes de autenticación del usuario. Puede usar esta tarea para añadir nuevas cuentas, modificar la configuración de las cuentas actuales o eliminar cuentas si es necesario. Puede usar tareas locales para equipos particulares, así como tareas de grupo para equipos de grupos de administración independientes o una selección de equipos.

Cómo ejecutar el Cifrado de disco de Kaspersky mediante la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de disco completo**.
4. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de disco de Kaspersky**.

   La tecnología Cifrado de disco de Kaspersky no se puede utilizar si el equipo cuenta con discos duros cifrados por BitLocker.

5. En la lista desplegable **Modo de cifrado**, seleccione **Cifrar todos los discos duros**.

   Si el equipo tiene varios sistemas operativos instalados, después de cifrar todos los discos duros solo podrá cargar el sistema operativo que tenga la aplicación instalada.

   Si tiene que excluir algunos de los discos duros del cifrado, cree una lista de estos discos duros.

6. Configure las opciones avanzadas de Cifrado de disco de Kaspersky (consulte la tabla a continuación).
7. Guarde los cambios.

Cómo ejecutar el Cifrado de disco de Kaspersky mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos → Cifrado de disco completo**.
5. Seleccione la tecnología **Cifrado de disco de Kaspersky**.

   La tecnología Cifrado de disco de Kaspersky no se puede utilizar si el equipo cuenta con discos duros cifrados por BitLocker.

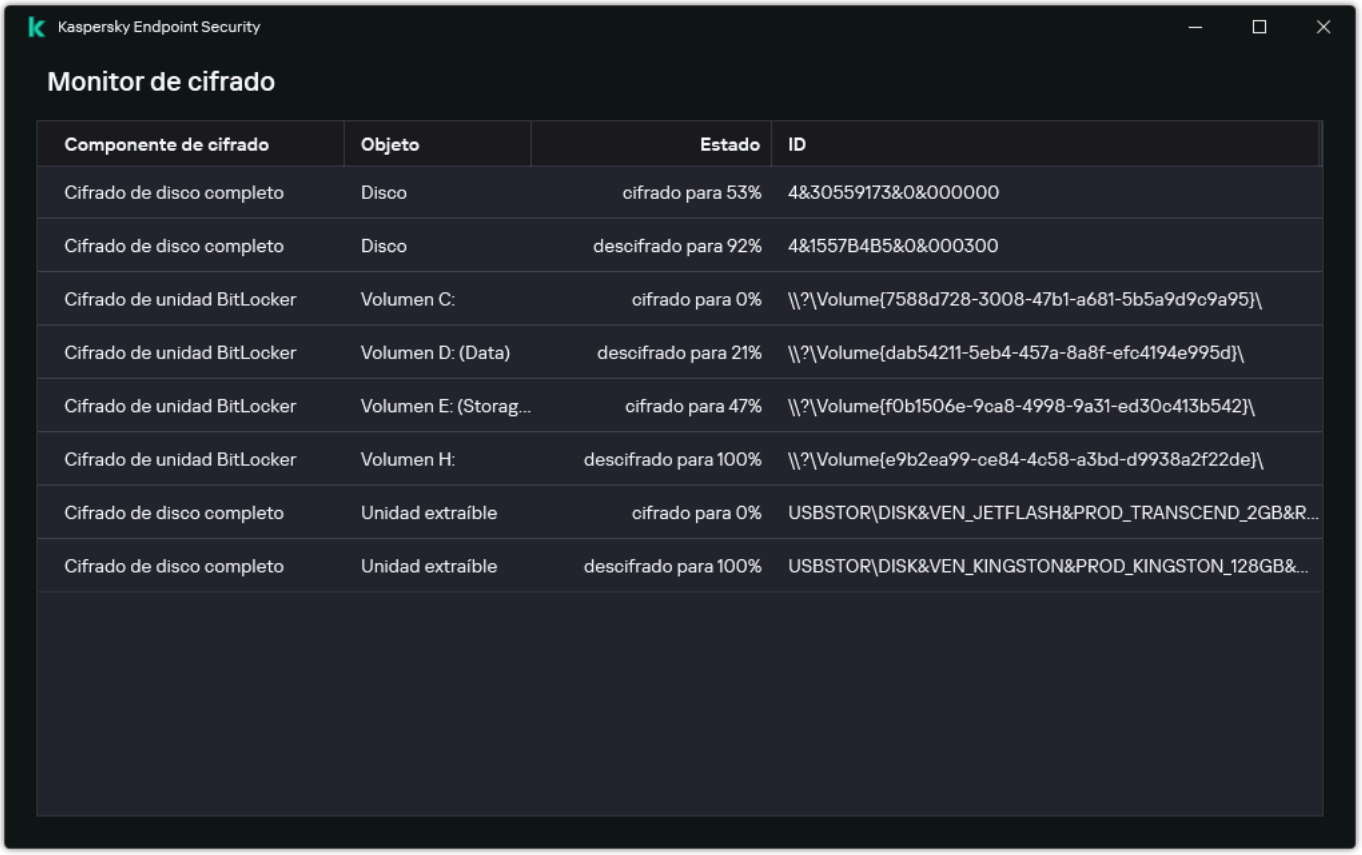
6. En el bloque **Acción en los dispositivos**, seleccione **Cifrar todos los discos duros**.

Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo en el que se hizo el cifrado.

Si tiene que excluir algunos de los discos duros del cifrado, cree una lista de estos discos duros.

7. Configure las opciones avanzadas de Cifrado de disco de Kaspersky (consulte la tabla a continuación).
8. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la ventana principal de la aplicación.



Monitor de cifrado

Si los discos duros del sistema están cifrados, el Agente de autenticación se carga antes del inicio del sistema operativo. Utilice el Agente de autenticación para completar la autenticación con el fin de obtener acceso a los discos duros cifrados del sistema y cargar el sistema operativo. Después de que se completa correctamente el procedimiento de autenticación, se carga el sistema operativo. Se repite el proceso de autenticación cada vez que el sistema operativo se reinicia.

Parámetro	Descripción
Crear automáticamente cuentas del Agente de autenticación para usuarios durante el cifrado	Si esta casilla de verificación está seleccionada, la aplicación creará cuentas de agente de autenticación según la lista de cuentas de usuario de Windows en el equipo. De forma predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario ha iniciado sesión en el sistema operativo durante los últimos 30 días.
Crear automáticamente cuentas del Agente de autenticación para todos los usuarios de este equipo al iniciar sesión	Si esta casilla de verificación está seleccionada, la aplicación verifica la información sobre las cuentas de usuario de Windows en el equipo antes de iniciar el Agente de autenticación. Si Kaspersky Endpoint Security detecta una cuenta de usuario de Windows que no tiene una cuenta de Agente de autenticación, la aplicación creará una nueva cuenta para acceder a las unidades cifradas. La nueva cuenta del Agente de autenticación tendrá la siguiente configuración predeterminada: inicio de sesión protegido con contraseña únicamente y cambio de contraseña en la primera autenticación. Por lo tanto, no es necesario agregar manualmente cuentas del Agente de autenticación mediante la tarea *Administrar cuentas del Agente de autenticación* para equipos con unidades ya cifradas.
Guardar el nombre de usuario introducido en el Agente de autenticación	Si se selecciona la casilla de verificación, la aplicación guarda el nombre de la cuenta del Agente de Autenticación. No se le solicitará introducir el nombre de la cuenta la próxima vez que intente realizar una autorización en el Agente de autenticación con la misma cuenta.
Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)	Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado. Activar o desactivar la función **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado. Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden. Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente. Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De forma predeterminada, la casilla de verificación está desactivada.
Utilizar Legacy USB Support (no recomendado)	Esta casilla de verificación activa o desactiva la función Legacy USB Support. *Legacy USB Support* **es** una función BIOS/UEFI que le permite usar dispositivos USB (como un token de seguridad) durante la fase de inicio del equipo antes de iniciar el sistema operativo (modo BIOS). Legacy USB Support no afecta a la compatibilidad con dispositivos USB después del inicio del sistema operativo. Si la casilla está seleccionada, se activará la compatibilidad con dispositivos USB durante el primer inicio del equipo. Cuando la función Legacy USB Support está activada, el Agente de autenticación en el modo BIOS no permite trabajar con tokens a través de USB. Se recomienda usar esta opción solo cuando existe un problema de compatibilidad de hardware y solo para los equipos en los cuales se produce el problema.

Creación de una lista de discos duros excluidos del cifrado

Puede crear una lista de exclusiones de cifrado solo para la tecnología Cifrado de disco de Kaspersky.

Para crear una lista de discos duros excluidos del cifrado:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de disco completo**.
4. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de disco de Kaspersky**.

   Las entradas que corresponden a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**. Esta tabla estará vacía si no ha creado previamente una lista de discos duros que se deben excluir del cifrado.
5. Para añadir discos duros a la lista de discos duros excluidos del cifrado:

   a. Haga clic en **Añadir**.

   b. En la ventana que se abre, especifique los valores para **Nombre del disp**, **Equipo**, **Tipo de disco**, **Cifrado de disco de Kaspersky**.

   c. Haga clic en **Actualizar**.

   d. En la columna **Nombre**, seleccione las casillas de verificación en las filas de la tabla que corresponden a los discos duros que desea añadir a la lista de discos duros excluidos del cifrado.

   e. Haga clic en **Aceptar**.

   Los discos duros seleccionados aparecen en la tabla **No cifrar los siguientes discos duros**.
6. Guarde los cambios.

Exportar e importar una lista de discos duros excluidos del cifrado

Puede exportar la lista de exclusiones de cifrado del disco duro a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de exclusiones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar las exclusiones a un servidor diferente.

Cómo exportar e importar una lista de exclusiones de cifrado del disco duro en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de disco completo**.
4. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de disco de Kaspersky**.

   Las entradas que corresponden a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**.

5. Para exportar la lista de exclusiones:

   a. Seleccione las exclusiones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

      Si no seleccionó ninguna exclusión, Kaspersky Endpoint Security exportará todas las exclusiones.

   b. Haga clic en el botón → **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.

6. Para importar la lista de reglas:

   a. Haga clic en el botón → **Importar**.

   b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.

   c. Abra el archivo.

      Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

7. Guarde los cambios.

Cómo exportar e importar una lista de exclusiones de cifrado del disco duro en Web Console.

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Cifrado de datos** → **Cifrado de disco completo**.

   Seleccione la tecnología **Cifrado de disco de Kaspersky**.

5. Haga clic en el enlace **Exclusiones**.

   Se abre la lista de exclusiones.

6. Para exportar la lista de reglas:

   a. Seleccione las exclusiones que desea exportar.

   b. Haga clic en el botón → **Exportar**.

      Kaspersky Endpoint Security exporta la lista de exclusiones a un archivo JSON en la carpeta de descargas predeterminada.

7. Para importar la lista de exclusiones:

   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON del que importar la lista de exclusiones.

b. Abra el archivo.

Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo JSON.

8. Guarde los cambios.

Activación de la tecnología de inicio de sesión único (SSO)

La tecnología Single Sign-On (SSO) le permite iniciar sesión automáticamente en el sistema operativo utilizando las credenciales del Agente de autenticación. Esto significa que un usuario debe introducir la contraseña una sola vez al iniciar sesión en Windows (contraseña de la cuenta del agente de autenticación). La tecnología de inicio de sesión único también le permite actualizar automáticamente la contraseña de la cuenta del agente de autenticación cuando se modifica la contraseña de la cuenta de Windows.

Cuando se utiliza la tecnología de inicio de sesión único, el Agente de autenticación ignora los requisitos de seguridad de la contraseña especificados en Kaspersky Security Center. Puede definir los requisitos de seguridad de la contraseña en la configuración del sistema operativo.

Activación de la tecnología de inicio de sesión único

Cómo activar el uso de la tecnología de inicio de sesión único en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Configuración común de cifrado**.
4. En el bloque **Configuración de contraseña**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, en la pestaña **Agente de autenticación**, elija la casilla de verificación **Utilizar la tecnología de inicio de sesión único (SSO)**.
6. Si está usando un proveedor de credenciales de terceros, elija la casilla de verificación **Ajustar proveedores de credenciales de terceros**.
7. Guarde los cambios.

Como resultado, el usuario necesita completar el procedimiento de autenticación solo una vez con el Agente. El procedimiento de autenticación no es necesario para cargar el sistema operativo. El sistema operativo se carga automáticamente.

Cómo activar el uso del inicio de sesión único en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Cifrado de datos → Cifrado de disco completo**.

5. Seleccione la tecnología **Cifrado de disco de Kaspersky**.

6. En el bloque **Configuración de contraseña**, seleccione la casilla de verificación **Usar la tecnología de inicio de sesión único (SSO)**.

7. Si está usando un proveedor de credenciales de terceros, elija la casilla de verificación **Ajustar proveedores de credenciales de terceros**.

8. Guarde los cambios.

Como resultado, el usuario necesita completar el procedimiento de autenticación solo una vez con el Agente. El procedimiento de autenticación no es necesario para cargar el sistema operativo. El sistema operativo se carga automáticamente.

Para que funcione el inicio de sesión único, la contraseña de la cuenta de Windows y la contraseña de la cuenta del Agente de autenticación deben coincidir. Si las contraseñas no coinciden, el usuario tiene que realizar el procedimiento de autenticación dos veces: en la interfaz del Agente de autenticación y antes de cargar el sistema operativo. Estas acciones deben realizarse una sola vez para sincronizar las contraseñas. Después de eso, Kaspersky Endpoint Security reemplaza la contraseña de la cuenta del Agente de autenticación con la de la cuenta de Windows. Cuando se modifica la contraseña de la cuenta de Windows, la aplicación actualiza automáticamente la contraseña de la cuenta del agente de autenticación.

Proveedores de credenciales de terceros

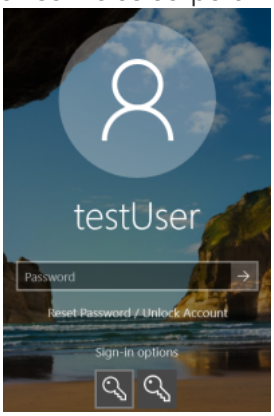
Kaspersky Endpoint Security es compatible con el proveedor de credenciales de terceros ADSelfService Plus.

Al trabajar con proveedores de credenciales de terceros, el agente de autenticación intercepta la contraseña antes de que se cargue el sistema operativo. Esto significa que un usuario debe introducir la contraseña una sola vez al iniciar sesión en Windows. Después de iniciar sesión en Windows, el usuario puede utilizar las capacidades del proveedor de credenciales de terceros para la autenticación en servicios corporativos, por ejemplo. Los proveedores de credenciales de terceros también permiten que los usuarios restablezcan su propia contraseña de forma independiente. En este caso, Kaspersky Endpoint Security actualizará automáticamente la contraseña para el agente de autenticación.

Si está utilizando un proveedor de credenciales de terceros que no es compatible con la aplicación, es posible que encuentre algunas limitaciones en la operación de la tecnología de inicio de sesión único. Al iniciar sesión en Windows, habrá dos perfiles disponibles para el usuario: el proveedor de credenciales interno del sistema y el proveedor de credenciales de terceros. Los iconos de estos perfiles serán idénticos (consulte la figura a continuación). El usuario tendrá las siguientes opciones para continuar:

- Si el usuario elige el *proveedor de credenciales de terceros*, el agente de autenticación no podrá sincronizar la contraseña con la cuenta de Windows. Por lo tanto, si el usuario ha modificado la contraseña de la cuenta de Windows, Kaspersky Endpoint Security no podrá actualizar la contraseña para la cuenta del agente de autenticación. De este modo, el usuario deberá realizar el procedimiento de autenticación dos veces: en la interfaz del agente de autenticación y antes de cargar el sistema operativo. En este caso, el usuario puede utilizar las funcionalidades del proveedor de credenciales de terceros para la autenticación en servicios corporativos, por ejemplo.

- Si el usuario elige el *proveedor de credenciales interno del sistema*, el agente de autenticación sincronizará las contraseñas con la cuenta de Windows. En este caso, el usuario no puede utilizar las funcionalidades de un proveedor de terceros para la autenticación en servicios corporativos, por ejemplo.



Perfil de autenticación del sistema y perfil de autenticación de terceros para inicio de sesión en Windows

Administración de cuentas del Agente de autenticación

Se necesita un Agente de autenticación para trabajar con unidades protegidas con la tecnología Cifrado de disco de Kaspersky (FDE). Antes de que se cargue el sistema operativo, el usuario debe completar la autenticación con el Agente. La tarea *Administrar cuentas del Agente de autenticación* está diseñada para configurar los ajustes de autenticación del usuario. Puede usar tareas locales para equipos particulares, así como tareas de grupo para equipos de grupos de administración independientes o una selección de equipos.

No puede configurar una planificación para iniciar la tarea *Administrar cuentas del Agente de autenticación*. También es imposible detener una tarea por la fuerza.

Cómo crear la tarea Administrar cuentas del Agente de autenticación en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Administrar cuentas del Agente de autenticación**.

Paso 2. Seleccionar un comando de administración de cuentas del Agente de autenticación

Genere una lista de comandos de administración de cuentas del Agente de autenticación. Los comandos de administración le permiten añadir, modificar y eliminar cuentas del Agente de autenticación (consulte las instrucciones más abajo). Solo los usuarios que tienen una cuenta de Agente de autenticación pueden completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Cuentas de administrador*.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el nuevo usuario puede completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Cómo crear la tarea Administrar cuentas del Agente de autenticación en Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.
   Se abre la lista de tareas.
2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Administrar cuentas del Agente de autenticación**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Cuentas de administrador*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

Paso 2. Administración de cuentas del Agente de autenticación

Genere una lista de comandos de administración de cuentas del Agente de autenticación. Los comandos de administración le permiten añadir, modificar y eliminar cuentas del Agente de autenticación (consulte las instrucciones más abajo). Solo los usuarios que tienen una cuenta de Agente de autenticación pueden completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Paso 3. Conclusión de la creación de tareas

Finalice el asistente. La nueva tarea aparecerá en la lista de tareas.

Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**.

Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el nuevo usuario puede completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Para añadir una cuenta del Agente de autenticación, debe añadir un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Es conveniente utilizar una tarea de grupo, por ejemplo, para añadir una cuenta de administrador a todos los equipos.

Kaspersky Endpoint Security le permite crear automáticamente cuentas de Agente de autenticación antes de cifrar una unidad. Puede activar la creación automática de cuentas del Agente de autenticación en la configuración de la directiva de cifrado de disco completo. También puede utilizar la tecnología de inicio de sesión único (SSO).

Cómo añadir una cuenta del Agente de autenticación mediante la Consola de administración (MMC)

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de tarea, seleccione la sección **Configuración**.
3. Haga clic en **Añadir → Comando de adición de cuentas**.
4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows que se utilizará para crear la cuenta del Agente de autenticación.
5. Si ha introducido el nombre de una cuenta de Windows manualmente, haga clic en el botón **Permitir** para definir el identificador de seguridad de la cuenta (SID).

   Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Permitir**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

   > Es necesario definir un identificador de seguridad de la cuenta de Windows para verificar que el nombre de la cuenta de Windows se ha introducido correctamente. Si la cuenta de Windows introducida no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con error.

6. Marque la casilla **Reemplazar una cuenta existente** si desea que la cuenta del Agente de autenticación que se ha creado previamente y se reemplace por la cuenta que se está creando.

   > Este paso está disponible cuando añade un comando de creación de cuentas del Agente de autenticación en las propiedades de una tarea de grupo para administrar las cuentas del Agente de autenticación. Este paso no está disponible cuando añade un comando de creación de cuentas del Agente de autenticación en las propiedades de la tarea local de *Administrar cuentas del Agente de autenticación*.

7. En el campo **Nombre de usuario**, introduzca el nombre de la cuenta del Agente de autenticación que debe introducirse durante el proceso de autenticación para acceder los discos duros cifrados.
8. Seleccione la casilla de verificación **Permitir la autenticación basada en contraseña** si desea que la aplicación solicite al usuario que introduzca la contraseña de la cuenta del Agente de autenticación durante la autenticación para acceder a los discos duros cifrados. Introduzca una contraseña para la cuenta del Agente de autenticación. Si es necesario, puede solicitar una nueva contraseña del usuario después de la primera autenticación.
9. Seleccione la casilla de verificación **Permitir la autenticación basada en certificado** si desea que la aplicación solicite al usuario que se conecte a un token o a tarjeta inteligente conectada al equipo durante la autenticación para acceder a los discos duros cifrados. Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token.
10. En el campo **Descripción del comando**, introduzca la información de la cuenta del Agente de autenticación necesaria para administrar el comando.
11. En el bloque **Acceso a la autenticación en el Agente de autenticación**, configure el acceso a la autenticación en el Agente de autenticación para el usuario que utiliza la cuenta especificada en el comando.
12. Guarde los cambios.

Cómo añadir una cuenta del Agente de autenticación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Administrar cuentas del Agente de autenticación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Añadir** y seleccione el tipo de comando **Añadir cuenta**.

5. Seleccione una cuenta de usuario. Puede seleccionar una cuenta de la lista de cuentas de dominio o introducir manualmente el nombre de la cuenta. Ir al paso siguiente.

   Kaspersky Endpoint Security determina el identificador de seguridad de la cuenta (Security Identifier, SID). Esto es necesario para verificar la cuenta. Si ha introducido el nombre de usuario de manera incorrecta, Kaspersky Endpoint Security finalizará la tarea con un error.

6. Configure los ajustes de la cuenta del Agente de autenticación.

   - **Crear una nueva cuenta del Agente de autenticación para reemplazar la cuenta existente**. Kaspersky Endpoint Security analiza las cuentas existentes en el equipo. Si el ID de seguridad del usuario en el equipo y en la tarea coinciden, Kaspersky Endpoint Security cambiará la configuración de la cuenta de usuario de acuerdo con la tarea.

   - **Nombre de usuario**. El nombre de usuario predeterminado de la cuenta del Agente de autenticación corresponde al nombre de dominio del usuario.

   - **Permitir la autenticación basada en contraseña**. Introduzca una contraseña para la cuenta del Agente de autenticación. Si es necesario, puede solicitar una nueva contraseña del usuario después de la primera autenticación. De esta manera, cada usuario tendrá su propia contraseña única. También puede establecer los requisitos de seguridad de la contraseña para la cuenta del Agente de autenticación en la directiva.

   - **Permitir la autenticación basada en certificado**. Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token. De esta manera, el usuario deberá introducir la contraseña de la tarjeta inteligente o token.

   - **Acceso de cuenta a datos cifrados**. Configure el acceso de usuario a la unidad cifrada. Por ejemplo, puede desactivar temporalmente la autenticación de usuario en lugar de eliminar la cuenta del Agente de autenticación.

   - **Comentario**. Introduzca una descripción de la cuenta, si es necesario.

7. Guarde los cambios.

8. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

   Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el nuevo usuario puede completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Para cambiar la contraseña y otros ajustes de la cuenta del Agente de autenticación, debe añadir un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Es conveniente utilizar una tarea de grupo, por ejemplo, para reemplazar el certificado del token de administrador en todos los equipos.

Cómo cambiar la cuenta del Agente de autenticación mediante la Consola de administración (MMC)

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de tarea, seleccione la sección **Configuración**.
3. Haga clic en **Añadir → Comando de modificación de cuentas**.
4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows que quiere modificar.
5. Si ha introducido el nombre de una cuenta de Windows manualmente, haga clic en el botón **Permitir** para definir el identificador de seguridad de la cuenta (SID).

   Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Permitir**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

   > Es necesario definir un identificador de seguridad de la cuenta de Windows para verificar que el nombre de la cuenta de Windows se ha introducido correctamente. Si la cuenta de Windows introducida no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con error.

6. Active la casilla de verificación **Cambiar el nombre de usuario** e introduzca un nombre de cuenta del Agente de autenticación nuevo si desea que Kaspersky Endpoint Security sustituya el nombre de usuario de todas las cuentas del Agente de autenticación que se hayan creado en función de la cuenta de Microsoft Windows que lleva el nombre que se indica en el campo **Cuenta de Windows** por el nombre introducido en el siguiente campo.
7. Seleccione la casilla de verificación **Modificar la configuración de la autenticación basada en contraseña** para poder editar los ajustes de autenticación basada en contraseña.
8. Seleccione la casilla de verificación **Permitir la autenticación basada en contraseña** si desea que la aplicación solicite al usuario que introduzca la contraseña de la cuenta del Agente de autenticación durante la autenticación para acceder a los discos duros cifrados. Introduzca una contraseña para la cuenta del Agente de autenticación.
9. Seleccione la casilla de verificación **Editar la regla de cambio de contraseña en la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security sustituya por el siguiente valor el valor del parámetro de cambio de contraseña de todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows que lleva el nombre indicado en el campo **Cuenta de Windows**.
10. Especifique el valor del parámetro de cambio de contraseña al autenticarse en el Agente de autenticación.
11. Seleccione la casilla de verificación **Modificar la configuración de la autenticación basada en certificado** para hacer editable la configuración de la autenticación en función del certificado electrónico de un token o una tarjeta inteligente.
12. Seleccione la casilla de verificación **Permitir la autenticación basada en certificado** si desea que la aplicación solicite al usuario la introducción de la contraseña al token o a la tarjeta inteligente conectada al equipo durante el proceso de autenticación para acceder a los discos duros cifrados. Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token.
13. Seleccione la casilla de verificación **Modificar la descripción del comando** y modifique la descripción de los comandos si desea que Kaspersky Endpoint Security cambie la descripción de los comandos de todas las cuentas del Agente de autenticación que se hayan creado con la cuenta de Microsoft Windows que lleva el nombre que se indica en el campo **Cuenta de Windows**.

14. Seleccione la casilla de verificación **Editar la regla de acceso a la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie la regla de acceso del usuario a la autenticación en el Agente de autenticación por el valor especificado más abajo para todas las cuentas del Agente de autenticación creadas con la cuenta de Microsoft Windows que lleva el nombre indicado en el campo **Cuenta de Windows**.

15. Especifique la regla para acceder al diálogo de autenticación en el Agente de autenticación.

16. Guarde los cambios.

Cómo cambiar la cuenta del Agente de autenticación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Administrar cuentas del Agente de autenticación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Añadir** y seleccione el tipo de comando **Editar cuenta**.

5. Seleccione una cuenta de usuario. Puede seleccionar una cuenta de la lista de cuentas de dominio o introducir manualmente el nombre de la cuenta. Ir al paso siguiente.

   Kaspersky Endpoint Security determina el identificador de seguridad de la cuenta (Security Identifier, SID). Esto es necesario para verificar la cuenta. Si ha introducido el nombre de usuario de manera incorrecta, Kaspersky Endpoint Security finalizará la tarea con un error.

6. Seleccione las casillas de verificación que hay junto a la configuración que desea editar.

7. Configure los ajustes de la cuenta del Agente de autenticación.

   - **Crear una nueva cuenta del Agente de autenticación para reemplazar la cuenta existente**. Kaspersky Endpoint Security analiza las cuentas existentes en el equipo. Si el ID de seguridad del usuario en el equipo y en la tarea coinciden, Kaspersky Endpoint Security cambiará la configuración de la cuenta de usuario de acuerdo con la tarea.

   - **Nombre de usuario**. El nombre de usuario predeterminado de la cuenta del Agente de autenticación corresponde al nombre de dominio del usuario.

   - **Permitir la autenticación basada en contraseña**. Introduzca una contraseña para la cuenta del Agente de autenticación. Si es necesario, puede solicitar una nueva contraseña del usuario después de la primera autenticación. De esta manera, cada usuario tendrá su propia contraseña única. También puede establecer los requisitos de seguridad de la contraseña para la cuenta del Agente de autenticación en la directiva.

   - **Permitir la autenticación basada en certificado**. Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token. De esta manera, el usuario deberá introducir la contraseña de la tarjeta inteligente o token.

   - **Acceso de cuenta a datos cifrados**. Configure el acceso de usuario a la unidad cifrada. Por ejemplo, puede desactivar temporalmente la autenticación de usuario en lugar de eliminar la cuenta del Agente de autenticación.

   - **Comentario**. Introduzca una descripción de la cuenta, si es necesario.

8. Guarde los cambios.

9. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Para eliminar una cuenta del Agente de autenticación, debe añadir un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Es conveniente utilizar una tarea de grupo, por ejemplo, para eliminar la cuenta de un trabajador despedido.

Cómo eliminar una cuenta del Agente de autenticación mediante la Consola de administración (MMC)

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.

2. En las propiedades de tarea, seleccione la sección **Configuración**.

3. Haga clic en **Añadir → Comando de eliminación de cuentas**.

4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de usuario de Windows que se utilizó para crear la cuenta del Agente de autenticación que quiere eliminar.

5. Si ha introducido el nombre de una cuenta de Windows manualmente, haga clic en el botón **Permitir** para definir el identificador de seguridad de la cuenta (SID).

   Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Permitir**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

   > Es necesario definir un identificador de seguridad de la cuenta de Windows para verificar que el nombre de la cuenta de Windows se ha introducido correctamente. Si la cuenta de Windows introducida no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con error.

6. Guarde los cambios.

Cómo eliminar una cuenta del Agente de autenticación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Administrar cuentas del Agente de autenticación** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Añadir** y seleccione el tipo de comando **Eliminar cuenta**.

5. Seleccione una cuenta de usuario. Puede seleccionar una cuenta de la lista de cuentas de dominio o introducir manualmente el nombre de la cuenta.

6. Guarde los cambios.

7. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el usuario no podrá completar el procedimiento de autenticación ni cargar el sistema operativo. Kaspersky Endpoint Security denegará el acceso a los datos cifrados.

Para ver la lista de usuarios que pueden completar la autenticación con el Agente y cargar el sistema operativo, tiene que acceder a las propiedades del equipo administrado.

Cómo ver la lista de cuentas del Agente de autenticación mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos**.
3. Haga doble clic para abrir la ventana de propiedades del equipo.
4. En la ventana de propiedades del equipo, seleccione la sección **Tareas**.
5. En la lista de tareas, seleccione **Administrar cuentas del Agente de autenticación** y abra las propiedades de la tarea haciendo doble clic.
6. En las propiedades de tarea, seleccione la sección **Configuración**.

Como resultado, podrá acceder a una lista de las cuentas del Agente de autenticación en este equipo. Solo los usuarios de la lista pueden completar la autenticación con el Agente y cargar el sistema operativo.

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Haga clic en el nombre del equipo en el que desea ver la lista de cuentas del Agente de autenticación.
3. En las propiedades del equipo, seleccione la pestaña **Tareas**.
4. En la lista de tareas, seleccione **Administrar cuentas del Agente de autenticación**.
5. En las propiedades de tarea, seleccione la pestaña **Configuración de la aplicación**.

Como resultado, podrá acceder a una lista de las cuentas del Agente de autenticación en este equipo. Solo los usuarios de la lista pueden completar la autenticación con el Agente y cargar el sistema operativo.

Utilizar una tarjeta inteligente y un token con el Agente de autenticación

Se puede utilizar una tarjeta inteligente o token para la autenticación cuando se accede a discos duros cifrados. Para ello, debe añadir el archivo del certificado electrónico de una tarjeta inteligente o token a la tarea *Administrar cuentas del Agente de autenticación*.

El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraran usando el algoritmo de cifrado AES56, no se podrá agregar el archivo del certificado electrónico al comando.

Kaspersky Endpoint Security admite los tókenes, los lectores de tarjeta inteligente y las tarjetas inteligentes siguientes:

- SafeNet eToken PRO 64 K (4.2b);
- SafeNet eToken PRO 72 K Java;

- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72 K Java;
- Aladdin-RD JaCarta PKI.

Para añadir el archivo de un certificado electrónico de token o tarjeta inteligente al comando con el fin de crear una cuenta del agente de autenticación, debe guardar primero el archivo usando el software de terceros para gestionar certificados.

El certificado del token o tarjeta inteligente tiene que tener las propiedades siguientes:

- El certificado debe cumplir con el estándar X.509 y el archivo de certificado tiene que tener codificación DER.
- El certificado contiene una clave RSA con una longitud de al menos 1024 bits.

Si el certificado electrónico del token o de la tarjeta electrónica no cumple con este requisito, no podrá cargar el archivo de certificado en el comando para crear una cuenta del Agente de autenticación.

El parámetro `KeyUsage` del certificado tiene que tener el valor `keyEncipherment` o `dataEncipherment`. El parámetro `KeyUsage` determina el propósito del certificado. Si el parámetro tiene un valor diferente, Kaspersky Security Center descargará el archivo del certificado pero mostrará una advertencia.

Si un usuario ha perdido un token o una tarjeta inteligente, el administrador debe añadir el archivo del certificado electrónico del token o la tarjeta inteligente al comando para crear una cuenta del Agente de autenticación. Luego, el usuario debe completar el procedimiento para obtener acceso a los dispositivos cifrados o restaurar datos de dispositivos cifrados.

Descifrado de discos duros

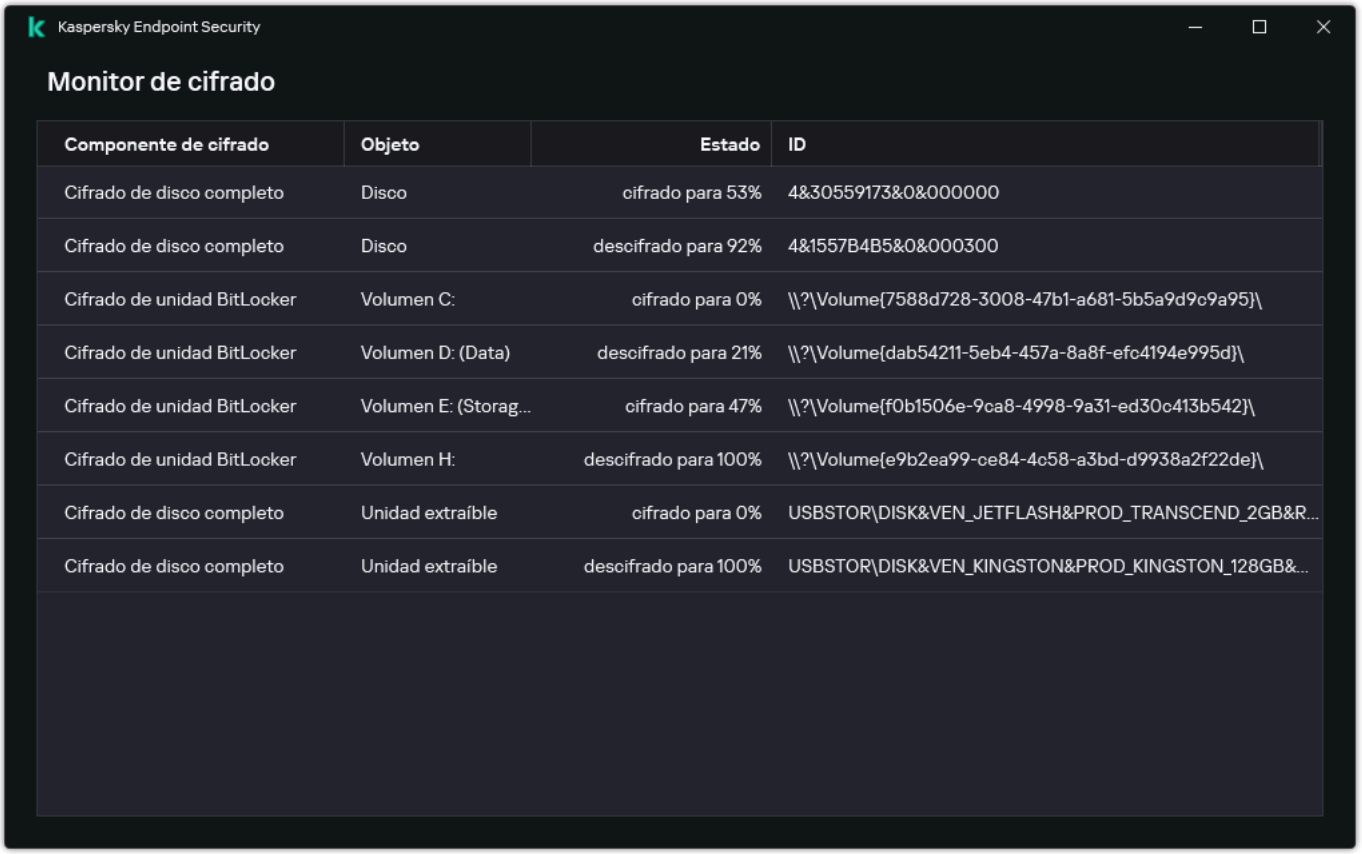
Puede descifrar discos duros incluso si no hay licencia actual que permita el cifrado de datos.

Para descifrar discos duros:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de disco completo**.
4. En la lista desplegable **Tecnología de cifrado**, seleccione la tecnología con la que se cifraron los discos duros.
5. Realice una de las siguientes acciones:
   - En la lista desplegable **Modo de cifrado**, seleccione la opción **Descifrar todos los discos duros** para descifrar todos los discos duros cifrados.
   - Añada los discos duros cifrados que desea descifrar a la tabla **No cifrar los siguientes discos duros**.

     Esta opción solo está disponible para la tecnología Cifrado de disco de Kaspersky.
6. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la ventana principal de la aplicación.



Monitor de cifrado

Si el usuario apaga o reinicia el equipo durante el descifrado de discos duros que fueron cifrados mediante tecnología de cifrado de disco de Kaspersky, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el descifrado del disco duro después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo cambia al modo de hibernación mientras se descifran discos duros que fueron cifrados mediante la tecnología de cifrado de disco de Kaspersky, el Agente de autenticación se carga cuando el sistema operativo sale del modo de hibernación. Kaspersky Endpoint Security reanuda el descifrado del disco duro después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo. Después de descifrar el disco duro, no se encontrará disponible el modo de hibernación hasta que se realice un primer reinicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el descifrado del disco duro, Kaspersky Endpoint Security reanudará el descifrado del disco duro cuando el sistema operativo salga del modo de hibernación sin cargar el Agente de autenticación.

Restauración del acceso a una unidad protegida por la tecnología Cifrado de disco de Kaspersky

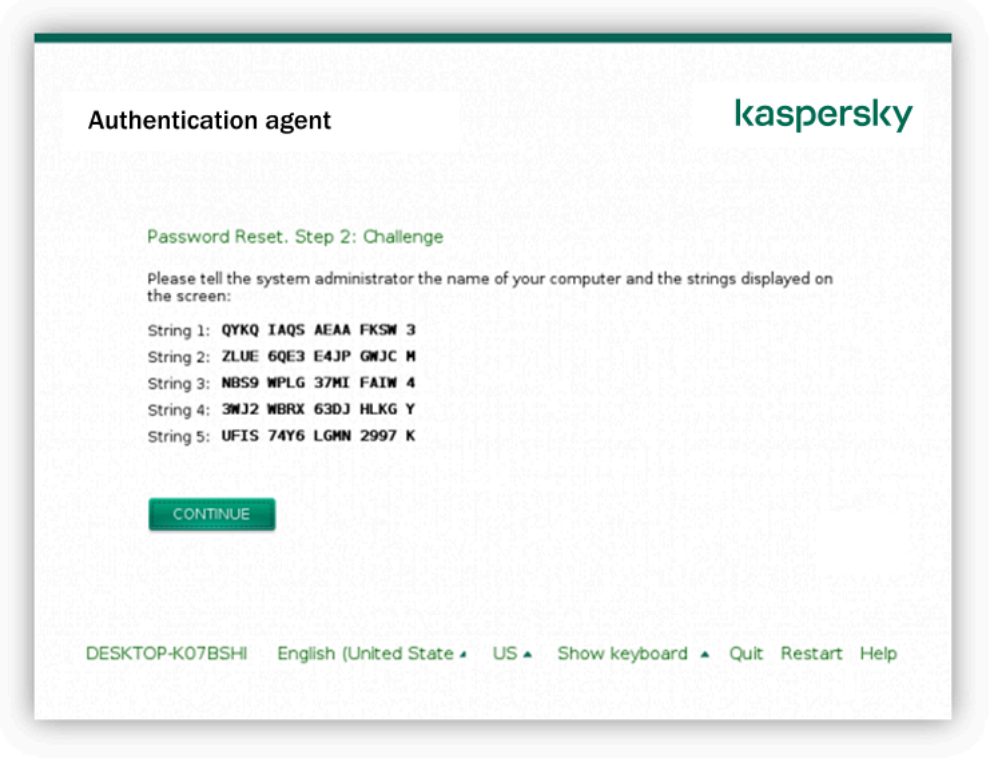
Si un usuario ha olvidado la contraseña para acceder a un disco duro protegido por la tecnología Cifrado de disco de Kaspersky, tiene que iniciar el procedimiento de recuperación (solicitud-respuesta). También puede utilizar la cuenta de servicio para obtener acceso al disco duro si esta característica está habilitada en la configuración de cifrado del disco.

Restauración del acceso al disco duro del sistema

La restauración del acceso a un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky consta de los siguientes pasos:

1. El usuario proporciona los bloques de solicitud al administrador (vea la imagen más abajo).
2. El administrador introduce los bloques de solicitud en Kaspersky Security Center, recibe los bloques de respuesta y proporciona los bloques de respuesta al usuario.

3. El usuario introduce los bloques de respuesta en la interfaz del Agente de autenticación y obtiene acceso al disco duro.



Restauración del acceso a un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky

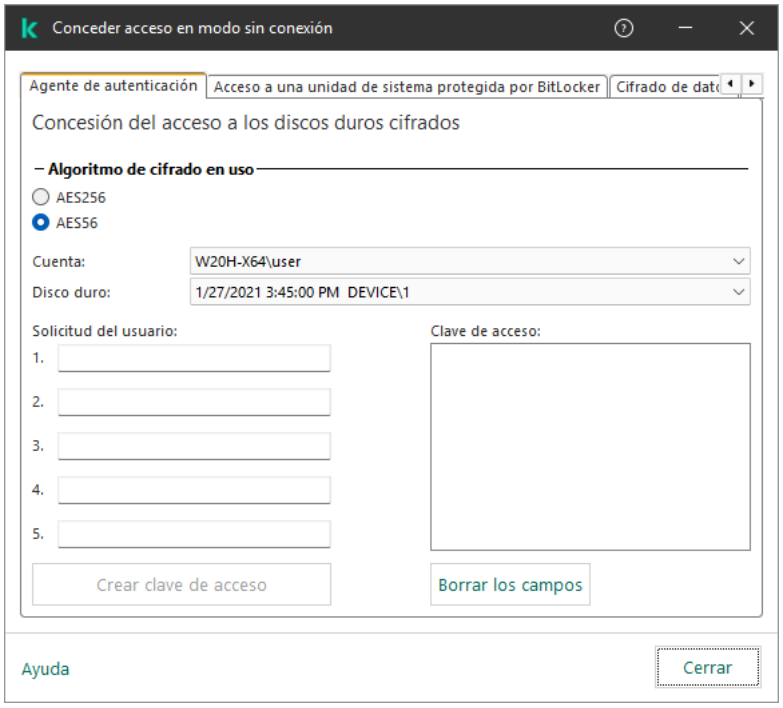
Para comenzar el procedimiento de recuperación, el usuario tiene que hacer clic en el botón **Forgot your password** en la interfaz del Agente de autenticación.

Cómo obtener bloques de respuesta para un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos**.
3. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
4. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
5. Se abre una ventana; en ella, seleccione la pestaña **Agente de autenticación**.
6. En el bloque **Algoritmo de cifrado en uso**, seleccione un algoritmo de cifrado: **AES56** o **AES256**.

   El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: *Cifrado fuerte (AES256)* o *Cifrado ligero (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.
7. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación del usuario que solicitó la recuperación del acceso a la unidad.
8. En la lista desplegable **Disco duro**, seleccione el disco duro cifrado para el cual debe recuperar el acceso.
9. En el bloque **Solicitud del usuario**, introduzca los bloques de solicitud que ha establecido el usuario.

Como resultado, el contenido de los bloques de la respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de la cuenta del Agente de autenticación se mostrará en el campo **Clave de acceso**. Transmita el contenido de los bloques de respuesta al usuario.



Conceder acceso en modo sin conexión

Cómo obtener bloques de respuesta para un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuya unidad quiere restaurar el acceso.
3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione la sección **Agente de autenticación**.
5. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación creada para el usuario que está solicitando la recuperación del nombre y la contraseña de la cuenta del Agente de autenticación.
6. Introduzca los bloques de solicitud transmitidos por el usuario.

   El contenido de las secciones de la respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de la cuenta del Agente de autenticación se mostrará en la parte inferior de la ventana. Transmita el contenido de los bloques de respuesta al usuario.

Tras completar el procedimiento de recuperación, el Agente de autenticación solicitará al usuario que cambie la contraseña.

Restauración del acceso a un disco duro que no pertenece al sistema

La restauración del acceso a un disco duro que no pertenece al sistema protegido por la tecnología Cifrado de disco de Kaspersky consta de los siguientes pasos:

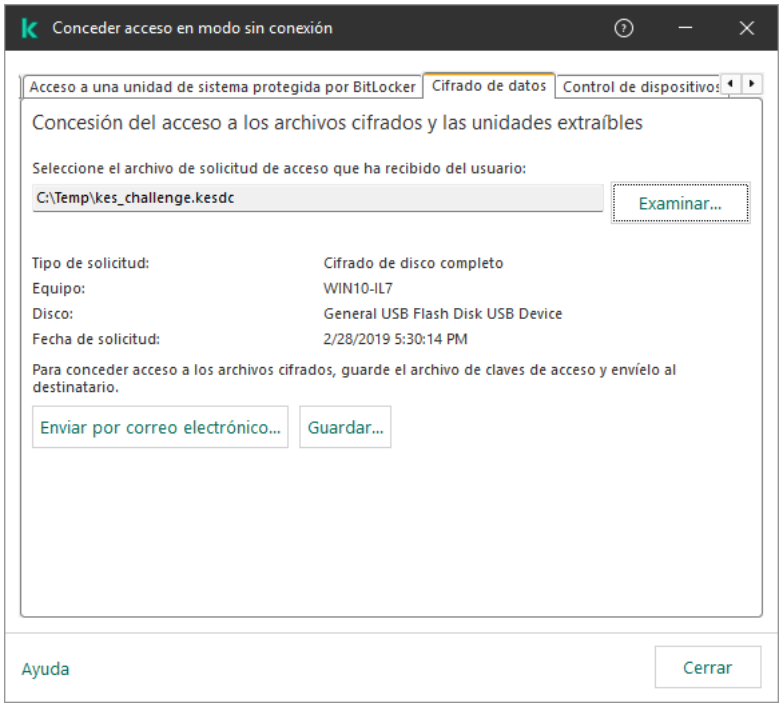
1. El usuario envía un archivo de solicitud de acceso al administrador.
2. El administrador añade el archivo de solicitud de acceso a Kaspersky Security Center, crea un archivo clave de acceso y lo envía al usuario.
3. El usuario añade el archivo clave de acceso a Kaspersky Endpoint Security y obtiene acceso al disco duro.

Para comenzar el procedimiento de recuperación, el usuario tiene que intentar acceder a un disco duro. Como resultado, Kaspersky Endpoint Security creará un archivo de solicitud de acceso (un archivo con la extensión KESDC), que el usuario tiene que enviar al administrador, por ejemplo, por correo electrónico.

Cómo obtener un archivo clave de acceso para un disco duro cifrado que no pertenece al sistema en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos**.
3. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
4. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
5. Se abre una ventana; en ella, seleccione la pestaña **Cifrado de datos**.
6. En la pestaña **Cifrado de datos**, haga clic en el botón **Examinar**.
7. En la ventana para seleccionar un archivo de solicitud de acceso, especifique la ruta al archivo recibido del usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.



Conceder acceso en modo sin conexión

Cómo obtener un archivo clave de acceso a un disco duro cifrado que no pertenece al sistema en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuyos datos quiere restaurar el acceso.
3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.
4. Seleccione **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión KESDC).

   Web Console mostrará información sobre la solicitud. Esto incluirá el nombre del equipo en el que el usuario solicita acceso al archivo.
6. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión KESDR).

Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

Inicio de sesión con la cuenta de servicio del Agente de autenticación

Kaspersky Endpoint Security le permite añadir una cuenta de servicio del Agente de autenticación al cifrar una unidad. La cuenta de servicio es necesaria para acceder al equipo, por ejemplo, cuando el usuario olvida la contraseña. También puede utilizar la cuenta de servicio como cuenta de reserva. Para añadir una cuenta, seleccione una cuenta de servicio en la configuración del cifrado de disco e ingrese el nombre de la cuenta de usuario (por defecto, `ServiceAccount`). Para autenticarse con el agente, necesitará una contraseña de un solo uso.

Cómo averiguar la contraseña de un solo uso en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos**.
3. Haga doble clic para abrir la ventana de propiedades del equipo.
4. En la ventana de propiedades del equipo, seleccione la sección **Tareas**.
5. En la lista de tareas, seleccione **Administrar cuentas del Agente de autenticación** y abra las propiedades de la tarea haciendo doble clic.
6. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
7. En la lista de cuentas, seleccione la cuenta de servicio del Agente de autenticación (por ejemplo, `WIN10-USER\ServiceAccount`).
8. En la lista desplegable **Acción**, seleccione **Ver cuenta**.
9. En las propiedades de la cuenta, seleccione la casilla de verificación **Mostrar contraseña original**.
10. Copie la contraseña de un solo uso para iniciar sesión con la cuenta de servicio.

Cómo encontrar la contraseña de un solo uso en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Haga clic en el nombre del equipo en el que desea ver la lista de cuentas del Agente de autenticación.

   Se abren las propiedades del equipo.
3. En las propiedades del equipo, seleccione la pestaña **Tareas**.
4. En la lista de tareas, seleccione **Administrar cuentas del Agente de autenticación**.
5. En las propiedades de tarea, seleccione la pestaña **Configuración de la aplicación**.
6. En la lista de cuentas, seleccione la cuenta de servicio del Agente de autenticación (por ejemplo, `WIN10-USER\ServiceAccount`).

7. En las propiedades de la cuenta, seleccione la casilla de verificación **Mostrar contraseña**.

8. Copie la contraseña de un solo uso para iniciar sesión con la cuenta de servicio.

Kaspersky Endpoint Security actualiza automáticamente la contraseña cada vez que un usuario se autentica con la cuenta de servicio. Después de autenticarse con el agente, debe ingresar la contraseña de la cuenta de Windows. Al iniciar sesión con la cuenta de servicio, no puede utilizar la tecnología SSO.

Actualización del sistema operativo

A la hora de actualizar el sistema operativo de un equipo protegido con la característica Cifrado de disco completo (FDE), existen ciertas consideraciones que se deben tener en cuenta. La actualización debe realizarse de este modo: primero se debe actualizar el SO de un único equipo, luego el de un grupo reducido de equipos y, finalmente, el de todos los equipos conectados a la red.

Cuando se utiliza la tecnología Cifrado de disco de Kaspersky, el Agente de autenticación se carga antes que el sistema operativo. El Agente de autenticación permite que el usuario inicie sesión en el sistema y reciba acceso a las unidades cifradas. Solo entonces comienza la carga del sistema operativo. Si intenta actualizar el sistema operativo de un equipo protegido con la tecnología Cifrado de disco de Kaspersky, el asistente para actualizar el SO desinstalará el Agente de autenticación. Como resultado, el equipo puede quedar bloqueado porque el cargador del SO no podrá acceder a la unidad cifrada.

Características de la actualización del sistema operativo:

- **Actualización del sistema operativo a través de WSUS**. Puede actualizar el sistema operativo de la forma habitual.

- **Actualización del sistema operativo desde ISO**. Para actualizar el sistema operativo, debe especificar la carpeta con los controladores de cifrado de disco de Kaspersky . La aplicación copia automáticamente los controladores en una carpeta separada. Haga lo siguiente:

  1. Monte la imagen ISO.

  2. Inicie la instalación de la actualización del sistema con la siguiente clave:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

La actualización automática del sistema operativo solo está disponible si el equipo ejecuta Windows 10 1607 (RS1) o una versión posterior. Para actualizar versiones anteriores del sistema operativo, se recomienda que primero descifre el disco, realice una actualización del sistema operativo y luego cifre el disco.

Cuando se utiliza la tecnología de cifrado de unidad BitLocker, no es necesario descifrar los discos duros para actualizar Windows 10. Para obtener más información sobre BitLocker, visite el sitio web de Microsoft.

Eliminación de errores al actualizar la función de cifrado

El Cifrado de disco completo se actualiza cuando la versión anterior de la aplicación se actualiza a Kaspersky Endpoint Security para Windows 14.2.

Al iniciar la actualización de la función Cifrado de disco completo, pueden ocurrir los siguientes errores:

- No se puede iniciar la actualización.
- El dispositivo no es compatible con el Agente de autenticación.

Para eliminar los errores que ocurrieron al iniciar el proceso de actualización de la función Cifrado de disco completo en la nueva versión de la aplicación es necesario:

1. Descifrar los discos duros.
2. Cifrar los discos duros de nuevo.

Durante la actualización de la función Cifrado de disco completo pueden ocurrir los siguientes errores:

- No se puede completar la actualización.
- La reversión de la actualización de Cifrado de disco completo se ha completado con un error.

Para eliminar los errores que ocurrieron durante el proceso de actualización de la función Cifrado de disco completo,

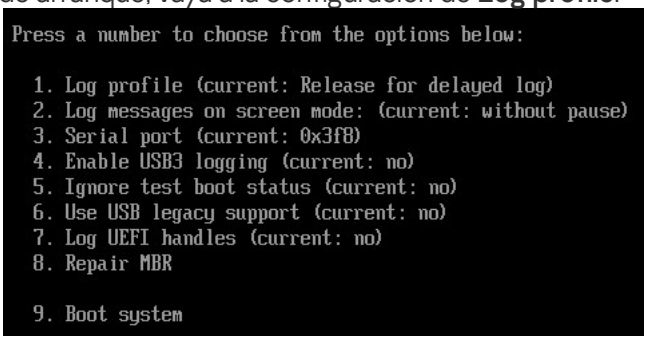
restaure el acceso a dispositivos cifrados con la Utilidad de Restauración.

Seguimiento del agente de autenticación

La aplicación registra información de servicio sobre el funcionamiento del Agente de autenticación e información sobre las operaciones de usuario con el Agente de autenticación en el archivo de seguimiento.

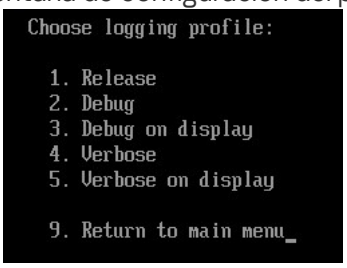
Para activar el seguimiento del Agente de autenticación:

1. Active el seguimiento de Kaspersky Endpoint Security.
2. Reinicie el equipo.
3. En cuanto se inicie un equipo con discos duros cifrados, pulse el botón **F3** para llamar a una ventana y configurar los ajustes del Agente de autenticación.
4. Después de que se inicie el cargador de arranque FDE, seleccione el administrador de arranque de **KES (FDE <version>)**.
5. En el menú del administrador de arranque, vaya a la configuración de **Log profile**.



Menú del administrador de arranque

6. Seleccione el nivel de seguimiento en la ventana de configuración del perfil de registro:



Niveles de seguimiento del Agente de autenticación

- **Release**. Si esta opción se selecciona, la aplicación no registra la información de eventos del Agente de autenticación en el archivo de seguimiento.
- **Debug**. Si se selecciona esta opción, la aplicación registra información sobre el funcionamiento del agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento.
- **Debug on display**. Si se selecciona esta opción, la aplicación registra información sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento y las transmite a través del puerto COM.

  Si un equipo con discos duros cifrados está conectado a otro equipo a través del puerto COM, los eventos del Agente de autenticación se pueden examinar desde este otro equipo.
- **Verbose**. Si se selecciona esta opción, la aplicación registra información detallada sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento.

  El nivel de detalle de las entradas de esta opción es superior en comparación con el nivel de la opción **Debug**. Un nivel elevado de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.
- **Verbose on display**. Si se selecciona esta opción, la aplicación incluye entradas detalladas sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento, y las transmite a través del puerto COM.

  El nivel de detalle de las entradas de esta opción es superior en comparación con el nivel de la opción **Debug on display**. Un nivel elevado de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.

Después de seleccionar un nivel de seguimiento, el administrador de arranque vuelve a mostrar el menú.

7. En el menú del administrador de arranque, seleccione **Boot system**.

   El cargador de arranque FDE inicia el Agente de autenticación.

   Reproduzca el problema.

   Los datos se registran en el archivo de seguimiento del Agente de autenticación si hay discos duros cifrados en el equipo o durante el cifrado de disco completo.

8. Para detener el proceso de seguimiento, vuelva a la ventana Herramientas de soporte y desactive el seguimiento.

Como resultado, se crean archivos de rastreo del funcionamiento del Agente de autenticación KES.SRV en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. El archivo de seguimiento del Agente de

autenticación no se envía a Kaspersky a diferencia de otros archivos de seguimiento de la aplicación. Si fuera necesario, puede enviar manualmente el archivo de seguimiento del Agente de autenticación a Kaspersky para su análisis.

Editar los textos de ayuda del Agente de autenticación

Antes de modificar los mensajes de ayuda del Agente de autenticación, revise la lista de caracteres que pueden usarse en un entorno de prearranque (ver más abajo).

Para editar los mensajes de ayuda del Agente de autenticación:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Configuración común de cifrado**.
4. En el bloque **Plantillas**, haga clic en el botón **Ayuda**.
5. En la ventana que se abre, haga lo siguiente:
   - Seleccione la pestaña **Autenticación** para editar el texto de ayuda que se muestra en la ventana Agente de autenticación cuando se introducen las credenciales de la cuenta.
   - Seleccione la pestaña **Cambiar la contraseña** para editar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se cambia la contraseña de la cuenta del Agente de autenticación.
   - Seleccione la pestaña **Recuperar la contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se recupera la contraseña de la cuenta del Agente de autenticación.
6. Modifique los mensajes de la ayuda.

   Si quiere restaurar el texto original, haga clic en el botón **Predeterminado**.

   Puede introducir texto de ayuda que contenga 16 líneas o menos. La longitud máxima de línea es 64 caracteres.
7. Guarde los cambios.

Compatibilidad limitada con los caracteres de los mensajes de ayuda del Agente de autenticación

En un entorno anterior al arranque, se admiten los siguientes caracteres de Unicode:

- Alfabeto latino básico (0000 - 007F)
- Caracteres de Latino-1 adicionales (0080 - 00FF)
- Latino-A ampliado (0100 - 017F)

- Latino-A ampliado (0180 - 024F)
- Caracteres de ID ampliados no combinados (02B0 - 02FF)
- Marcas diacríticas combinadas (0300 - 036F)
- Alfabetos griego y copto (0370 - 03FF)
- Alfabeto cirílico (0400 - 04FF)
- Hebreo (0590 - 05FF)
- Script árabe (0600 - 06FF)
- Latino ampliado adicional (1E00 - 1EFF)
- Signos de puntuación (2000 - 206F)
- Símbolos de divisa (20A0 - 20CF)
- Símbolos parecidos a una letra (2100 - 214F)
- Cifras geométricas (25A0 - 25FF)
- Formularios de presentación de alfabeto árabe B (FE70 - FEFF)

Los caracteres que no se especifican en esta lista no se admiten en un entorno anterior al arranque. No se recomienda usar tales caracteres en mensajes de ayuda del Agente de autenticación.

Eliminar los objetos y datos restantes después de probar el Agente de autenticación

Durante la desinstalación de la aplicación, si Kaspersky Endpoint Security detecta objetos y datos que permanecieron en el disco duro del sistema después de la operación de prueba del Agente de autenticación, la desinstalación de aplicación se interrumpe y se hace imposible hasta que esos objetos y datos se eliminan.

Solamente en casos excepcionales, los objetos y los datos pueden permanecer en el disco duro del sistema después de la operación de prueba del Agente de autenticación. Por ejemplo, esto puede suceder si el equipo no se ha reiniciado después de que se aplicara una directiva de Kaspersky Security Center con configuración de cifrado o la aplicación no puede iniciarse después de la operación de prueba del Agente de autenticación.

Puede quitar objetos y datos restantes en el disco duro del sistema después de una operación de prueba del Agente de autenticación de varias maneras:

- Mediante la directiva de Kaspersky Security Center.
- mediante Utilidad de restauración.

Para utilizar una directiva de Kaspersky Security Center con el fin de eliminar objetos y datos que permanecieron después de la operación de prueba del Agente de autenticación:

1. Aplique al equipo una directiva de Kaspersky Security Center con la configuración definida para descifrar todos los discos duros del equipo.
2. Inicie Kaspersky Endpoint Security.

Para utilizar la Utilidad de restauración con el fin de eliminar objetos y datos que quedaron después de la operación de prueba del Agente de autenticación:

1. Ejecute el archivo con el nombre fdert.exe, que es el archivo ejecutable de la Utilidad de restauración. Kaspersky Endpoint Security crea este archivo.
2. En la ventana de la Utilidad de restauración, seleccione el dispositivo requerido.
3. Haga clic en **Analizar**.
4. Si, después de diagnosticar el disco duro del sistema, recibe un mensaje que indica que quedan objetos y datos de la operación de prueba del Agente de autenticación, haga clic en **Eliminar objetos y datos de AA**.

   El botón **Eliminar objetos y datos de AA** solo está disponible si se detectan objetos y datos que quedan después de la operación de prueba del Agente de autenticación.

Para eliminar la información sobre la incompatibilidad de la aplicación con Agente de autenticación,

escriba el comando `avp pbatestreset` en la línea de comandos.

Administración de BitLocker

BitLocker es una tecnología de cifrado integrada en los sistemas operativos Windows. Kaspersky Endpoint Security le permite controlar y administrar BitLocker utilizando Kaspersky Security Center. BitLocker cifra los volúmenes lógicos. BitLocker no se puede utilizar para el cifrado de unidades extraíbles. Para obtener más detalles sobre BitLocker, consulte la documentación de Microsoft.

Al cifrar el disco, BitLocker coloca el cargador de arranque y otros archivos auxiliares en la system partition. Esta partición no está cifrada. El sistema operativo crea la partición del sistema automáticamente durante la instalación de Windows. Si el disco está completamente particionado antes de instalar Windows, el sistema operativo no puede crear una partición del sistema. En este caso, cuando inicia el cifrado de disco de BitLocker, el sistema operativo le solicita que vuelva a particionar el disco y cree una partición del sistema. Después de crear una partición del sistema, el sistema operativo inicia el cifrado de BitLocker.

El algoritmo de cifrado de BitLocker no depende de la versión de la biblioteca AES incluida en el paquete de distribución (AES256 o AES56). El cifrado utiliza la biblioteca de cifrado incorporada en el sistema operativo.

De forma predeterminada, la aplicación utiliza el algoritmo de cifrado BitLocker con una longitud de clave efectiva de 256 bits para cifrar los dispositivos que nunca se han cifrado. En el caso de un dispositivo que se haya cifrado antes de instalar la aplicación, el algoritmo de cifrado puede ser diferente. Para obtener información detallada sobre la selección del algoritmo de cifrado, consulte el sitio web del soporte técnico de Microsoft. A partir de la versión 12.9, Kaspersky Endpoint Security envía a Kaspersky Security Center la clave de recuperación original de dispositivos previamente cifrados por aplicaciones de terceros.

BitLocker proporciona almacenamiento seguro de claves de acceso utilizando un módulo de plataforma segura. Un *Trusted Platform Module* (TPM) es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del equipo e interactúa con todos los otros componentes del sistema a través del bus de hardware. Utilizar el módulo TPM es el modo más seguro de almacenar las clave de acceso de BitLocker, ya que TPM proporciona verificación de integridad del sistema antes del inicio. Sigue pudiendo cifrar unidades en un equipo sin un módulo TPM. En este caso, la clave de acceso se cifrará con una contraseña. BitLocker utiliza los siguientes métodos de autenticación:

- TPM.
- TPM y PIN.
- Contraseña.

Después de cifrar el disco duro del sistema, el usuario debe pasar por el procedimiento de autenticación de BitLocker para iniciar el sistema operativo. Después de la autenticación, BitLocker permite que el usuario inicie sesión. BitLocker no admite la tecnología Single Sign-On (SSO).

Después de cifrar una unidad, BitLocker crea una clave de recuperación. Kaspersky Endpoint Security envía la clave maestra a Kaspersky Security Center para que pueda restaurar el acceso al disco, por ejemplo, si un usuario ha olvidado su contraseña.

Si un usuario cifra un disco con BitLocker, Kaspersky Endpoint Security enviará la clave de recuperación y información sobre el cifrado de disco a Kaspersky Security Center.

Si está utilizando directivas de grupo de Windows, desactive la administración de BitLocker en la configuración de directivas. La configuración de directivas de Windows puede entrar en conflicto con la configuración de directivas de Kaspersky Endpoint Security. Al cifrar una unidad, pueden producirse errores.

Inicio del Cifrado de unidad BitLocker

Antes de comenzar el cifrado de disco completo, es aconsejable asegurarse de que el equipo no esté infectado. Para ello, ejecute la tarea Análisis completo o Análisis de áreas críticas. Cifrar un disco completo en un equipo infectado con un rootkit puede provocar que el equipo se inutilice.

Para usar el Cifrado de unidad BitLocker en equipos con sistemas operativos Windows para servidores, puede ser necesario instalar el componente Cifrado de unidad BitLocker. Instale el componente con las herramientas del sistema operativo (Asistente para añadir roles y componentes). Para obtener más información sobre cómo instalar el Cifrado de unidad BitLocker, consulte la documentación de Microsoft.

Cómo ejecutar el Cifrado de unidad BitLocker mediante la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de disco completo**.
4. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de unidad BitLocker**.

5. En la lista desplegable **Modo de cifrado**, seleccione **Cifrar todos los discos duros**.

> Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo en el que se hizo el cifrado.

6. Configure las opciones avanzadas de Cifrado de unidad BitLocker (consulte la tabla a continuación).
7. Guarde los cambios.

Cómo ejecutar el Cifrado de unidad BitLocker mediante Web Console

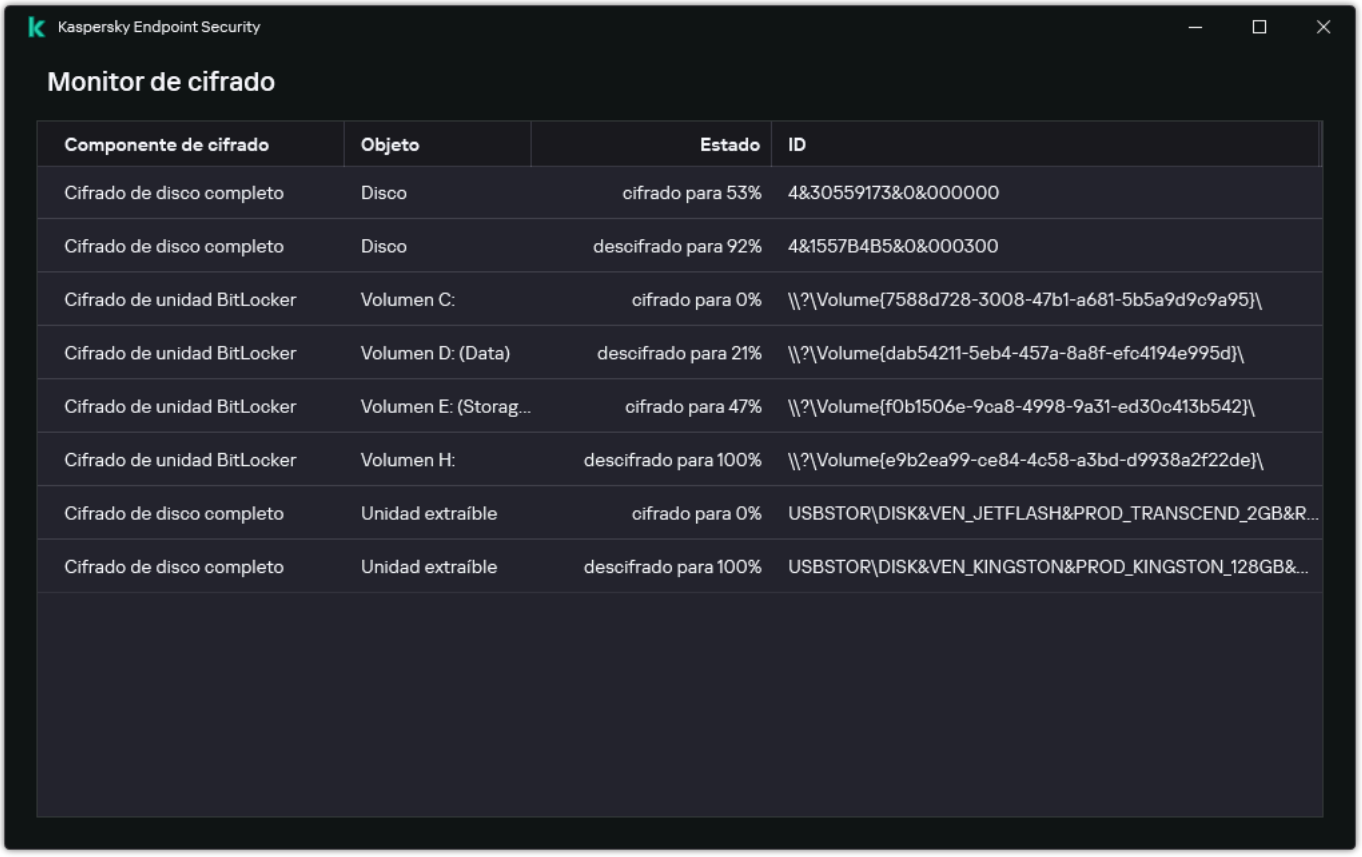
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos** → **Cifrado de disco completo**.
5. Seleccione la tecnología **Cifrado de disco BitLocker**.
6. En el bloque **Acción en los dispositivos**, seleccione **Cifrar todos los discos duros**.

> Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo en el que se hizo el cifrado.

7. Configure las opciones avanzadas de Cifrado de unidad BitLocker (consulte la tabla a continuación).
8. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la ventana principal de la aplicación.



Monitor de cifrado

Después de aplicar la directiva, la aplicación muestra las siguientes preguntas según la configuración de la autenticación:

- Solo TPM. No se requiere la acción del usuario. El disco se cifrará cuando se reinicie el equipo.
- TPM + PIN/Contraseña. Si un módulo TPM está disponible, se abre una ventana para escribir el código PIN. Si un módulo TPM no está disponible, verá una ventana de contraseña para la autenticación previa al arranque.
- Solo contraseña. Verá una ventana de solicitud de contraseña para la autenticación previa al inicio.

Si el modo de compatibilidad con los Estándares federales de procesamiento de la información está habilitado para el sistema operativo del equipo, entonces en Windows 8 y versiones anteriores del sistema operativo se mostrará una solicitud para conectar un dispositivo de almacenamiento para guardar el archivo clave de recuperación. Puede guardar varios archivos de clave de recuperación en un solo dispositivo de almacenamiento.

Después de establecer una contraseña o un PIN, BitLocker le pedirá que reinicie su equipo para completar el cifrado. A continuación, el usuario debe pasar por el procedimiento de autenticación de BitLocker. Tras el procedimiento de autenticación, el usuario debe iniciar sesión en el sistema. Una vez que el sistema operativo se haya cargado, BitLocker completará el cifrado.

Si no hay acceso a claves de cifrado, el usuario puede solicitar que el administrador de la red local le proporcione una clave de recuperación (siempre que la clave de recuperación no se haya guardado anteriormente en el dispositivo USB o se haya perdido).

Parámetro	Descripción
Activar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en tabletas	Uso de la autenticación que requiere la entrada de datos en un entorno de prearranque, incluso si la plataforma no tiene la capacidad de entrada de prearranque (por ejemplo, con los teclados de la pantalla táctil de las tabletas). La pantalla táctil de las tabletas no está disponible en el entorno de prearranque. Para completar la autenticación BitLocker en tabletas, el usuario debe conectar un teclado USB, por ejemplo. Si selecciona, se permite el uso de la autenticación que requiere la entrada de prearranque en las tabletas. Recomendamos utilizar esta configuración solo en dispositivos con herramientas alternativas de entrada de datos en un entorno de prearranque, como un teclado USB, además de los teclados de la pantalla táctil. Si se desactiva, el Cifrado de unidad BitLocker no es posible en tabletas.
Utilizar cifrado de hardware (Windows 8 y versiones posteriores)	Si se selecciona, la aplicación utiliza el cifrado basado en hardware, lo que le permite aumentar la velocidad de cifrado y utilizar menos recursos del equipo.
Cifrar solo el espacio en disco utilizado (Windows 8 y versiones posteriores)	Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado. Activar o desactivar la función **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado. Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden. Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente. Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De forma predeterminada, la casilla de verificación está desactivada.

Parámetro	Descripción
Método de autenticación	**Solo contraseña (Windows 8 y versiones posteriores)** Si se selecciona esta opción, Kaspersky Endpoint Security solicita una contraseña al usuario cada vez que este intenta acceder a la unidad cifrada. Se puede seleccionar cuando el módulo de plataforma segura (TPM) no se está utilizando. **Módulo de plataforma segura (TPM)** Si se selecciona esta opción, BitLocker utiliza el módulo de plataforma segura (TPM). Un *Trusted Platform Module* (TPM) es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del equipo e interactúa con todos los otros componentes del sistema a través del bus de hardware. En equipos con Windows 7 o Windows Server 2008 R2, solo es posible utilizar el cifrado con módulo TPM. El cifrado BitLocker no está disponible en equipos que no cuentan con este módulo. No es posible utilizar una contraseña en tales equipos. Un dispositivo equipado con un módulo de plataforma segura puede crear claves de cifrado que solo con dicho dispositivo se pueden descifrar. El módulo de plataforma segura cifra las claves de cifrado con su propia clave raíz de almacenamiento. La clave raíz de almacenamiento se guarda en el módulo de plataforma segura, lo que proporciona un nivel adicional de protección contra los intentos de piratear las claves de cifrado. Esta acción está seleccionada de forma predeterminada. Puede establecer una capa de protección adicional para acceder a la clave de cifrado, y cifrar la clave con una contraseña o PIN: • **Utilizar PIN para el TPM**. Si esta casilla de verificación está seleccionada, un usuario puede utilizar un código PIN para obtener acceso a una clave de cifrado almacenada en el módulo de plataforma segura (TPM). Si la casilla no está seleccionada, se prohíbe a los usuarios utilizar códigos PIN. Para acceder a la clave de cifrado, un usuario debe introducir la contraseña. • **Módulo de plataforma segura (TPM), o contraseña si el TPM no está disponible**. Si se selecciona esta opción, el usuario podrá utilizar una contraseña para acceder a claves de cifrado cuando el módulo de plataforma segura (TPM) no esté disponible. Si no se seleccionó la casilla de verificación y el módulo TPM no está disponible, no comenzará el cifrado de disco completo. El método de autenticación seleccionado debe configurarse especificando requisitos de contraseña o PIN: • **Longitud mínima de PIN (caracteres)** (el valor predeterminado es 6). • **Longitud mínima de la contraseña (caracteres)** (el valor predeterminado es 8). • **Número máximo de contraseñas/PIN almacenados** (el valor predeterminado es 5). • **Limitar el período de validez de la contraseña / PIN para el TPM (días)** (desactivado de forma predeterminada). • **Usar un PIN mejorado (letras y números)**. El *PIN optimizado* permite utilizar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios. Desactivado de forma predeterminada.
Recrear automáticamente la clave de recuperación (días)	Actualice automáticamente la contraseña para restaurar el acceso a una unidad protegida por BitLocker. Si la casilla está seleccionada, especifique el periodo de validez de la contraseña de la clave de recuperación. Esto evita que la contraseña de la clave de recuperación se reutilice.

Descifrado de un disco duro protegido por BitLocker

Los usuarios pueden descifrar un disco utilizando el sistema operativo (la función *Desactivar BitLocker*). Después de eso, Kaspersky Endpoint Security solicitará al usuario que vuelva a cifrar el disco. Kaspersky Endpoint Security solicitará el cifrado del disco, a menos que active el descifrado del disco en la directiva.

Cómo descifrar un disco duro protegido por BitLocker a través de la Consola de administración (MMC)

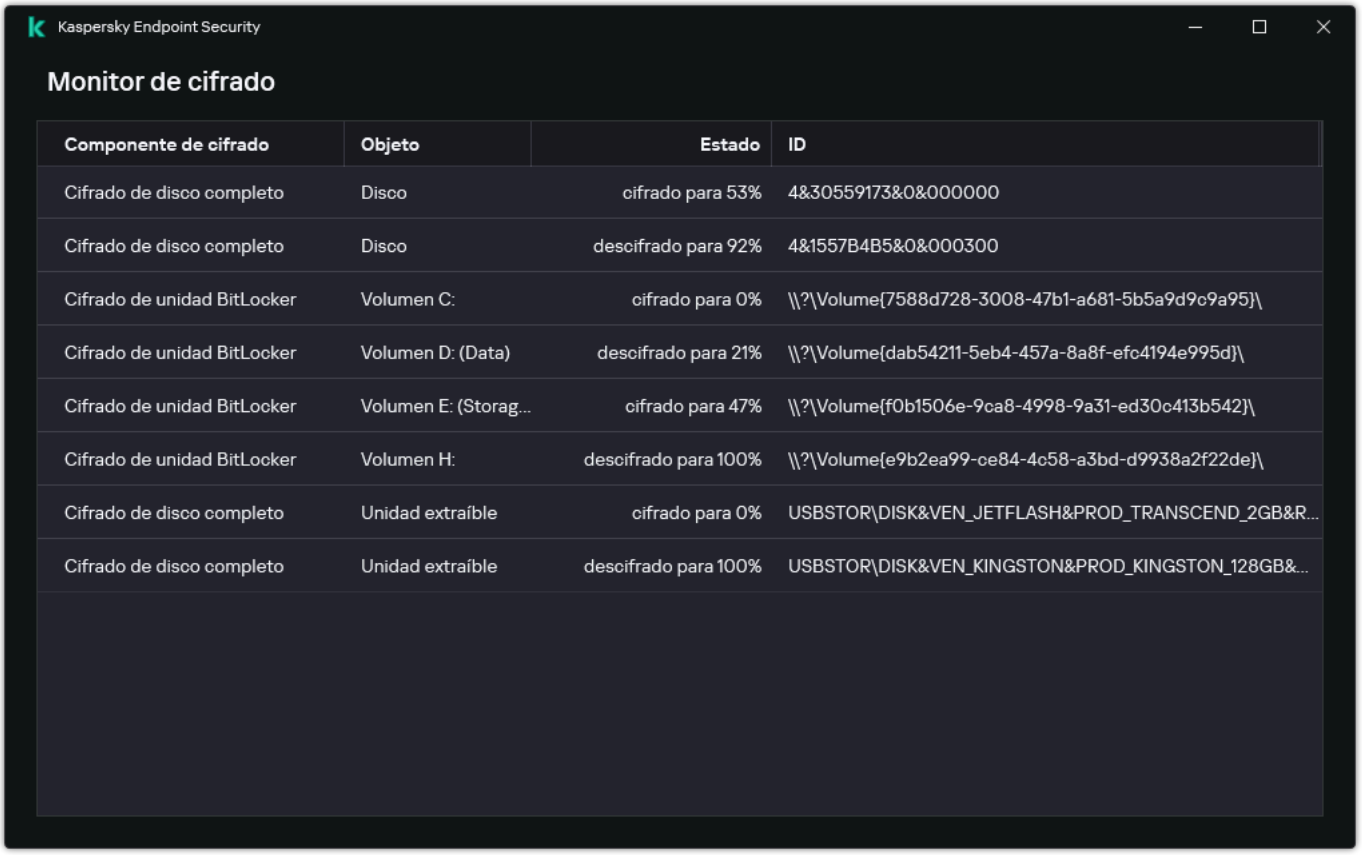
1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de disco completo**.
4. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de unidad BitLocker**.

5. En la lista desplegable **Modo de cifrado**, seleccione **Descifrar todos los discos duros**.
6. Guarde los cambios.

Cómo descifrar un disco duro cifrado con BitLocker mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos** → **Cifrado de disco completo**.
5. Seleccione la tecnología **Cifrado de disco BitLocker**.
6. En el bloque **Acción en los dispositivos**, seleccione **Descifrar todos los discos duros**.
7. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la ventana principal de la aplicación.



Monitor de cifrado

Restauración del acceso a una unidad protegida por BitLocker

Si un usuario ha olvidado la contraseña para acceder a un disco duro cifrado por BitLocker, tiene que iniciar el procedimiento de recuperación (solicitud-respuesta).

Si el sistema operativo del equipo tiene activado el modo de compatibilidad estándar de procesamiento de información federal (FIPS), entonces en Windows 8 y versiones anteriores, el archivo clave de recuperación se guarda en la unidad extraíble antes del cifrado. Para restaurar el acceso a la unidad, inserte la unidad extraíble y siga las instrucciones en pantalla.

La restauración del acceso a un disco duro cifrado por BitLocker consta de los siguientes pasos:

1. El usuario le dice al administrador el ID de la clave de recuperación (vea la imagen más abajo).
2. El administrador comprueba el ID de la clave de recuperación en las propiedades del equipo de Kaspersky Security Center. El ID que proporcionó el usuario debe coincidir con el ID que se muestra en las propiedades del equipo.
3. Si los ID de la clave de recuperación coinciden, el administrador proporciona al usuario la clave de recuperación o envía un archivo clave de recuperación.

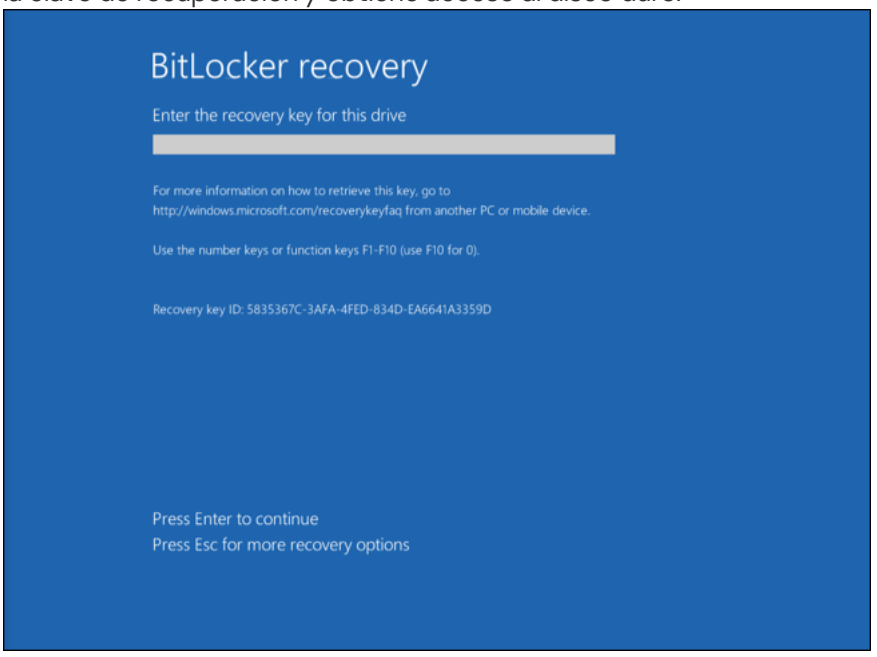
   Se utiliza un archivo clave de recuperación para los equipos que ejecutan los siguientes sistemas operativos:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   Para el resto de sistemas operativos, se utiliza una clave de recuperación.

   Para evitar la reutilización de la contraseña de la clave de recuperación, puede configurar la actualización automática de la contraseña en la configuración de la directiva.

4. El usuario introduce la clave de recuperación y obtiene acceso al disco duro.



Restauración del acceso a un disco duro cifrado por BitLocker

Restauración del acceso a un disco duro

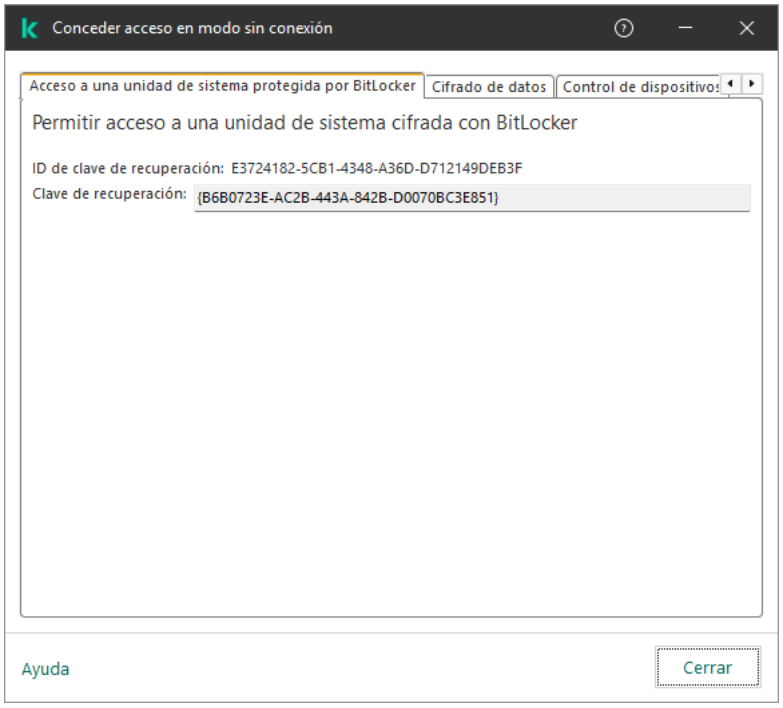
Para comenzar el procedimiento de recuperación, el usuario tiene que pulsar la tecla **Esc** en la etapa de autenticación en el prearranque.

Cómo ver la clave de recuperación para una unidad del sistema cifrada por BitLocker en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos administrados**.
3. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
4. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
5. Se abre una ventana; en ella, seleccione la pestaña **Acceso a una unidad de sistema protegida por BitLocker**.
6. Solicite al usuario el ID de la clave de recuperación indicado en la ventana de introducción de la contraseña de BitLocker y compárelo con el ID del campo **ID de clave de recuperación**.

   Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

Como resultado, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá transferirse al usuario.



Restauración del acceso a una unidad cifrada por BitLocker

Cómo ver la clave de recuperación para una unidad del sistema cifrada por BitLocker en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuya unidad quiere restaurar el acceso.
3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione la sección **BitLocker**.
5. Compruebe el ID de clave de recuperación. El ID proporcionado por el usuario debe coincidir con el ID que se muestra en la configuración del equipo.

   Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

6. Haga clic en **Recibir clave**.

Como resultado, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá transferirse al usuario.

Una vez que se carga el sistema operativo, Kaspersky Endpoint Security solicita al usuario que cambie la contraseña o el código PIN. Después de establecer una nueva contraseña o código PIN, BitLocker creará una nueva clave de recuperación y la enviará a Kaspersky Security Center. Como resultado, se actualizarán la clave de recuperación y el archivo clave de recuperación. Si el usuario no ha cambiado la contraseña, puede usar la antigua clave de recuperación la próxima vez que se cargue el sistema operativo.

Los equipos que cuenten con el sistema operativo Windows 7 no permiten cambiar la contraseña o el código PIN. Una vez que se introduce la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no le solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, no es posible establecer un nuevo código PIN o contraseña. Este problema proviene de las particularidades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.

Restauración del acceso a una unidad que no pertenece al sistema

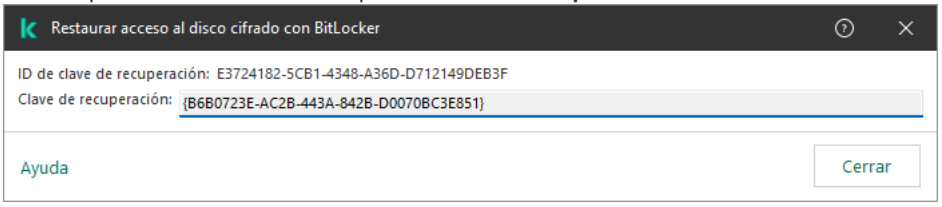
Para comenzar el procedimiento de recuperación, el usuario tiene que hacer clic en el enlace **Forgot your password** en la ventana que proporciona acceso a la unidad. Después de obtener acceso a la unidad cifrada, el usuario puede activar el desbloqueo automático de la unidad durante la autenticación de Windows en la configuración de BitLocker.

Cómo ver la clave de recuperación para una unidad que no pertenece al sistema cifrada por BitLocker en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Avanzado → Protección y cifrado de datos → Dispositivos cifrados**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que desea crear un archivo de clave de acceso. Luego, en el menú contextual del dispositivo, haga clic en **Obtener acceso para el dispositivo Kaspersky Endpoint Security**.
4. Solicite al usuario el ID de la clave de recuperación indicado en la ventana de introducción de la contraseña de BitLocker y compárelo con el ID del campo **ID de clave de recuperación**.

   Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

5. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.



Restauración del acceso a una unidad cifrada por BitLocker

Cómo ver la clave de recuperación para una unidad cifrada por BitLocker que no pertenece al sistema en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Operaciones → Protección y cifrado de datos → Dispositivos cifrados**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuya unidad quiere restaurar el acceso.
3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.

   Se iniciará el Asistente para otorgar acceso a un dispositivo.
4. Siga las instrucciones del Asistente para otorgar acceso a un dispositivo:

   a. Seleccione el complemento **Kaspersky Endpoint Security para Windows**

   b. Compruebe el ID de clave de recuperación. El ID proporcionado por el usuario debe coincidir con el ID que se muestra en la configuración del equipo.

   > Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

   c. Haga clic en **Recibir clave**.

Como resultado, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá transferirse al usuario.

Pausar la protección de BitLocker para actualizar el software

Hay una serie de consideraciones especiales para actualizar el sistema operativo, instalar paquetes de actualización para el sistema operativo o actualizar otro software con la protección BitLocker activada. La instalación de actualizaciones puede requerir el reinicio del equipo varias veces. Después de cada reinicio, el usuario debe completar la autenticación de BitLocker. Para asegurarse de que las actualizaciones se instalen correctamente, puede desactivar temporalmente la autenticación de BitLocker. En este caso, el disco permanece cifrado y el usuario tiene acceso a los datos después de iniciar sesión en el sistema. Para administrar la autenticación de BitLocker, puede usar la tarea de *Administración de la protección de BitLocker*. Puede usar esta tarea para especificar el número de reinicios del equipo que no requieren la autenticación de BitLocker. De esta forma, una vez instaladas las actualizaciones y después de que finalice la tarea de *Administración de la protección de BitLocker*, la autenticación de BitLocker se activa automáticamente. Puede activar la autenticación de BitLocker en cualquier momento.

Cómo pausar la protección de BitLocker con la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Administración de la protección de BitLocker**.

Paso 2. Administración de la protección de BitLocker

Configure la autenticación de BitLocker. Para pausar la protección de BitLocker, seleccione **Permitir temporalmente omitir la autenticación de BitLocker** e introduzca el número de reinicios sin autenticación de BitLocker (de 1 a 15 veces). Si es necesario, introduzca una fecha y hora de caducidad para la tarea. A la hora especificada, la tarea se desactiva automáticamente y el usuario debe completar la autenticación de BitLocker cuando se reinicia el equipo.

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Definir el nombre de la tarea

Introduzca el nombre de la tarea, por ejemplo, *Actualización a Windows 10*.

Paso 5. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Cómo pausar la protección de BitLocker mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Administración de la protección de BitLocker**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Actualización a Windows 10*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

Paso 2. Administración de la protección de BitLocker

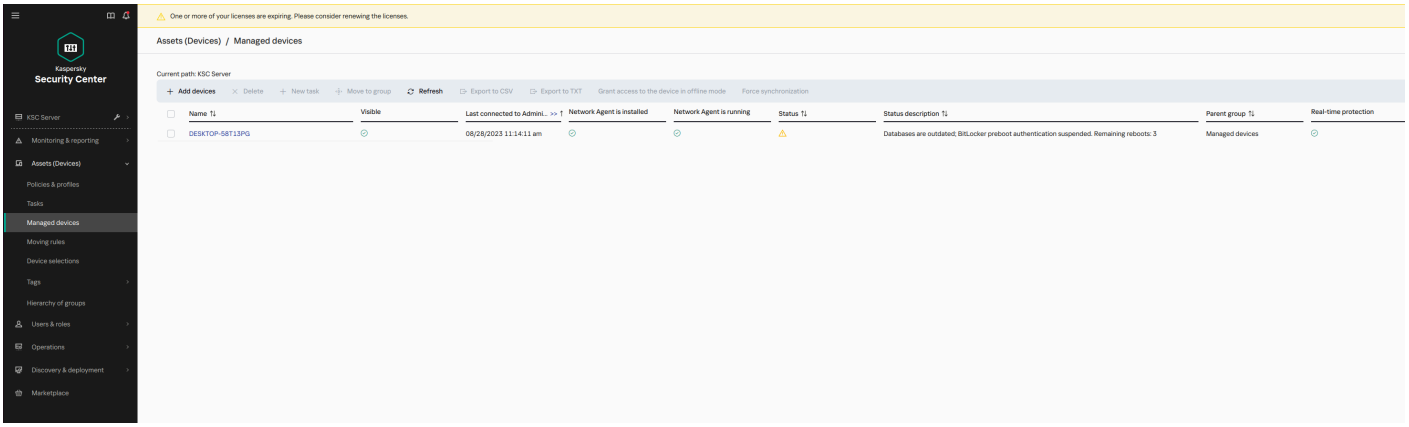
Configure la autenticación de BitLocker. Para pausar la protección de BitLocker, seleccione **Permitir temporalmente omitir la autenticación de BitLocker** e introduzca el número de reinicios sin autenticación de BitLocker (de 1 a 15 veces). Si es necesario, introduzca una fecha y hora de caducidad para la tarea. A la hora especificada, la tarea se desactiva automáticamente y el usuario debe completar la autenticación de BitLocker cuando se reinicia el equipo.

Paso 3. Conclusión de la creación de tareas

Finalice el asistente. La nueva tarea aparecerá en la lista de tareas.

Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**.

Como resultado, cuando la tarea se está ejecutando, después del próximo reinicio del equipo, BitLocker no solicita la autenticación al usuario. Después de cada reinicio del equipo sin la autenticación de BitLocker, Kaspersky Endpoint Security genera un evento correspondiente y registra el número de reinicios restantes. Luego, Kaspersky Endpoint Security envía el evento a Kaspersky Security Center para que lo supervise el administrador. También puede ver el número de reinicios restantes en la carpeta **Dispositivos administrados** de la consola de Kaspersky Security Center en la descripción del estado del dispositivo.



La lista de dispositivos administrados

Cuando se alcanza el número especificado de reinicios o la hora de caducidad de la tarea, la autenticación de BitLocker se activa automáticamente. Para obtener acceso a los datos, el usuario debe completar la autenticación de BitLocker.

En equipos que ejecutan Windows 7, BitLocker no puede contar los reinicios de equipos. Kaspersky Endpoint Security gestiona el recuento de reinicios en equipos con Windows 7. Por lo tanto, para activar automáticamente la autenticación de BitLocker después de cada reinicio, se debe iniciar Kaspersky Endpoint Security.

Para activar la autenticación de BitLocker antes de tiempo, abra las propiedades de la tarea de *Administración de la protección de BitLocker* y seleccione **Solicitar autenticación en cada oportunidad previa al arranque**.

Cifrado de archivos en unidades locales del equipo

El cifrado de archivos no es compatible con equipos basados en Arm.

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El cifrado de archivo tiene las siguientes características especiales:

- Kaspersky Endpoint Security cifra y descifra los archivos de las carpetas predeterminadas solo para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifra ni descifra los archivos de las carpetas predeterminadas de los perfiles de usuario en itinerancia, de los perfiles de usuario obligatorio, de los perfiles de usuario temporal ni de las carpetas redirigidas.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo o aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas se encuentran en la lista de exclusiones del cifrado:
  - %WINDIR%;
  - %PROGRAMFILES% y %PROGRAMFILES(X86)%;
  - Archivos de registro de Windows.

  No se puede ver ni modificar la lista de exclusiones del cifrado. Los archivos y las carpetas de la lista de exclusiones del cifrado se pueden añadir a la lista de cifrado, pero no se cifrarán durante el cifrado de archivos.

Cifrado de los archivos de las unidades del equipo local

Kaspersky Endpoint Security no cifra los archivos que se encuentran en el almacenamiento en la nube de OneDrive o en otras carpetas que tienen OneDrive como nombre. Kaspersky Endpoint Security también bloquea la copia de archivos cifrados a carpetas de OneDrive si esos archivos no se añaden a la regla de descifrado.

Para cifrar los archivos de las unidades de disco locales:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de archivos**.
4. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.
5. En la pestaña **Cifrado**, haga clic en el botón **Añadir** y en la lista desplegable seleccione uno de los elementos siguientes:
   a. Seleccione el elemento **Carpetas predeterminadas** para añadir archivos desde carpetas de perfiles de usuario locales sugeridos por expertos de Kaspersky a una regla de cifrado.
      - **Documentos**. Los archivos en la carpeta estándar *Documentos* del sistema operativo y sus subcarpetas.
      - **Favoritos**. Los archivos en la carpeta estándar *Favoritos* del sistema operativo y sus subcarpetas.
      - **Escritorio**. Los archivos en la carpeta estándar *Escritorio* del sistema operativo y sus subcarpetas.
      - **Archivos temporales**. Archivos temporales relacionados con el funcionamiento de aplicaciones instaladas en el equipo. Por ejemplo, las aplicaciones de Microsoft Office crean archivos temporales que contienen copias de seguridad de documentos.

        No se recomienda cifrar os archivos temporales, ya que esto puede provocar la pérdida de datos. Por ejemplo, Microsoft Word crea archivos temporales al procesar un documento. Si se cifran los archivos temporales, pero no el archivo original, el usuario puede recibir un error de *Acceso denegado* al intentar guardar el documento. Además, Microsoft Word puede llegar a guardar el archivo, pero no se podrá abrir el documento la próxima vez que se intente hacerlo, lo cual quiere decir que se perderán los datos.

      - **Archivos de Outlook**. Archivos relacionados con el funcionamiento del cliente de correo Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de libretas de direcciones sin conexión (OAB) y archivos de libretas de direcciones personales (PAB).

   b. Seleccione el elemento **Carpeta personalizada** para añadir una ruta de la carpeta introducida manualmente a una regla de cifrado.

Al añadir una ruta de carpeta, cumpla las siguientes reglas:

- Use una variable de entorno (por ejemplo, `%FOLDER%\UserFolder\`). Puede usar una variable de entorno solo una vez y solo al comienzo de la ruta.
- No use rutas relativas.
- No utilice los caracteres `*` y `?`.
- No utilice rutas UNC.
- Utilice `;` o `,` como carácter de separación.

c. Seleccione el elemento **Archivos por extensión** para añadir extensiones de archivo individuales a una regla de cifrado. Kaspersky Endpoint Security cifra los archivos de todas las unidades de disco locales del equipo que tienen las extensiones especificadas.

d. Seleccione el elemento **Archivos por grupos de extensiones** para añadir grupos de extensiones de archivo a una regla de cifrado (por ejemplo, *Documentos de Microsoft Office*). Kaspersky Endpoint Security cifra archivos cuyas extensiones se incluyen en los grupos de extensiones de todas las unidades de disco locales del equipo.

6. Guarde los cambios.

Una vez que se aplica la directiva, Kaspersky Endpoint Security cifra los archivos incluidos en la regla de cifrado que no se incluyen en la regla de descifrado.

El cifrado de archivo tiene las siguientes características especiales:

- Si se añade el mismo archivo a una regla de cifrado y a una regla de descifrado, Kaspersky Endpoint Security realiza las siguientes acciones:
  - Si el archivo no está cifrado, Kaspersky Endpoint Security no cifra este archivo.
  - Si el archivo está cifrado, Kaspersky Endpoint Security descifra este archivo.
- Kaspersky Endpoint Security continúa cifrando archivos nuevos si estos cumplen los criterios de la regla de cifrado. Por ejemplo, cuando cambia las propiedades de un archivo sin cifrar (ruta o extensión), el archivo cumple los criterios de la regla de cifrado. Kaspersky Endpoint Security cifra este archivo.
- Cuando el usuario crea un nuevo archivo cuyas propiedades cumplen los criterios de la regla de cifrado, Kaspersky Endpoint Security cifra el archivo en cuanto se abre.
- Kaspersky Endpoint Security pospone el cifrado de archivos abiertos hasta que se cierren.
- Si mueve un archivo cifrado a otra carpeta de la unidad local, el archivo se mantiene cifrado, sin considerar si la carpeta se incluye o no en la regla de cifrado.
- Si descifra un archivo y lo copia a otra carpeta local que no está incluida en la regla de descifrado, se puede cifrar una copia del archivo. Para evitar que el archivo copiado se cifre, cree una regla de descifrado para la carpeta de destino.

Creación de reglas de acceso a archivos cifrados para aplicaciones

De forma predeterminada, todas las aplicaciones funcionan con archivos cifrados en un estado descifrado. Si utiliza determinadas aplicaciones con frecuencia (por ejemplo, navegadores o editores de texto), puede crear reglas de acceso a archivos cifrados para proteger la información.

Recomendamos crear una regla de acceso a archivos cifrados para los navegadores Microsoft Internet Explorer y Microsoft Edge. Debido a cómo funcionan estos navegadores, si carga un archivo cifrado en un sitio web (por ejemplo, para almacenamiento en la nube), el archivo se descifra automáticamente. Esto puede provocar una filtración de datos. No es posible cargar un archivo cifrado con estos navegadores. Recomendamos configurar la regla **Conceder acceso a los archivos cifrados solo como texto cifrado**. No es necesario crear una regla para otros navegadores (como Google Chrome).

Para crear reglas de acceso a archivos cifrados para aplicaciones:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de archivos**.
4. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.

   Las reglas de acceso solo se aplican cuando se está en el modo **De acuerdo con las reglas**. Tras aplicar reglas de acceso en el modo **De acuerdo con las reglas**, si cambia al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de acceso. Todas las aplicaciones tendrán acceso a todos los archivos cifrados.

5. En la parte derecha de la ventana, seleccione la pestaña **Reglas para aplicaciones**.
6. Si desea seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.
   a. Especifique los filtros para restringir la lista de aplicaciones de la tabla. Para ello, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período añadido**, así como todas las casillas de verificación del bloque **Grupo**.
   b. Haga clic en **Actualizar**.
   c. La tabla muestra las aplicaciones que cumplen los filtros aplicados.
   d. En la columna **Aplicación**, active las casillas de las aplicaciones para las que desea crear reglas de acceso a archivos cifrados.

e. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a los archivos cifrados.

f. En la lista desplegable **Acciones para aplicaciones seleccionadas antes**, seleccione la acción que Kaspersky Endpoint Security llevará a cabo en las reglas de acceso a archivos cifrados que se han formado previamente para dichas aplicaciones.

La información sobre las reglas de acceso a archivos cifrados para aplicaciones se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

7. Si desea seleccionar manualmente las aplicaciones, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

a. En el campo de entrada, introduzca el nombre o la lista de nombres de archivos de aplicaciones ejecutables, incluidas sus extensiones.

También puede añadir nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center haciendo clic en el botón **Añadir de la lista de Kaspersky Security Center**.

b. Si es preciso, en el campo **Descripción**, introduzca una descripción de la lista de aplicaciones.

c. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a los archivos cifrados.

La información sobre las reglas de acceso a archivos cifrados para aplicaciones se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

8. Guarde los cambios.

Cifrar archivos creados o modificados por aplicaciones específicas

Puede crear una regla según la cual Kaspersky Endpoint Security cifrará todos los archivos creados o modificados por las aplicaciones especificadas en la regla.

> Los archivos que fueron creados o modificados por las aplicaciones especificadas antes de que se aplicara la regla de cifrado no se cifrarán.

Para configurar el cifrado de archivos que se crean o modifican por aplicaciones específicas:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de archivos**.

4. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.

   Las reglas de cifrado se aplican únicamente en el modo **De acuerdo con las reglas**. Después de aplicar reglas de cifrado en el modo **De acuerdo con las reglas**, si cambia al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de cifrado. Los archivos que se cifraron con anterioridad permanecerán cifrados.

5. En la parte derecha de la ventana, seleccione la pestaña **Reglas para aplicaciones**.

6. Si desea seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.

   a. Especifique los filtros para restringir la lista de aplicaciones de la tabla. Para ello, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período añadido**, así como todas las casillas de verificación del bloque **Grupo**.

   b. Haga clic en **Actualizar**.

      La tabla muestra las aplicaciones que cumplen los filtros aplicados.

   c. En la columna **Aplicación**, seleccione las casillas situadas junto a las aplicaciones cuyos archivos creados quiere cifrar.

   d. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

   e. En la lista desplegable **Acciones para aplicaciones seleccionadas antes**, seleccione la acción que Kaspersky Endpoint Security llevará a cabo en las reglas de cifrado de archivos que se han creado previamente para las aplicaciones mencionadas.

   La información sobre la regla de cifrado para archivos creados o modificados por aplicaciones seleccionadas se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

7. Si desea seleccionar manualmente las aplicaciones, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

   a. En el campo de entrada, introduzca el nombre o la lista de nombres de archivos de aplicaciones ejecutables, incluidas sus extensiones.

      También puede añadir nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center haciendo clic en el botón **Añadir de la lista de Kaspersky Security Center**.

   b. Si es preciso, en el campo **Descripción**, introduzca una descripción de la lista de aplicaciones.

   c. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

   La información sobre la regla de cifrado para archivos creados o modificados por aplicaciones seleccionadas se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

8. Guarde los cambios.

Generación de una regla de descifrado

Para generar una regla de descifrado:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de archivos**.
4. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.
5. En la pestaña **Descifrado**, haga clic en el botón **Añadir** y en la lista desplegable seleccione uno de los elementos siguientes:
   a. Seleccione el elemento **Carpetas predeterminadas** para añadir archivos desde carpetas de perfiles de usuario locales sugeridos por expertos de Kaspersky a una regla de descifrado.
   b. Seleccione el elemento **Carpeta personalizada** para añadir una ruta de la carpeta introducida manualmente a una regla de descifrado.
   c. Seleccione el elemento **Archivos por extensión** para añadir extensiones de archivo individuales a una regla de descifrado. Kaspersky Endpoint Security no cifra los archivos de todas las unidades de disco locales del equipo que tienen las extensiones especificadas.
   d. Seleccione el elemento **Archivos por grupos de extensiones** para añadir grupos de extensiones de archivo a una regla de descifrado (por ejemplo, *Documentos de Microsoft Office*). Kaspersky Endpoint Security no cifra archivos cuyas extensiones se incluyen en los grupos de extensiones de todas las unidades de disco locales del equipo.
6. Guarde los cambios.

Si un mismo archivo se ha añadido a la regla de cifrado y a la de descifrado, Kaspersky Endpoint Security no cifra este archivo si está descifrado y descifra el archivo si está cifrado.

Descifrado de archivos de las unidades del equipo local

Para descifrar los archivos de las unidades de disco locales:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de archivos**.
4. En la parte derecha de la ventana, seleccione la pestaña **Cifrado**.

5. Elimine los archivos y las carpetas que desea descifrar de la lista de cifrado. Para ello, seleccione los archivos y el elemento **Eliminar regla y descifrar archivos** del menú contextual del botón **Eliminar**.

   Los archivos y las carpetas que se eliminan de la lista de cifrado se añaden automáticamente a la lista de descifrado.

6. Cree una lista de descifrado de archivos.

7. Guarde los cambios.

En cuanto se aplique la directiva, Kaspersky Endpoint Security descifra los archivos cifrados que se añaden a la lista de descifrado.

Kaspersky Endpoint Security descifra los archivos cifrados si sus parámetros (ruta del archivo/nombre del archivo/extensión del archivo) cambian para coincidir con los parámetros de los objetos añadidos a la lista de descifrado.

Kaspersky Endpoint Security pospone el descifrado de archivos abiertos hasta que se cierren.

Creación de paquetes cifrados

Para proteger sus datos cuando envía archivos a usuarios fuera de la red corporativa, puede usar paquetes cifrados. Los paquetes cifrados pueden resultar convenientes para transferir archivos grandes en unidades extraíbles, ya que los clientes de correo electrónico tienen restricciones de tamaño de archivo.

Antes de crear paquetes cifrados, Kaspersky Endpoint Security le pedirá al usuario una contraseña. Para proteger los datos de manera fiable, puede activar la evaluación de seguridad de la contraseña y especificar los requisitos de seguridad de la contraseña. Esto evitará que los usuarios usen contraseñas cortas y sencillas como, por ejemplo, `1234`.

Cómo activar la evaluación de seguridad de la contraseña al crear archivos comprimidos cifrados en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Cifrado de datos → Configuración común de cifrado**.

4. En el bloque **Configuración de contraseña**, haga clic en el botón **Configuración**.

5. Se abre una ventana; en ella, seleccione la pestaña **Paquetes cifrados**.

6. Configure los ajustes de la complejidad de la contraseña al crear paquetes cifrados.

Cómo activar la evaluación de seguridad de la contraseña al crear archivos comprimidos cifrados en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.

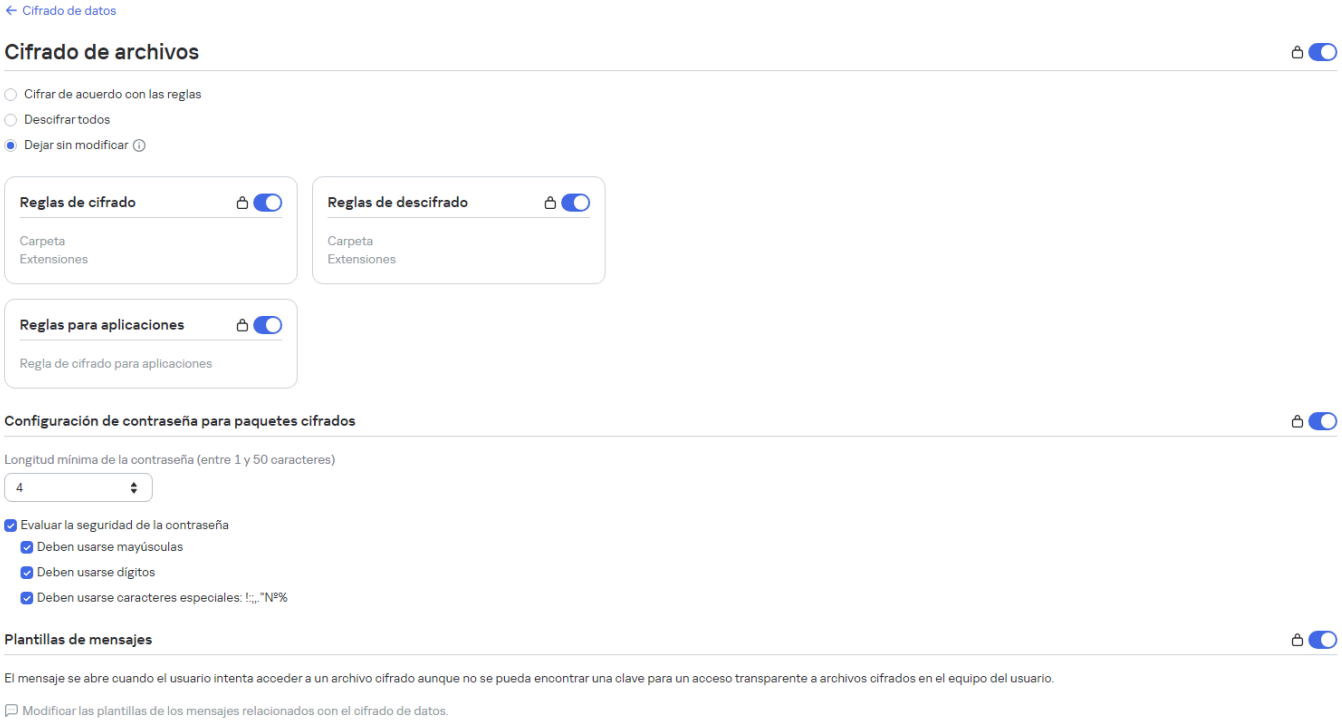
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Cifrado de datos → Cifrado de archivos**.

5. En el bloque **Configuración de contraseña para paquetes cifrados**, configure los criterios de seguridad de la contraseña necesarios para crear paquetes cifrados.



Configuración de cifrado de archivos

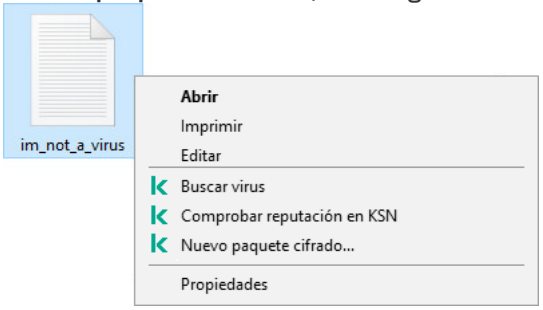
Puede crear paquetes cifrados en equipos con Kaspersky Endpoint Security instalado con Cifrado de archivos disponible.

Cuando se añade un archivo al paquete cifrado cuyo contenido reside en el almacenamiento en nube de OneDrive, Kaspersky Endpoint Security descarga el contenido del archivo y realiza el cifrado.

Para crear un paquete cifrado:

1. En cualquier gestor de archivos, seleccione los archivo o carpetas que desee añadir al paquete cifrado. Haga clic con el botón derecho del ratón para abrir su menú contextual.

2. En el menú contextual, seleccione **Nuevo paquete cifrado** (vea la figura a continuación).



Creación de un paquete cifrado

3. En la ventana que se abre, especifique la contraseña y confírmela.

   La contraseña debe cumplir los criterios de complejidad especificados en la directiva.

4. Haga clic en **Crear**.

   Se inicia el proceso de creación del paquete cifrado. Kaspersky Endpoint Security no comprime los archivos cuando crea un paquete cifrado. Cuando el proceso termina, se crea un paquete cifrado autoextraíble y protegido con contraseña (un archivo ejecutable con la extensión .exe – ) en la carpeta de destino seleccionada.

Para acceder a los archivos de un paquete cifrado, haga doble clic en él para iniciar el Asistente de descompresión y, a continuación, introduzca la contraseña. Si ha olvidado o ha perdido su contraseña, no es posible recuperarla y acceder a los archivos en el paquete cifrado. Puede recrear el paquete cifrado.

Restauración del acceso a los archivos cifrados

Cuando los archivos se cifran, Kaspersky Endpoint Security recibe una clave de cifrado para acceder directamente a los archivos cifrados. Al utilizar esta clave de cifrado, un usuario que trabaje con una cuenta de Windows que se encontrara activa durante el cifrado de archivos podrá acceder a dichos archivos directamente. Los usuarios que trabajen con cuentas de Windows que no se encontraran activas durante el cifrado de archivos deberán conectarse a Kaspersky Security Center para acceder a los archivos cifrados.

Es posible que los archivos cifrados no sean accesibles en las siguientes circunstancias:

- El equipo del usuario almacena las claves de cifrado, pero no existe conexión con Kaspersky Security Center para administrar las claves. En este caso, el usuario debe solicitar acceso a los archivos cifrados al administrador de la red de área local.

  Si no existe acceso a Kaspersky Security Center, debe hacer lo siguiente:

  - solicitar una clave de acceso para acceder a archivos cifrados en discos duros del equipo;
  - para acceder a archivos cifrados almacenados en unidades extraíbles, deberá solicitar claves de acceso separadas para los archivos cifrados en cada unidad extraíble.

- Los componentes de cifrado se eliminan desde el equipo del usuario. En este evento, el usuario puede abrir archivos cifrados en unidades locales y extraíbles, pero el contenido de esos archivos aparecerá cifrado.

  El usuario puede trabajar con archivos cifrados en las siguientes circunstancias:

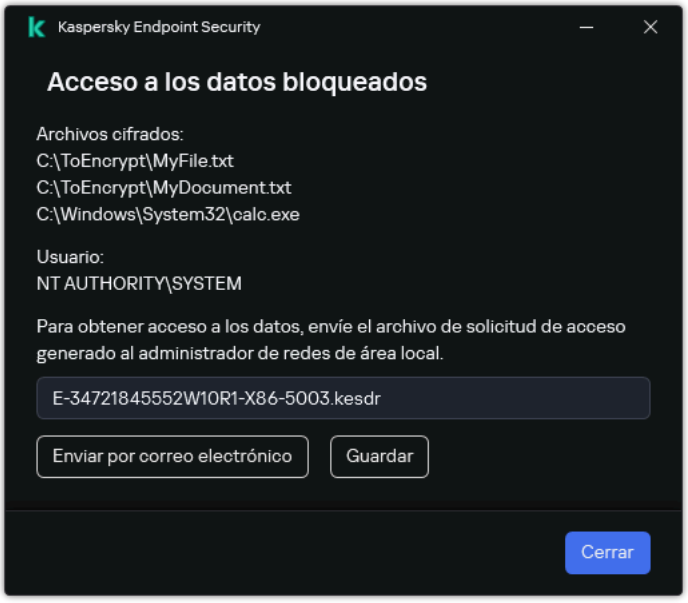
  - Los archivos se encuentran dentro de paquetes cifrados creados en un equipo con Kaspersky Endpoint Security.
  - Los archivos se almacenan en unidades extraíbles en las cuales se permitió el modo portátil.

Para obtener acceso a los archivos cifrados, el usuario tiene que comenzar el procedimiento de recuperación (solicitud-respuesta).

La recuperación del acceso a los archivos cifrados consta de los siguientes pasos:

1. El usuario envía un archivo de solicitud de acceso al administrador (vea la imagen más abajo).
2. El administrador añade el archivo de solicitud de acceso a Kaspersky Security Center, crea un archivo clave de acceso y lo envía al usuario.

3. El usuario añade el archivo clave de acceso a Kaspersky Endpoint Security y obtiene acceso a los archivos.



Restauración del acceso a los archivos cifrados

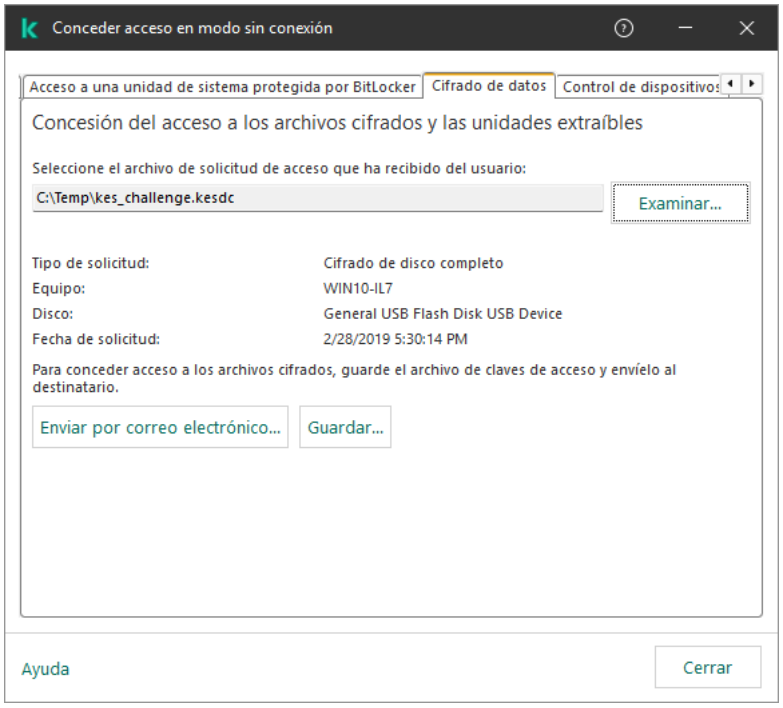
Para comenzar el procedimiento de recuperación, el usuario tiene que intentar acceder a un archivo. Como resultado, Kaspersky Endpoint Security creará un archivo de solicitud de acceso (un archivo con la extensión KESDC), que el usuario tiene que enviar al administrador, por ejemplo, por correo electrónico.

Kaspersky Endpoint Security genera un archivo de solicitud de acceso para acceder a todos los archivos cifrados almacenados en la unidad del equipo (unidad local o extraíble).

Cómo obtener un archivo clave de acceso a datos cifrados en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos**.
3. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
4. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
5. Se abre una ventana; en ella, seleccione la pestaña **Cifrado de datos**.
6. En la pestaña **Cifrado de datos**, haga clic en el botón **Examinar**.
7. En la ventana para seleccionar un archivo de solicitud de acceso, especifique la ruta al archivo recibido del usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.



Conceder acceso en modo sin conexión

Cómo obtener un archivo clave de acceso a datos cifrados en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuyos datos quiere restaurar el acceso.
3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.
4. Seleccione **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión KESDC).

   Web Console mostrará información sobre la solicitud. Esto incluirá el nombre del equipo en el que el usuario solicita acceso al archivo.
6. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión KESDR).

Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

Tras recibir el archivo clave de acceso a datos cifrados, el usuario tiene que ejecutar el archivo haciendo doble clic en él. Como resultado, Kaspersky Endpoint Security concederá acceso a todos los archivos cifrados almacenados en la unidad. Para acceder a archivos cifrados almacenados en otras unidades, obtenga un archivo clave de acceso independiente para cada unidad.

Restauración del acceso a los datos cifrados después del error del sistema operativo

Puede restaurar el acceso a los datos después del error del sistema operativo solo con el cifrado de archivos (CA). No puede restaurar el acceso a los datos si se utiliza cifrado de disco completo (FDE).

Para restaurar el acceso a los datos cifrados después del error del sistema operativo:

1. Vuelva a instalar el sistema operativo sin formatear el disco duro.
2. Instale Kaspersky Endpoint Security.
3. Establezca una conexión entre el equipo y el Servidor de administración de Kaspersky Security Center que controló el equipo cuando se cifraron los datos.

   Se concederá el acceso a los datos cifrados bajo las mismas condiciones que se aplicaban antes del error del sistema operativo.

Modificación de plantillas de mensajes de acceso a archivos cifrados

Para modificar las plantillas de los mensajes de acceso a archivos cifrados:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos** → **Configuración común de cifrado**.
4. En el bloque **Plantillas**, haga clic en el botón **Plantillas**.
5. En la ventana que se abre, haga lo siguiente:

   - Si desea editar la plantilla del mensaje del usuario, seleccione la pestaña **Mensaje del usuario**. La siguiente ventana se abre cuando el usuario intenta acceder a un archivo cifrado y no existe ninguna clave para acceder a archivos cifrados disponible en el equipo (consulte la figura que aparece abajo). Al hacer clic en el botón **Enviar por correo electrónico**, se crea un mensaje de usuario de forma automática. Este mensaje se envía al administrador de la red de área local corporativa junto con el archivo de solicitud de acceso a archivos cifrados.

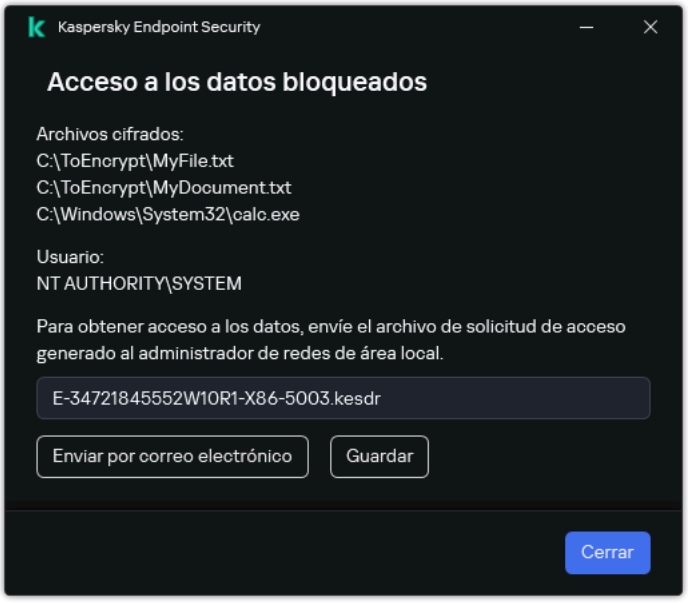
   - Si desea editar la plantilla del mensaje del administrador, seleccione la pestaña **Mensaje del administrador**. El usuario recibe este mensaje después de que se conceda el acceso a los archivos cifrados.

6. Modifique las plantillas de mensajes.

   Para añadir una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y elija la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto predeterminado de la plantilla utilizando el botón **Predeterminado**.

7. Guarde los cambios.



Restauración del acceso a los archivos cifrados

Cifrado de unidades extraíbles

El cifrado de unidades extraíbles no se admite en equipos basados en Arm.

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si una unidad extraíble con un sistema de archivos no compatible está conectada al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Para proteger los datos de las unidades extraíbles, puede usar los siguientes tipos de cifrado:

- Full Disk Encryption (FDE).

  Cifrado de toda la unidad extraíble, incluido el sistema de archivos.

  No se puede acceder a datos cifrados fuera de la red corporativa. También es imposible acceder a datos cifrados dentro de la red corporativa si el equipo no está conectado a Kaspersky Security Center (p. ej., en un equipo "invitado").

- File Level Encryption (FLE).

  Cifrado solo de los archivos en una unidad extraíble. El sistema de archivos permanece sin cambios.

El cifrado de archivos en unidades extraíbles proporciona la capacidad de acceder a datos fuera de la red corporativa mediante un modo especial llamado *modo portátil*.

Durante el cifrado, Kaspersky Endpoint Security crea una clave maestra. Kaspersky Endpoint Security guarda la clave maestra en los siguientes repositorios:

- Kaspersky Security Center.
- Equipo del usuario.

  La clave maestra está cifrada con la clave secreta del usuario.
- Unidad extraíble.

  La clave maestra está cifrada con la clave pública de Kaspersky Security Center.

Una vez que se completa el cifrado, se puede acceder a los datos de la unidad extraíble dentro de la red corporativa como si fuera una unidad extraíble convencional sin cifrar.

Acceso a datos cifrados

Cuando se conecta una unidad extraíble con datos cifrados, Kaspersky Endpoint Security realiza las siguientes acciones:

1. Comprueba si hay una clave maestra en el almacenamiento local en el equipo del usuario.

   Si se encuentra la clave maestra, el usuario obtiene acceso a los datos en la unidad extraíble.

   Si la clave maestra no se encuentra, Kaspersky Endpoint Security realiza las siguientes acciones:

   a. Envíe una solicitud a Kaspersky Security Center.

      Después de recibir la solicitud, Kaspersky Security Center envía una respuesta que contiene la clave maestra.

   b. Kaspersky Endpoint Security guarda la clave maestra en el almacenamiento local en el equipo del usuario para operaciones posteriores con la unidad extraíble cifrada.
2. Descifre los datos.

Características especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles tiene las siguientes características especiales:

- La directiva con la configuración preestablecida para el cifrado extraíble de la unidad se forma para un grupo específico de equipos administrados. Por lo tanto, el resultado de aplicar la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al que se conecta la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra archivos de solo lectura almacenados en las unidades extraíbles.

- Los siguientes tipos de dispositivo son compatibles como unidades extraíbles:
  - Medios de datos conectados por medio del puerto USB
  - Discos duros conectados por medio de los puertos USB y FireWire
  - Unidades SSD conectadas por medio de los puertos USB y FireWire

Iniciar el cifrado de unidades extraíbles

Puede usar una directiva para descifrar una unidad extraíble. Se genera una directiva con configuraciones definidas para el cifrado de unidades extraíbles para un grupo de administración específico. Por lo tanto, el resultado del descifrado de los datos en las unidades extraíbles depende del equipo con el cual la unidad extraíble está conectada.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si una unidad extraíble con un sistema de archivos no compatible está conectada al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Antes de cifrar archivos en una unidad extraíble, asegúrese de que esté formateada y de que no haya particiones ocultas (como una partición del sistema EFI). Si la unidad contiene particiones sin formatear u ocultas, el cifrado de archivos puede fallar y generar un error.

Para cifrar unidades extraíbles:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de unidades extraíbles**.
4. En la lista desplegable **Modo de cifrado**, indique qué hará Kaspersky Endpoint Security por defecto con las unidades extraíbles:
   - **Cifrar toda la unidad extraíble** (FDE). Kaspersky Endpoint Security cifrará el contenido de las unidades extraíbles sector por sector. Con ello, se cifrarán no solo los archivos de las unidades, sino también sus sistemas de archivos, incluidos los nombres de los archivos y las estructuras de carpetas.
   - **Cifrar todos los archivos** (FLE). Kaspersky Endpoint Security cifrará todos los archivos que se encuentren en las unidades extraíbles. La aplicación no cifra los sistemas de archivos de las unidades extraíbles, incluidos los nombres de los archivos y las estructuras de carpetas.
   - **Cifrar solo archivos nuevos** (FLE). De los archivos de las unidades extraíbles, Kaspersky Endpoint Security cifrará únicamente aquellos que se hayan añadido o modificado desde la última aplicación de la directiva de Kaspersky Security Center.

   Si una unidad extraíble ya está cifrada, Kaspersky Endpoint Security no la vuelve a cifrar.

5. Si desea que las unidades extraíbles se cifren en modo portátil, active la casilla de verificación **Modo portátil**.

   El *modo portátil* es un modo de cifrado de archivos (FLE) para unidades extraíbles que ofrece la capacidad de acceder a los datos fuera de una red corporativa. El modo portátil también le permite trabajar con datos cifrados en equipos que no tengan instalado Kaspersky Endpoint Security.

6. Para cifrar unidades extraíbles nuevas, recomendamos activar la casilla **Cifrar solo el espacio en disco utilizado**. Si la casilla de verificación queda desactivada, Kaspersky Endpoint Security cifrará todos los archivos que encuentre en una unidad, incluidos los remanentes de archivos eliminados o modificados.

7. Si desea configurar opciones de cifrado para unidades extraíbles específicas, puede definir reglas de cifrado.

8. Si desea cifrar las unidades extraíbles en modo sin conexión utilizando el cifrado de disco completo, active la casilla de verificación **Permitir el cifrado de las unidades extraíbles en modo sin conexión**.

   El *modo de cifrado sin conexión* hace referencia al cifrado de unidades extraíbles (FDE) cuando no hay conexión con Kaspersky Security Center. Durante el cifrado, Kaspersky Endpoint Security guarda la clave maestra únicamente en el equipo del usuario. La clave maestra se envía a Kaspersky Security Center cuando se realiza la siguiente sincronización.

   > Si el equipo en el que está almacenada la clave maestra sufre un desperfecto y los datos no se transfirieron a Kaspersky Security Center, será imposible acceder a la unidad extraíble.

   Si la casilla de verificación **Permitir el cifrado de las unidades extraíbles en modo sin conexión** no está activada y no hay conexión con Kaspersky Security Center, las unidades extraíbles no se podrán cifrar.

9. Guarde los cambios.

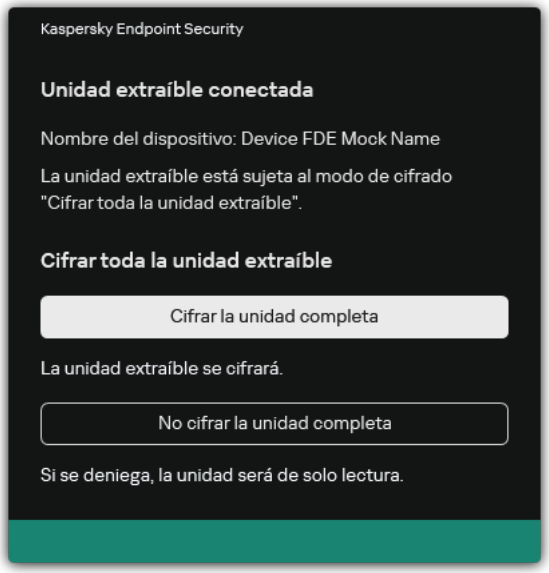
Cuando se conecte una unidad extraíble (o cuando ya haya una unidad extraíble conectada) después de que se aplique la directiva, Kaspersky Endpoint Security le solicitará al usuario que confirme la operación de cifrado (vea la imagen de más abajo).

La aplicación podrá realizar las siguientes acciones:

- Si el usuario confirma la solicitud de cifrado, Kaspersky Endpoint Security cifrará los datos.
- Si el usuario rechaza la solicitud de cifrado, Kaspersky Endpoint Security no modificará los datos y asignará acceso de solo lectura a la unidad extraíble.
- Si el usuario ignora la solicitud de cifrado, Kaspersky Endpoint Security no modificará los datos y asignará acceso de solo lectura a la unidad extraíble. La aplicación repetirá la solicitud la siguiente vez que se aplique una directiva o cuando se vuelva a conectar la misma unidad extraíble.

Si el usuario inicia la extracción segura de una unidad extraíble durante el cifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de cifrado de datos y permite la extracción de la unidad extraíble antes de que el proceso de cifrado haya finalizado. El proceso de cifrado se reanudará cuando el usuario conecte la unidad nuevamente al equipo.

Si el proceso de cifrado de una unidad extraíble falla, puede ver el informe **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Es posible que otra aplicación bloquee el acceso a los archivos. En tal caso, pruebe a desconectar la unidad extraíble del equipo y volver a conectarla.



Solicitud de cifrado para una unidad extraíble

Añadir una regla de cifrado para unidades extraíbles

Para añadir una regla de cifrado de unidades extraíbles:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de unidades extraíbles**.
4. Haga clic en el botón **Añadir** y, en la lista desplegable, seleccione uno de los siguientes elementos:
   - Si desea añadir reglas de cifrado para las unidades extraíbles que están en la lista de dispositivos de confianza del componente Control de dispositivos, seleccione **De una lista de dispositivos de confianza de esta directiva**.
   - Si desea añadir reglas de cifrado para las unidades extraíbles que están en la lista de Kaspersky Security Center, seleccione **De la lista de dispositivos de Kaspersky Security Center**.
5. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione la acción que Kaspersky Endpoint Security debe realizar en los archivos almacenados en las unidades extraíbles seleccionadas.

6. Seleccione la casilla de verificación **Modo portátil** si desea que Kaspersky Endpoint Security prepare las unidades extraíbles antes del cifrado, permitiendo, así, utilizar los archivos cifrados que contienen en modo portátil.

   El modo portátil le permite utilizar los archivos cifrados almacenados en las unidades extraíbles conectadas a los equipos que no disponen de la funcionalidad de cifrado.

7. Seleccione la casilla de verificación **Cifrar solo el espacio en disco utilizado** si desea que Kaspersky Endpoint Security cifre solo esos sectores del disco que están ocupados por archivos.

   Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable. La función **Cifrar solo el espacio en disco utilizado** se recomienda para las unidades nuevas que no se han utilizado anteriormente.

   Si un dispositivo se cifró anteriormente mediante la función **Cifrar solo el espacio en disco utilizado**, después de aplicar una directiva en el modo **Cifrar toda la unidad extraíble**, los sectores que aún no están ocupados por archivos no se cifrarán.

8. En la lista desplegable **Acciones para dispositivos que se seleccionaron antes**, seleccione la acción que realizará Kaspersky Endpoint Security conforme a las reglas de cifrado definidas previamente para las unidades extraíbles:

   - Si desea que la regla de cifrado creada anteriormente para la unidad extraíble no sufra modificaciones, seleccione **Omitir**.
   - Si desea que la regla de cifrado creada anteriormente para la unidad extraíble sea reemplazada por la regla nueva, seleccione **Actualizar**.

9. Guarde los cambios.

Las reglas de cifrado añadidas para las unidades extraíbles se aplicarán a las unidades extraíbles conectadas a cualquier equipo de la organización.

Exportación e importación de una lista de reglas de cifrado para unidades extraíbles

Puede exportar la lista de reglas de cifrado de unidades extraíbles a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de reglas para el mismo tipo de unidades extraíbles. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas o para migrar las reglas a un servidor diferente.

Cómo exportar e importar una lista de reglas de cifrado de unidades extraíbles en la Consola de administración (MMC)

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos → Cifrado de unidades extraíbles**.

5. En el bloque **Reglas de cifrado para los dispositivos seleccionados**, haga clic en el enlace **<N> reglas**.

   Esto abre una lista de reglas de cifrado para unidades extraíbles.

6. Para exportar la lista de reglas de cifrado para unidades extraíbles:

   a. Seleccione las reglas que quiera exportar.

   b. Haga clic en **Exportar**.

   c. Confirme que desea exportar solo las reglas seleccionadas o exportar la lista completa.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de reglas a un archivo XML en la carpeta de descargas predeterminada.

7. Para importar la lista de reglas:

   a. Haga clic en el enlace **Importar**.

      En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.

   b. Abra el archivo.

      Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

8. Guarde los cambios.

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de unidades extraíbles**.

4. Para exportar la lista de reglas de cifrado para unidades extraíbles:

   a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.

   b. Haga clic en el enlace **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.

5. Para importar una lista de reglas de cifrado para unidades extraíbles:

   a. Haga clic en el enlace **Importar**.

      En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.

b. Abra el archivo.

Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

6. Guarde los cambios.

Modo portátil para acceder a archivos cifrados de unidades extraíbles

El *modo portátil* es un modo de cifrado de archivos (FLE) para unidades extraíbles que ofrece la capacidad de acceder a los datos fuera de una red corporativa. El modo portátil también le permite trabajar con datos cifrados en equipos que no tengan instalado Kaspersky Endpoint Security.

Resulta útil usar el modo portátil en los siguientes casos:

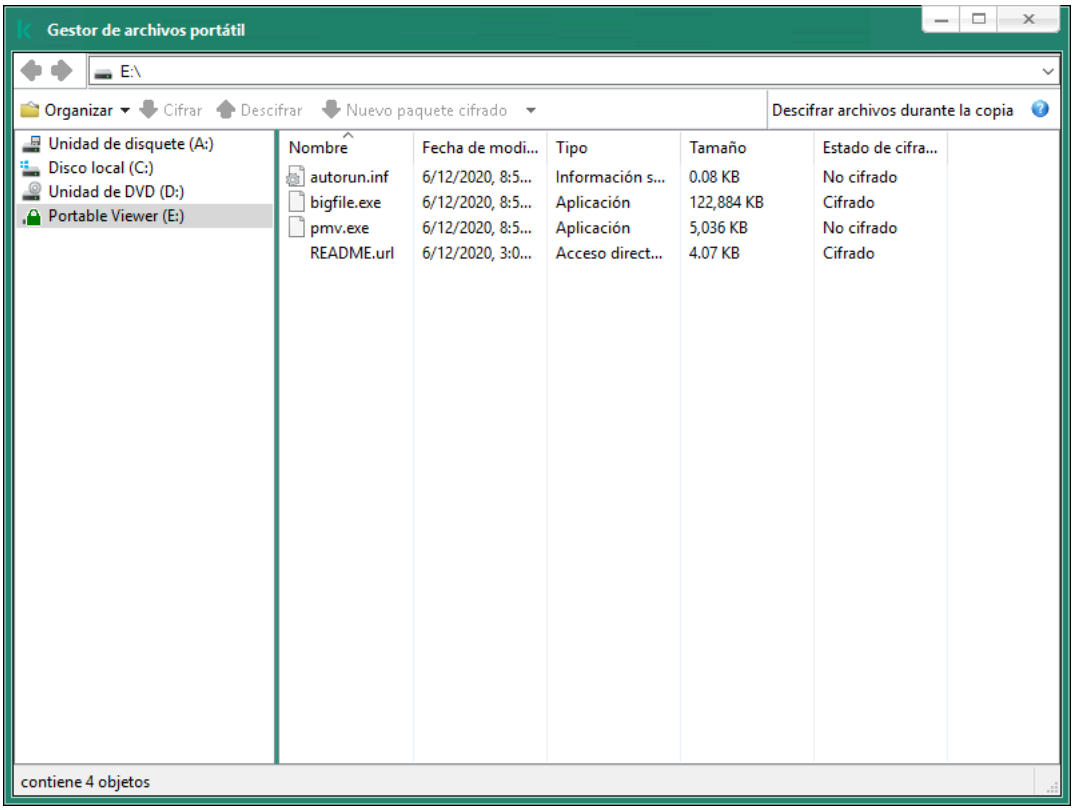
- No hay una conexión entre el equipo y el Servidor de administración de Kaspersky Security Center.
- La infraestructura ha cambiado con la modificación del Servidor de administración de Kaspersky Security Center.
- Kaspersky Endpoint Security no está instalado en el equipo.

Administrador de archivos portátil

Para trabajar en el modo portátil, Kaspersky Endpoint Security instala un módulo de cifrado especial denominado *Gestor de archivos portátil* en una unidad extraíble. El Gestor de archivos portátil proporciona una interfaz para trabajar con datos cifrados si Kaspersky Endpoint Security no está instalado en el equipo (vea la imagen más abajo). Si Kaspersky Endpoint Security está instalado en su equipo, puede trabajar con unidades extraíbles cifradas utilizando su gestor de archivos habitual (por ejemplo, Explorador).

El Gestor de archivos portátil almacena una clave para cifrar archivos en una unidad extraíble. La clave está cifrada con la contraseña del usuario. El usuario establece una contraseña antes de cifrar archivos en una unidad extraíble.

El Gestor de archivos portátil se inicia automáticamente cuando se conecta una unidad extraíble a un equipo en el que no está instalado Kaspersky Endpoint Security. Si el inicio automático de las aplicaciones está desactivado en el equipo, inicie manualmente el Gestor de archivos portátil. Para ello, ejecute el archivo con el nombre pmv.exe que se almacena en la unidad extraíble.



Administrador de archivos portátil

Compatibilidad con el modo portátil para trabajar con archivos cifrados

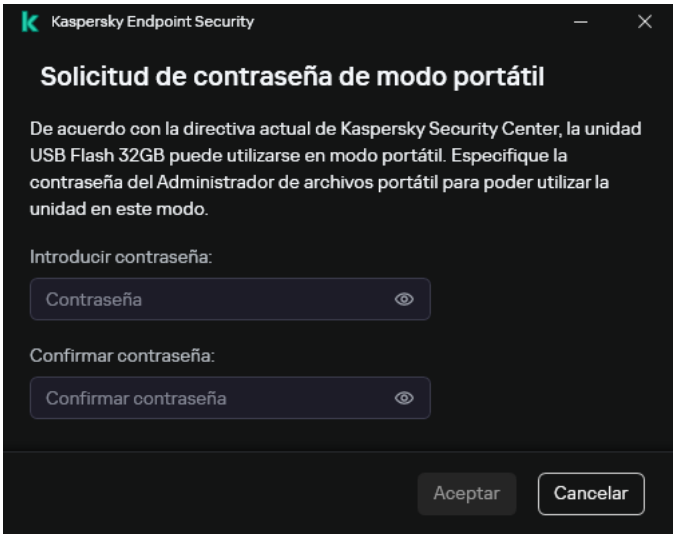
Cómo activar la compatibilidad con el modo portátil para trabajar con archivos cifrados en unidades extraíbles en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de unidades extraíbles**.
4. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione **Cifrar todos los archivos** o **Cifrar solo archivos nuevos**.

   El modo portátil solo está disponible con el Cifrado de archivos (FLE). No se puede activar la compatibilidad con el modo portátil para el Cifrado de disco completo (FDE).

5. Seleccione la casilla **Modo portátil**.
6. Si es necesario, añada reglas de cifrado para unidades extraíbles específicas.
7. Guarde los cambios.
8. Después de aplicar la directiva, conecte la unidad extraíble al equipo.
9. Confirme la operación de cifrado del disco extraíble.

Esto abre una ventana en la cual puede crear una contraseña para el Gestor de archivos portátil.



Solicitud de contraseña de modo portátil

10. Especifique una contraseña que cumpla con los requisitos de resistencia y confírmela.
11. Guarde los cambios.

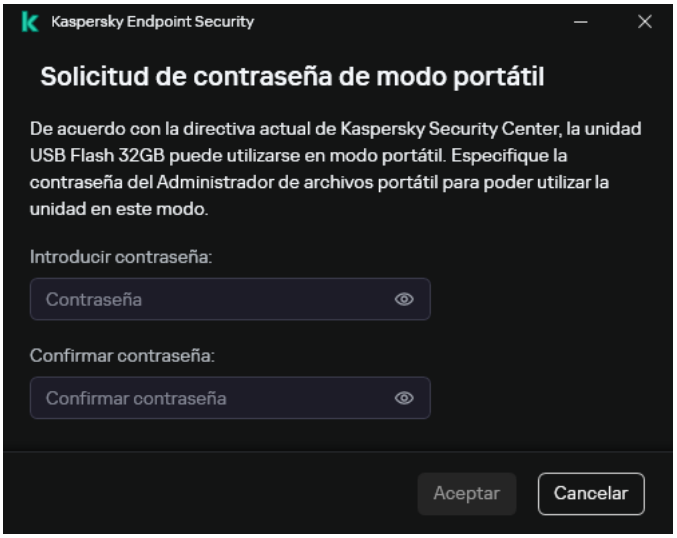
Cómo activar la compatibilidad con el modo portátil para trabajar con archivos cifrados en unidades extraíbles en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos** → **Cifrado de unidades extraíbles**.
5. En el bloque **Acción predeterminada**, seleccione **Cifrar todos los archivos** o **Cifrar solo archivos nuevos**.

   El modo portátil solo está disponible con el Cifrado de archivos (FLE). No se puede activar la compatibilidad con el modo portátil para el Cifrado de disco completo (FDE).
6. Seleccione la casilla **Modo portátil**.
7. Si es necesario, añada reglas de cifrado para unidades extraíbles específicas.
8. Guarde los cambios.
9. Después de aplicar la directiva, conecte la unidad extraíble al equipo.
10. Confirme la operación de cifrado del disco extraíble.

Esto abre una ventana en la cual puede crear una contraseña para el Gestor de archivos portátil.



Solicitud de contraseña de modo portátil

11. Especifique una contraseña que cumpla con los requisitos de resistencia y confírmela.
12. Guarde los cambios.

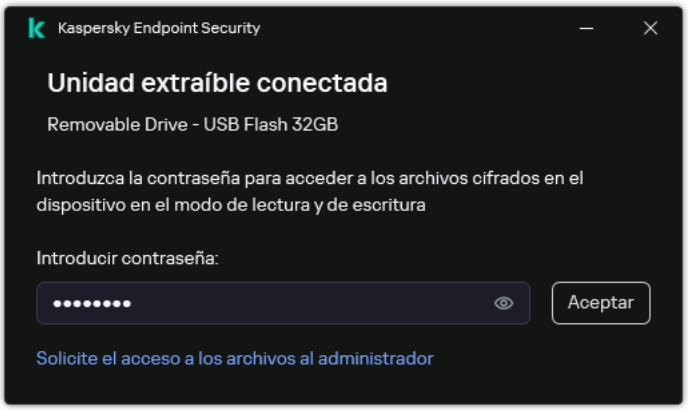
Kaspersky Endpoint Security cifrará los archivos en la unidad extraíble. El Gestor de archivos portátil utilizado para trabajar con archivos cifrados también se añadirá al disco extraíble. Si ya hay archivos cifrados en la unidad extraíble, Kaspersky Endpoint Security los volverá a cifrar con su propia clave. Esto permite al usuario acceder a todos los archivos de la unidad extraíble en el modo portátil.

Acceso a los archivos cifrados en una unidad extraíble

Después de cifrar los archivos en una unidad extraíble con compatibilidad con el modo portátil, están disponibles los siguientes métodos de acceso a los archivos:

- Si Kaspersky Endpoint Security no está instalado en el equipo, el Gestor de archivos portátil le solicitará que introduzca una contraseña. Deberá introducir la contraseña cada vez que reinicie el equipo o vuelva a conectar la unidad extraíble.
- Si el equipo se encuentra fuera de la red corporativa y Kaspersky Endpoint Security está instalado en el equipo, la aplicación le pedirá que introduzca la contraseña o le envíe al administrador una solicitud para acceder a los archivos. Después de obtener acceso a los archivos en una unidad extraíble, Kaspersky Endpoint Security guardará la clave secreta en el almacén de claves del equipo. Esto permitirá el acceso a los archivos en el futuro sin tener que introducir una contraseña ni pedírselo al administrador (vea la imagen más abajo).

- Si el equipo se encuentra dentro de la red corporativa y Kaspersky Endpoint Security está instalado en el equipo, obtendrá acceso al dispositivo sin tener que introducir una contraseña. Kaspersky Endpoint Security recibirá la clave secreta del Servidor de Administración de Kaspersky Security Center al que está conectado el equipo.



Acceso a los archivos cifrados en una unidad extraíble

Recuperar la contraseña para trabajar en el modo portátil

Si ha olvidado la contraseña para trabajar en el modo portátil, tiene que conectar la unidad extraíble a un equipo con Kaspersky Endpoint Security instalado dentro de la red corporativa. Obtendrá acceso a los archivos porque la clave secreta se guarda en el almacén de claves del equipo o en el Servidor de administración. Descifre y vuelva a cifrar archivos con una nueva contraseña.

Características del modo portátil al conectar una unidad extraíble a un equipo desde otra red

Si el equipo se encuentra fuera de la red corporativa y Kaspersky Endpoint Security está instalado en el equipo, puede acceder a los archivos de las siguientes maneras:

- **Acceso basado en contraseña**

  Después de introducir la contraseña, podrá ver, modificar y guardar archivos en la unidad extraíble (*acceso transparente*). Kaspersky Endpoint Security puede establecer un derecho de acceso de solo lectura para una unidad extraíble si los siguientes parámetros están definidos en la configuración de la directiva para el cifrado de unidades extraíbles:

  - La compatibilidad con el modo portátil está desactivado.
  - El modo **Cifrar todos los archivos** o **Cifrar solo archivos nuevos** está seleccionado.

  En todos los demás casos, obtendrá acceso completo a la unidad extraíble (permiso de lectura/escritura). Podrá añadir y eliminar archivos.

  Puede cambiar los permisos de acceso a la unidad extraíble incluso cuando esta está conectada al equipo. Si se cambian los permisos de acceso a la unidad extraíble, Kaspersky Endpoint Security bloqueará el acceso a los archivos y le pedirá la contraseña de nuevo.

  Después de introducir la contraseña, no puede aplicar la configuración de la directiva de cifrado para la unidad extraíble. En este caso, resulta imposible descifrar o volver a cifrar archivos en la unidad extraíble.

- **Solicitar al administrador acceso a los archivos**

Si ha olvidado la contraseña para trabajar en el modo portátil, solicite al administrador acceso a los archivos. Para acceder a los archivos, el usuario debe enviar al administrador un archivo de solicitud de acceso (un archivo con la extensión KESDC). El usuario puede enviar el archivo de solicitud de acceso por correo electrónico, por ejemplo. El administrador enviará un archivo de acceso a datos cifrados (un archivo con la extensión KESDR).

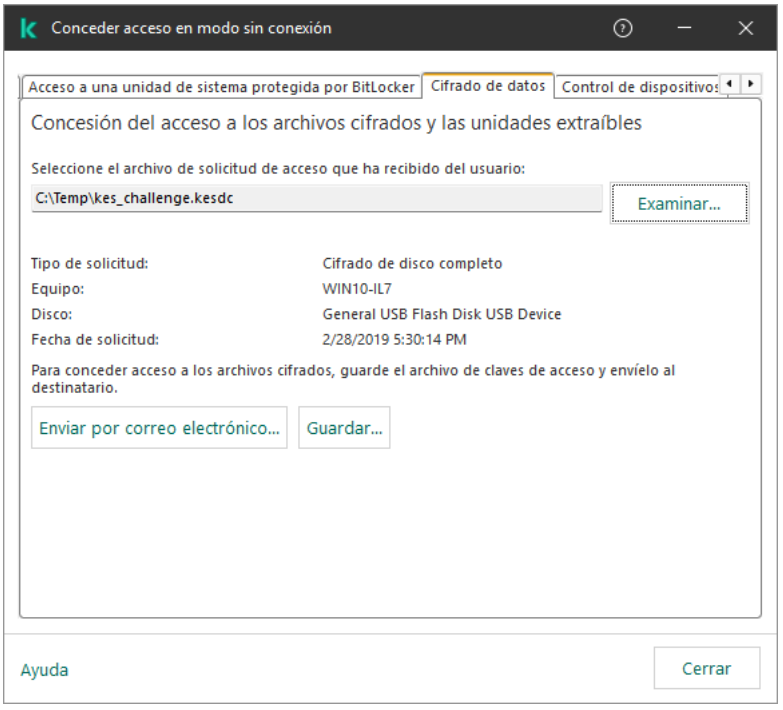
Después de completar el procedimiento de recuperación de contraseña de solicitud-respuesta, recibirá acceso transparente a los archivos de la unidad extraíble y acceso completo a la unidad extraíble (permiso de lectura/escritura).

Puede aplicar una directiva de cifrado de la unidad extraíble y descifrar archivos, por ejemplo. Después de recuperar la contraseña, o cuando se actualice la directiva, Kaspersky Endpoint Security le pedirá que confirme los cambios.

Cómo obtener un archivo de acceso a datos cifrados en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos**.
3. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
4. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
5. Se abre una ventana; en ella, seleccione la pestaña **Cifrado de datos**.
6. En la pestaña **Cifrado de datos**, haga clic en el botón **Examinar**.
7. En la ventana para seleccionar un archivo de solicitud de acceso, especifique la ruta al archivo recibido del usuario.

   Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.



Conceder acceso en modo sin conexión

Cómo obtener un archivo de acceso a datos cifrados en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuyos datos quiere restaurar el acceso.
3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.
4. Seleccione **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión KESDC).

   Web Console mostrará información sobre la solicitud. Esto incluirá el nombre del equipo en el que el usuario solicita acceso al archivo.
6. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión KESDR).

Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

Descifrado de unidades extraíbles

Puede usar una directiva para descifrar una unidad extraíble. Se genera una directiva con configuraciones definidas para el cifrado de unidades extraíbles para un grupo de administración específico. Por lo tanto, el resultado del descifrado de los datos en las unidades extraíbles depende del equipo con el cual la unidad extraíble está conectada.

Para descifrar unidades extraíbles:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Cifrado de datos → Cifrado de unidades extraíbles**.
4. Si desea descifrar todos los archivos cifrados almacenados en las unidades extraíbles, en la lista desplegable **Modo de cifrado**, seleccione **Descifrar toda la unidad extraíble**.

5. Para descifrar los datos que se almacenan en unidades extraíbles individuales, modifique las reglas de cifrado de las unidades extraíbles cuyos datos desea descifrar. Para ello:

   a. En la lista de unidades extraíbles para las cuales se han configurado reglas de cifrado, seleccione la entrada correspondiente a la unidad extraíble pertinente.

   b. Haga clic en el botón **Establecer una regla** para editar la regla de cifrado de la unidad extraíble seleccionada.

   c. En el menú contextual del botón **Establecer una regla**, seleccione el elemento **Descifrar toda la unidad extraíble**.

6. Guarde los cambios.

Como resultado, si un usuario conecta una unidad extraíble o si ya está conectada, Kaspersky Endpoint Security descifra la unidad extraíble. La aplicación advierte al usuario de que el proceso de descifrado puede tardar un tiempo. Si el usuario inicia la extracción segura de una unidad extraíble durante el descifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de descifrado de datos y permite la extracción de la unidad extraíble antes de que la operación de descifrado haya finalizado. El proceso de descifrado se reanudará cuando el usuario conecte la unidad nuevamente al equipo.

Si el proceso de descifrado de una unidad extraíble falla, puede ver el informe **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Es posible que otra aplicación bloquee el acceso a los archivos. En tal caso, pruebe a desconectar la unidad extraíble del equipo y volver a conectarla.

Visualización de los detalles del cifrado de datos

Mientras que las tareas de cifrado y descifrado están en curso, Kaspersky Endpoint Security envía a Kaspersky Security Center información sobre el estado de los parámetros del cifrado aplicados a los equipos cliente.

Ver el estado de cifrado

Puede ver el estado para supervisar el cifrado de datos. Kaspersky Endpoint Security asigna los siguientes estados de cifrado:

- **No cumple la directiva; cancelado por el usuario**. El usuario ha cancelado el cifrado de datos.
- **No cumple la directiva debido a un error**. Error de cifrado de datos; por ejemplo, falta una licencia.
- **Aplicando la directiva; se requiere reiniciar**. Cifrado de datos en curso en el equipo. Reinicie el equipo para completar el cifrado de datos.
- **No se ha especificado ninguna directiva de cifrado**. El cifrado de datos está desactivado en la configuración de directiva.
- **No compatible**. Los componentes de cifrado de datos no están instalados en el equipo.
- **Aplicando la directiva**. El cifrado y el descifrado de datos está en curso en el equipo.

Para ver el estado del cifrado de los datos del equipo:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Dispositivos administrados**.
3. En la pestaña **Dispositivos** del espacio de trabajo, mueva la barra de desplazamiento hacia la derecha. Si la columna **Estado de cifrado** no aparece, añádala en la configuración de la consola de Kaspersky Security Center.

   La columna **Estado de cifrado** muestra el estado del cifrado de los datos de los equipos que pertenecen al grupo de administración seleccionado. Este estado se forma según la información sobre el cifrado del archivo en unidades de disco locales del equipo y sobre el cifrado de disco completo.
4. Si el estado del cifrado de datos del equipo es **Aplicar directiva**, puede supervisar el panel de progreso de cifrado:
   a. Abra las propiedades del equipo con el estado **Aplicar directiva** haciendo doble clic en él.
   b. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.
   c. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows**.
   d. Haga clic en **Estadísticas**.
   e. En **Cifrado de dispositivos** puede ver el progreso actual del cifrado de datos como porcentaje.

Ver las estadísticas del cifrado en los paneles de Kaspersky Security Center

Para ver el estado del cifrado en los paneles de Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione el nodo **Servidor de administración**.
3. En el espacio de trabajo situado a la derecha del árbol de la consola de administración, seleccione la pestaña **Estadísticas**.
4. Cree una nueva página con paneles de información que contengan estadísticas de cifrado de datos. Para ello:
   a. En la pestaña **Estadísticas**, haga clic en el botón **Personalizar vista**.
   b. En la ventana que se abre, haga clic en el botón **Añadir**.
   c. En la ventana que se abre, en la sección **General**, escriba el nombre de la página.
   d. En la sección **Paneles de información**, haga clic en el botón **Agregar**.
   e. En la ventana que se abre, en el grupo **Estado de la protección**, seleccione el elemento **Cifrado de dispositivos**.
   f. Haga clic en **Aceptar**.

g. Si es necesario, edite la configuración del panel de detalles. Para hacerlo, utilice las secciones **Ver** y **Dispositivos**.

h. Haga clic en **Aceptar**.

i. Repita los pasos d-h del proceso, seleccionando el elemento **Cifrado de unidades extraíbles** en la sección **Estado de la protección**.

Los paneles de detalles añadidos aparecen en la lista de **Paneles de información**.

j. Haga clic en **Aceptar**.

El nombre de la página con los paneles de detalles creados en los pasos anteriores aparece en la lista **Páginas**.

k. Haga clic en el botón **Cerrar**.

5. En la pestaña **Estadísticas**, abra la página que se creó en los pasos anteriores de las instrucciones.

Aparecen los paneles de información que muestran el estado del cifrado de los equipos y de las unidades extraíbles.

Ver errores de cifrado de archivos en unidades del equipo local

Para ver los errores del cifrado del archivo en unidades del equipo local:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione **Dispositivos administrados**.

3. En la pestaña **Dispositivos**, seleccione el nombre del equipo en la lista y haga clic con el botón derecho del mouse para abrir el menú contextual.

4. En el menú contextual del equipo, seleccione el elemento **Propiedades**. En la ventana que se abre, seleccione la sección **Protección**.

5. Haga clic en el enlace **Ver errores de cifrado de datos** para abrir la ventana **Errores de cifrado de datos**.

Esta ventana muestra la información de los errores de cifrado de archivos de las unidades del equipo local. Cuando se corrige un error, Kaspersky Security Center elimina la información del error de la ventana **Errores de cifrado de datos**.

Visualización del informe del cifrado de datos

Kaspersky Security Center le permite crear informes de cifrado de datos:

- **Informe sobre el estado del cifrado de los dispositivos administrados**. El informe incluye información sobre si el estado de cifrado del equipo cumple con la directiva de cifrado.

- **Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo**. El informe incluye información sobre el estado de cifrado de dispositivos externos y dispositivos de almacenamiento.

- **Informe sobre los derechos de acceso a dispositivos cifrados**. El informe incluye información sobre el estado de las cuentas que tienen acceso a unidades cifradas.
- **Informe sobre errores en el cifrado de archivos**. El informe incluye información sobre los errores que se produjeron durante la ejecución de tareas de cifrado o descifrado de datos en los equipos.
- **Informe sobre el bloqueo del acceso a archivos cifrados**. El informe incluye información sobre aplicaciones bloqueadas para que no disponer de acceso a archivos cifrados.

Para ver el informe del cifrado de datos:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.

   Se inicia el Asistente de nueva plantilla de informe.
4. Siga los pasos del Asistente de plantillas de informe. En la ventana **Selección del tipo de plantilla de informe** de la sección **Otro**, seleccione uno de los informes de cifrado de datos.

   Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.
5. Seleccione la plantilla del informe que se creó en los pasos anteriores de las instrucciones.
6. En el menú contextual de la plantilla, seleccione **Mostrar informe**.

Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

Trabajar con dispositivos cifrados cuando no hay acceso a estos

Obtener acceso a los dispositivos cifrados

Es posible que se requiera a un usuario solicitar acceso a dispositivos cifrados en los siguientes casos:

- El disco duro se cifró en un equipo diferente.
- La clave de cifrado para un dispositivo no está en el equipo (por ejemplo, después del primer intento de acceder a la unidad extraíble cifrada en el equipo), y el equipo no está conectado a Kaspersky Security Center.

  Después de que el usuario ha aplicado la clave de acceso al dispositivo cifrado, Kaspersky Endpoint Security guarda la clave de cifrado en el equipo del usuario y permite el acceso a este dispositivo después de sucesivos intentos de acceso, incluso si no hay conexión con Kaspersky Security Center.

El acceso a dispositivos cifrados se puede obtener de la siguiente manera:

1. El usuario usa la interfaz de aplicación Kaspersky Endpoint Security para crear un archivo de solicitud de acceso con la extensión kesdc y lo envía al administrador de la red de área local corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo clave de acceso con la extensión kesdr y lo envía al usuario.
3. El usuario aplica la clave de acceso.

Restauración de datos de dispositivos cifrados

Un usuario puede usar la Utilidad de restauración de dispositivos cifrados (denominada en lo sucesivo la Utilidad de restauración) para trabajar con dispositivos cifrados. Esto se puede requerir en los siguientes casos:

- Falló el procedimiento para usar una clave de acceso para obtener acceso.
- Los componentes de cifrado no se han instalado en el equipo con el dispositivo cifrado.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración permanecen durante un tiempo sin cifrar en la memoria del equipo del usuario. Para reducir el riesgo de acceso no autorizado a estos datos, se aconseja restaurar el acceso a dispositivos cifrados en equipos de confianza.

Los datos en dispositivos cifrados se pueden restaurar de la siguiente manera:

1. El usuario usa la Utilidad de restauración para crear un archivo de solicitud de acceso con la extensión fdertc y lo envía al administrador de la red de área local corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo clave de acceso con la extensión fdertr y lo envía al usuario.
3. El usuario aplica la clave de acceso.

Para restaurar datos de discos duros de sistemas cifrados, el usuario también puede especificar las credenciales de la cuenta del Agente de autenticación en la Utilidad de restauración. Si los metadatos de la cuenta del Agente de autenticación están dañados, el usuario debe completar el procedimiento de restauración con un archivo de solicitud de acceso.

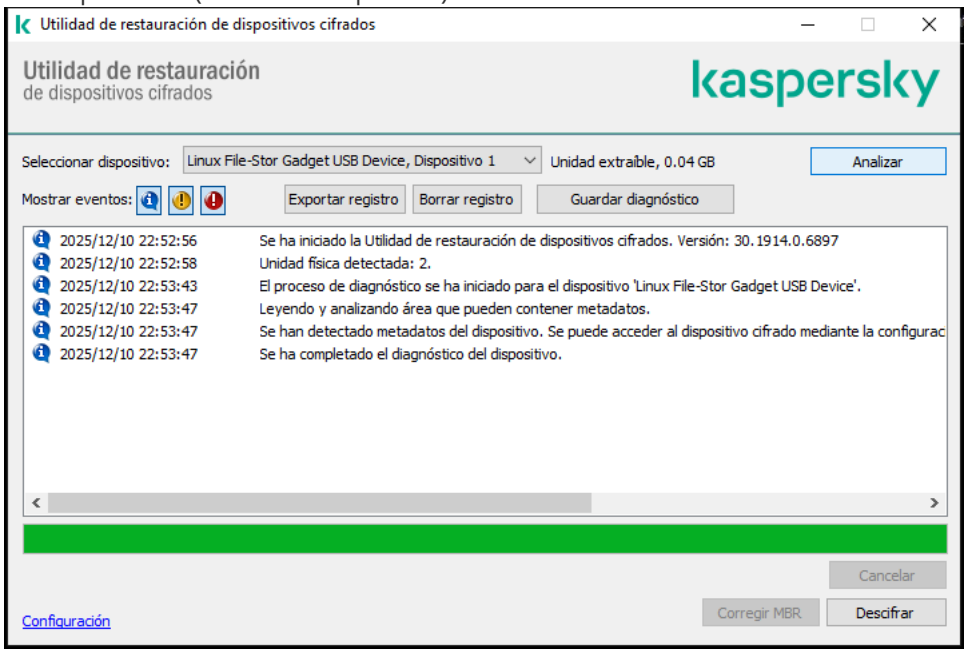
Antes de restaurar los datos en los dispositivos cifrados, se recomienda cancelar la directiva de Kaspersky Security Center o desactivar el cifrado en la configuración de la directiva de Kaspersky Security Center en el equipo donde el procedimiento se realizará. Esto evita que el dispositivo vuelva a cifrarse.

Recuperación de datos mediante la Utilidad de restauración FDERT

Si el disco duro falla, el sistema de archivos podría estar dañado. Si es así, los datos protegidos por la tecnología Cifrado de disco de Kaspersky no estará disponible. Puede descifrar los datos y copiarlos a una nueva unidad.

La recuperación de datos de un disco duro protegido por la tecnología Cifrado de disco de Kaspersky consta de los siguientes pasos:

1. Cree una Utilidad de restauración independiente (vea la imagen más abajo).
2. Conecte una unidad a un equipo que no tenga instalados los componentes de cifrado de Kaspersky Endpoint Security.
3. Ejecute la Utilidad de restauración y diagnostique el disco duro.
4. Acceda a los datos del disco. Para hacerlo, introduzca las credenciales del Agente de autenticación o inicie el procedimiento de recuperación (solicitud-respuesta).



Utilidad de restauración FDERT

Creación de una Utilidad de restauración independiente

Para crear el archivo ejecutable de la Utilidad de restauración:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Restaurar dispositivo cifrado**.

   Se ejecuta la Utilidad de restauración de dispositivos cifrados.

3. Haga clic en el botón **Crear Utilidad de restauración independiente** de la ventana de la Utilidad de restauración.

4. Guarde la Utilidad de restauración independiente en la memoria del equipo.

   Como resultado, el archivo ejecutable de la Utilidad de restauración (fdert.exe) se guardará en la carpeta especificada. Copie la Utilidad de restauración a un equipo que no tenga los componentes de cifrado de Kaspersky Endpoint Security. Esto evita que la unidad vuelva a cifrarse.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración permanecen durante un tiempo sin cifrar en la memoria del equipo del usuario. Para reducir el riesgo de acceso no autorizado a estos datos, se aconseja restaurar el acceso a dispositivos cifrados en equipos de confianza.

Recuperación de los datos de un disco duro

Para restaurar el acceso a un dispositivo cifrado por medio de la Utilidad de restauración:

1. Ejecute el archivo con el nombre fdert.exe, que es el archivo ejecutable de la Utilidad de restauración. Kaspersky Endpoint Security crea este archivo.

2. En la ventana Utilidad de restauración, seleccione el dispositivo cifrado al que desea restaurar el acceso.

3. Haga clic en el botón **Analizar** para permitir a la utilidad definir qué acciones se deben llevar a cabo en el dispositivo: si se debe desbloquear o descifrar.

   Si el equipo tiene acceso a la funcionalidad de cifrado de Kaspersky Endpoint Security, la Utilidad de restauración le pedirá a usted que desbloquee el dispositivo. Aunque el desbloqueo de un dispositivo no lo descifra, puede accederse a este directamente como consecuencia de estar desbloqueado. Si el equipo no tiene acceso a la funcionalidad de cifrado de Kaspersky Endpoint Security, la Utilidad de restauración le pedirá a usted que descifre el dispositivo.

4. Si desea importar información de diagnóstico, haga clic en el botón **Guardar diagnóstico**.

   La utilidad guardará un archivo comprimido con los archivos que contienen la información de diagnóstico.

5. Haga clic en el botón **Corregir MBR** si el diagnóstico del disco duro del sistema cifrado ha devuelto un mensaje acerca de que hay problemas relacionados con el registro de arranque principal (MBR) del dispositivo.

   Reparar el registro de arranque maestro puede reducir el tiempo que requiere obtener la información necesaria para desbloquear o descifrar el dispositivo.

6. Haga clic en el botón **Descifrar** o **Desbloquear**, según los resultados del diagnóstico.

7. Si desea restaurar los datos utilizando una cuenta del Agente de autenticación, seleccione la opción **Utilizar la configuración de la cuenta del Agente de autenticación** e introduzca las credenciales del Agente de autenticación.

   Este método solo es posible al restaurar datos en un disco duro del sistema. Si el disco duro del sistema está dañado y los datos de la cuenta del Agente de autenticación se han perdido, debe obtener una clave de acceso del administrador de la red de área local corporativa para restaurar datos en un dispositivo cifrado.

8. Si desea comenzar el procedimiento de recuperación, haga lo siguiente:

   a. Seleccione la opción **Especificar la clave de acceso al dispositivo manualmente**.

   b. Haga clic en el botón **Recibir la clave de acceso** y guarde el archivo de solicitud de acceso en la memoria del equipo (un archivo con la extensión FDERTC).

   c. Envíe el archivo de solicitud de acceso al administrador de la red de área local corporativa.

   > No cierre la ventana **Recibir clave de acceso al dispositivo** hasta que haya recibido la clave de acceso. Si esta ventana se abre de nuevo, no podrá aplicar la clave de acceso que el administrador había creado anteriormente.

   d. Reciba y guarde el archivo de acceso (un archivo con la extensión FDERTR) que creó y le proporcionó el administrador de la red de área local corporativa (consulte las instrucciones más abajo).

   e. Descargue el archivo de acceso en la ventana **Recibir clave de acceso al dispositivo**.

9. Si está descifrando un dispositivo, debe configurar ajustes de descifrado adicionales.

   - Especificar el área que se debe descifrar:
     - Si desea descifrar el dispositivo completo, seleccione la opción **Descifrar todo el dispositivo**.
     - Si desea descifrar una parte de los datos de un dispositivo, seleccione la opción **Descifrar áreas individuales del dispositivo** y especifique los límites de la parte que se va a descifrar.
   - Seleccione la ubicación para escribir los datos descifrados:
     - Si desea que los datos del dispositivo original se vuelvan a escribir con los datos descifrados, anule la selección de la casilla de selección **Descifrar en un archivo de imagen de disco**.
     - Si desea guardar los datos descifrados por separado de los datos cifrados originales, seleccione la casilla de selección **Descifrar en un archivo de imagen de disco** y el botón **Examinar** para especificar la ruta donde desea guardar el archivo VHD.

10. Haga clic en **Aceptar**.

Comienza el proceso de descifrado o desbloqueo.

Cómo crear un archivo de acceso a datos cifrados en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la Consola de administración, seleccione la carpeta **Avanzado → Protección y cifrado de datos → Dispositivos cifrados**.

3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que desea crear un archivo de clave de acceso. Luego, en el menú contextual del dispositivo, haga clic en **Obtener acceso para el dispositivo Kaspersky Endpoint Security**.

   Si no está seguro de para qué equipo se generó el archivo de solicitud de acceso, en el árbol de la Consola de administración, seleccione la carpeta **Avanzado → Protección y cifrado de datos** y, en el espacio de trabajo, haga clic en el enlace **Obtener clave de cifrado del dispositivo en Kaspersky Endpoint Security**.

4. En la ventana que se abre, seleccione el algoritmo de cifrado que quiere usar: AES256 o AES56.

   El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: *Cifrado fuerte (AES256)* o *Cifrado ligero (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

5. Haga clic en **Examinar** para abrir una ventana. En esta ventana, especifique la ruta al archivo de solicitud con la extensión fdertc que se recibió del usuario.

6. Haga clic en **Desbloquear**.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.

Cómo crear un archivo de acceso a datos cifrados en Web Console

1. En la ventana principal de Web Console, seleccione **Operaciones → Protección y cifrado de datos → Dispositivos cifrados**.

2. Seleccione la casilla de verificación junto al nombre del equipo del que quiere recuperar los datos.

3. Haga clic en **Conceder acceso al dispositivo en modo desconectado**.

   Se iniciará el Asistente para otorgar acceso a un dispositivo.

4. Siga las instrucciones del Asistente para otorgar acceso a un dispositivo:

   a. Seleccione el complemento Kaspersky Endpoint Security para Windows.

   b. Seleccione el algoritmo de cifrado que quiere usar: AES256 o AES56.

      El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: *Cifrado fuerte (AES256)* o *Cifrado ligero (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

   c. Seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión FDERTC).

   d. Seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión FDERTR).

Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

Creación de un disco de rescate del sistema operativo

El disco de rescate del sistema operativo puede ser útil cuando no se puede acceder a un disco duro cifrado por alguna razón y el sistema operativo no se puede cargar.

Puede cargar una imagen del sistema operativo Windows por medio del disco de rescate y restaurar el acceso al disco duro cifrado por medio de la Utilidad de restauración incluida en la imagen del sistema operativo.

Para crear un disco de rescate del sistema operativo:

1. Cree un archivo ejecutable para la Utilidad de restauración de dispositivos cifrados.

2. Cree una imagen personalizada del entorno de prearranque de Windows. Mientras tanto, añada el archivo ejecutable de la Utilidad de restauración a la imagen.

3. Guardar la imagen personalizada del entorno de preinstalación de Windows en medios de arranque como, por ejemplo, un lector de CD o una unidad extraíble.

   Consulte los archivos de ayuda de Microsoft para recibir instrucciones sobre la creación de una imagen personalizada del entorno de prearranque de Windows (por ejemplo, en el recurso Microsoft TechNet).

Componentes de Detection and Response.

Las soluciones de Kaspersky Detection and Response son sistemas de seguridad para detectar amenazas avanzadas e indicadores de ataque en diferentes niveles de la infraestructura de una organización. Las soluciones de Detection and Response brindan información sobre la amenaza detectada y permiten administrar las acciones de Threat Response.

Por lo tanto, la solución Detection and Response hace lo siguiente:

- Recibir información sobre el funcionamiento de un equipo, servidor u otros dispositivos (telemetría).
- Analizar automáticamente la información para detectar amenazas.
- Generar detalles de alerta como columnas de la cadena de desarrollo de amenazas para el análisis y la elección de acciones de respuesta a amenazas.
- Llevar a cabo acciones de Threat Response (por ejemplo, aislamiento de red del equipo).

Kaspersky Endpoint Security admite soluciones de Detection and Response usando un agente integrado. El agente integrado envía telemetría a los servidores de soluciones y lleva a cabo acciones de Threat Response. El agente integrado es compatible con:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) versión 7.1 o anterior
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Puede usar Kaspersky Endpoint Security con la solución Detection and Response en varias configuraciones; por ejemplo, [EDR Optimum+MDR].

Licencias de MDR y EDR Optimum

Kaspersky Endpoint Security admite la funcionalidad de las soluciones Kaspersky Managed Detection and Response (MDR) y Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Puede usar Kaspersky Endpoint Security con estas soluciones en varias configuraciones y crear un sistema de protección personalizado que satisfaga sus requisitos particulares. Para hacerlo, debe comprar una licencia para cada una de las soluciones. La licencia puede cubrir el derecho a usar una única solución (por ejemplo, solo el complemento de MDR) o varias soluciones (complemento [EDR Optimum + MDR]).

MDR y EDR Optimum admiten los siguientes métodos de licencia:

- La funcionalidad de MDR o EDR Optimum está incluida en la licencia de Kaspersky Endpoint Security para Windows.

  La funcionalidad estará disponible inmediatamente después de la activación de Kaspersky Endpoint Security para Windows. Solo necesita añadir una clave.

- Licencias independientes para MDR o EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  La funcionalidad está disponible después de agregar una clave separada para el complemento MDR, el complemento EDR Optimum o el complemento [EDR Optimum + MDR]. Como resultado, se añaden dos claves en el equipo: una para Kaspersky Endpoint Security y otra para MDR o EDR Optimum. La clave de Kaspersky Endpoint Security debe ser la primera en añadirse.

Kaspersky Endpoint Security permite añadir solo una *clave activa* para licencias MDR y EDR Optimum. Por lo tanto, si necesita activar ambas soluciones, debe añadir una clave del [EDR Optimum+MDR] Add-on en lugar de una clave independiente para cada solución. También puede añadir una *clave de reserva*.

Si usó un archivo BLOB al implementar MDR, no necesita una clave independiente para activar MDR. El archivo BLOB ya contiene información de licencia.

Licencias iniciales de soluciones

Al implementar MDR y EDR Optimum por primera vez, las soluciones se activan de la misma manera que la aplicación Kaspersky Endpoint Security. Puede añadir una clave usando la tarea *Añadir clave* o usar la función de distribución automática de claves. La clave de licencia se añade a la aplicación como una segunda clave activa o como clave de reserva si selecciona la casilla de verificación correspondiente.

Cambiar de una licencia a otra

Si su organización ya tiene implementada una de estas soluciones y se ha añadido la clave correspondiente a la aplicación, existen algunas consideraciones especiales relacionadas con la licencia de la nueva configuración. Al cambiar a una licencia diferente, la aplicación no añade la nueva clave a la aplicación, sino que reemplaza la clave actual con la nueva clave. El motivo de esto es la restricción que permite a la aplicación añadir una única clave para activar MDR y EDR Optimum.

Por ejemplo, suponga que su organización tiene implementada la solución [EDR Optimum+MDR] y decide cambiar a la configuración del complemento MDR. Para cambiar a la nueva configuración, debe reemplazar la clave del [EDR Optimum+MDR] Add-on por la clave del complemento MDR.

Ya no está disponible una licencia independiente para EDR Optimum y MDR (complemento [EDR Optimum + MDR]). Si desea utilizar ambas soluciones, debe activar MDR mediante un archivo BLOB y EDR Optimum con una clave de licencia.

Con la función de distribución automática de claves, la aplicación rechaza las claves de licencia que cubren el mismo número de soluciones. Es decir, si tiene una clave de complemento de EDR Optimum añadida, no puede reemplazar esta clave con una clave de complemento de MDR. Sin embargo, puede reemplazar la clave del complemento EDR Optimum con una clave del complemento [EDR Optimum + MDR]. La aplicación también rechaza claves si intenta reemplazar una clave de complemento de MDR con una clave de complemento de EDR. Para reemplazar una clave, puede ejecutar la tarea *Añadir clave*. La tarea *Añadir clave* permite reemplazar las claves de licencia con cualquier cantidad de soluciones.

Si tiene una clave de reserva de [EDR Optimum+MDR] Add-on añadida, para agregar correctamente una clave activa de complemento de EDR Optimum o MDR correctamente, debe reemplazar antes la clave de reserva con una clave de complemento de EDR Optimum o MDR o, alternativamente, eliminar la clave de reserva y reemplazar a continuación la clave activa.

Compatibilidad con soluciones EDR de terceros

Puede utilizar Kaspersky Endpoint Security para proteger estaciones de trabajo y servidores junto con soluciones EDR de terceros. Para eliminar falsos positivos, recomendamos añadir archivos ejecutables de Kaspersky Endpoint Security y Network Agent a la zona de confianza de su solución EDR de terceros.

Zona de confianza para la compatibilidad con soluciones EDR de terceros

	Kaspersky Endpoint Security para Windows	Agente de red de Kaspersky Security Center
Carpeta de trabajo	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Archivos ejecutables	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent admite la interacción entre la aplicación y otras soluciones de Kaspersky para detectar amenazas avanzadas (por ejemplo Kaspersky Sandbox). Las soluciones de Kaspersky son compatibles con versiones determinadas de Kaspersky Endpoint Agent.

Para utilizar Kaspersky Endpoint Agent como parte de las soluciones de Kaspersky, debe activar dichas soluciones con la correspondiente clave de licencia.

Para obtener información completa sobre Kaspersky Endpoint Agent incluido en la solución de software que está utilizando y para obtener información completa sobre la solución independiente, consulte la Guía de ayuda del producto correspondiente:

- Ayuda de Kaspersky Anti Targeted Attack Platform
- Ayuda de Kaspersky Sandbox
- Ayuda de Kaspersky Endpoint Detection and Response Optimum
- Ayuda de Kaspersky Managed Detection and Response

El kit de distribución para Kaspersky Endpoint Security versiones 11.2.0 – 11.8.0 incluye Kaspersky Endpoint Agent. Puede seleccionar Kaspersky Endpoint Agent al instalar Kaspersky Endpoint Security para Windows. Como resultado, se instalarán dos aplicaciones en el equipo: KEA y KES. En Kaspersky Endpoint Security 11.9.0, el paquete de distribución de Kaspersky Endpoint Agent ya no forma parte del kit de distribución de Kaspersky Endpoint Security.

Correspondencia de las versiones de KEA (como parte de KES) con las versiones de KES

Kaspersky Endpoint Security para Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky está cambiando todo Detection and Response para que funcione con el agente integrado de Kaspersky Endpoint Security en lugar de Kaspersky Endpoint Agent. Kaspersky está agregando gradualmente soporte para estas soluciones y eliminando Kaspersky Endpoint Agent (consulte la tabla a continuación). A partir de la versión 12.1, la aplicación admite todas las soluciones de Detection and Response. Además, a partir de la versión 12.1, la aplicación ya no es compatible con Kaspersky Endpoint Agent y ya no es posible instalar ambas aplicaciones en paralelo en el mismo equipo.

Versión de Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (componente Endpoint Detection and Response Expert)	Kaspersky Anti Targeted Attack Platform (componente Network Detection and Response Expert)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent
12.6	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**

Migrar la configuración [KES + KEA] a la configuración [KES + agente incorporado]

Kaspersky Endpoint Security incluye agentes incorporados para trabajar con soluciones de Detection and Response. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con estas soluciones. Al desplegar Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, las soluciones de Detection and Response seguirán funcionando con Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo.

El kit de distribución para Kaspersky Endpoint Security versiones 11.2.0 – 11.8.0 incluye Kaspersky Endpoint Agent. Puede seleccionar Kaspersky Endpoint Agent al instalar Kaspersky Endpoint Security para Windows. Como resultado, se instalarán dos aplicaciones en el equipo: KEA y KES. En Kaspersky Endpoint Security 11.9.0, el paquete de distribución de Kaspersky Endpoint Agent ya no forma parte del kit de distribución de Kaspersky Endpoint Security.

La migración de la configuración de [KES + KEA] a [KES + agente incorporado] implica los siguientes pasos:

1. **Actualizar Kaspersky Security Center**

   Actualizar todos los componentes de Kaspersky Security Center a la versión 13.2 o superior, incluidos el Agente de red en equipos de usuarios y Web Console.

2. **Actualizar el complemento web de Kaspersky Endpoint Security**

En Kaspersky Security Center Web Console, actualizar el complemento web de Kaspersky Endpoint Security a la versión 11.7.0 o superior. Para administrar los componentes EDR Optimum y Kaspersky Sandbox, debe usar Web Console.

Para usar Kaspersky Anti Targeted Attack Platform (EDR), necesitará un complemento web para Kaspersky Endpoint Security versión 12.1 o posterior.

Para usar Kaspersky Anti Targeted Attack Platform (NDR), necesitará un complemento web para Kaspersky Endpoint Security versión 12.7 o posterior.

3. **Migrar las directivas y tareas**

   Use el Asistente de migración de directivas y tareas de Kaspersky Endpoint Agent para migrar la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows.

   Esto crea una nueva directiva de Kaspersky Endpoint Security. La directiva nueva tiene el estado *Inactiva*. Para aplicar la directiva, abra las propiedades de la directiva, acepte la Declaración de Kaspersky Security Network y configure el estado a *Activa*.

4. **Funcionalidad de licencias**

   Si utiliza una licencia común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Agent, la funcionalidad EDR Optimum se activa de manera automática después de actualizar la aplicación a la versión 11.7.0. No necesita realizar ninguna otra acción.

   Si utiliza una licencia independiente adicional de Kaspersky Endpoint Detection and Response Optimum para activar la funcionalidad EDR Optimum, debe asegurarse de que la clave del complemento EDR Optimum se añada al repositorio de Kaspersky Security Center y de que la funcionalidad de distribución automática de claves de licencia esté activada. Después de actualizar la aplicación a la versión 11.7.0, la funcionalidad EDR Optimum se activa de manera automática.

   Si utiliza una licencia de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Agent, y una licencia diferente para activar Kaspersky Endpoint Security para Windows, debe reemplazar la clave para Kaspersky Endpoint Security para Windows con la clave común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. Puede reemplazar la clave con la tarea *Añadir clave*.

   No necesita activar la funcionalidad Kaspersky Sandbox. Kaspersky Sandbox estará disponible de forma inmediata después de actualizar y activar Kaspersky Endpoint Security para Windows.

   Solo se puede usar la licencia de Kaspersky Anti Targeted Attack Platform para activar Kaspersky Endpoint Security como parte de la solución Kaspersky Anti Targeted Attack Platform. Después de actualizar la aplicación a la versión 12.1, la funcionalidad EDR (KATA) se activa de manera automática. No necesita realizar ninguna otra acción.

5. **Actualizar la aplicación de Kaspersky Endpoint Security**

   Para actualizar la aplicación y migrar las funcionalidades EDR Optimum y Kaspersky Sandbox, se recomienda usar una tarea de instalación remota.

Para actualizar la aplicación mediante una tarea de instalación remota, debe modificar las siguientes configuraciones:

- Seleccione los componentes de las soluciones de Detection and Response en la configuración del paquete de instalación.
- Excluya el componente Kaspersky Endpoint Agent en la configuración del paquete de instalación (para Kaspersky Endpoint Security para Windows versiones 11.2.0 – 11.8.0).
- Si la Protección con contraseña está habilitada para restringir el acceso a Kaspersky Endpoint Agent, introduzca la contraseña de desinstalación de la aplicación en la configuración de la tarea *Instalar aplicación en remoto*. Puede introducir la contraseña de desinstalación a partir de Kaspersky Security Center Linux 15.1.

También puede actualizar la aplicación con los siguientes métodos:

- Utilizando el servicio de actualización de Kaspersky (Seamless Update - SMU).
- De forma local, utilizando el Asistente de instalación.

Kaspersky Endpoint Security admite la selección automática de componentes al actualizar la aplicación en un equipo con la aplicación Kaspersky Endpoint Agent instalada. La selección automática de componentes depende de los permisos de la cuenta de usuario que está actualizando la aplicación.

Si está actualizando Kaspersky Endpoint Security con el archivo EXE o MSI en la cuenta del sistema (SYSTEM), Kaspersky Endpoint Security obtiene acceso a las licencias actuales de las soluciones de Kaspersky. Por lo tanto, si el equipo tiene, por ejemplo, Kaspersky Endpoint Agent instalado y la solución EDR Optimum activada, el instalador de Kaspersky Endpoint Security configura automáticamente el conjunto de componentes y selecciona el componente EDR Optimum. Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina Kaspersky Endpoint Agent. La ejecución del instalador MSI con la cuenta del sistema (SYSTEM) se realiza normalmente cuando se actualiza a través del servicio de actualización de Kaspersky (SMU) o cuando se despliega un paquete de instalación a través de Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tendrá acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes según la configuración de Kaspersky Endpoint Agent. Tras esto, Kaspersky Endpoint Security pasa a utilizar el agente integrado y elimina Kaspersky Endpoint Agent.

6. **Reinicio del equipo**

   Reinicie el equipo para terminar de actualizar la aplicación con el agente incorporado. Al actualizar la aplicación, el instalador elimina Kaspersky Endpoint Agent antes de reiniciar el equipo. Después de reiniciar el equipo, el instalador añade el agente incorporado. Esto significa que Kaspersky Endpoint Security no realiza las funciones de EDR y Kaspersky Sandbox hasta que no se reinicia el equipo.

7. **Revisar el estado de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox**

Si, después de la actualización, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.
- Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*.
- Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

- Asegúrese de que la funcionalidad EDR Optimum esté activada mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, compruebe que la funcionalidad de distribución automática de claves de licencia de EDR Optimum esté activada.

Migración de directivas y tareas para Kaspersky Endpoint Agent

Kaspersky Endpoint Security para Windows incluye un asistente para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Puede migrar la configuración de directivas y tareas para las siguientes soluciones:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Un asistente para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security solo funciona en Web Console y Cloud Console. En la Consola de administración (MMC), solo puede migrar la configuración de la solución Kaspersky Anti Targeted Attack Platform (EDR) mediante el Asistente de migración de directivas y tareas estándar de Kaspersky Security Center.

Se recomienda comenzar con la migración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en un solo equipo, luego, en un grupo de equipos y después completar la migración en todos los equipos de la organización.

Para migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security, haga lo siguiente:

En la ventana principal de Web Console, seleccione **Operaciones → Migración desde Kaspersky Endpoint Agent**.

Esto ejecuta el asistente de migración de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Migración de directivas

El Asistente de migración crea una directiva nueva que combina las configuraciones de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee unir con la directiva de Kaspersky Endpoint Security. Haga clic en una directiva de Kaspersky Endpoint Agent para seleccionar la directiva de Kaspersky Endpoint Security con la que desea unir la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de tareas

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desee crear para la directiva de Kaspersky Endpoint Security. El asistente admite tareas para Kaspersky Endpoint Detection and Response y Kaspersky Sandbox. Ir al paso siguiente.

Paso 3: Fin del asistente

Finalice el asistente. Como resultado, el asistente hace lo siguiente:

- Crea una directiva de Kaspersky Endpoint Security.

  La directiva une la configuración de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. La directiva se denomina *<nombre de la directiva de Kaspersky Endpoint Security> y <nombre de la directiva de Kaspersky Endpoint Agent>*. La directiva nueva tiene el estado *Inactiva*. Para continuar, cambie los estados de las directivas de Kaspersky Endpoint Agent y Kaspersky Endpoint Security a *Inactiva* y active la directiva nueva y combinada.

  Después de realizar la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, asegúrese de que la directiva nueva tenga configurada la funcionalidad para la transferencia de datos al Servidor de administración (datos del archivo en cuarentena y datos de la cadena de desarrollo de la amenaza). Los valores de parámetros de la transferencia de datos no se migran desde una directiva de Kaspersky Endpoint Agent.

  Al migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para la solución Kaspersky Anti Targeted Attack Platform (EDR), es posible que encuentre errores al conectar el equipo a los servidores del Nodo Central. El motivo es que el asistente de migración de Web Console omite las siguientes configuraciones de directivas y no las migra:

  - Prohibición de modificar la configuración **Conexión a servidores de KATA** ("candado").

    De forma predeterminada, la configuración se puede modificar (el "candado" está abierto). Por lo tanto, la configuración no se aplica en el equipo. Debe prohibir la modificación de la configuración y cerrar el "candado".

  - Contenedor criptográfico.

    Si está utilizando la autenticación bidireccional para conectarse a los servidores del Nodo Central, debe volver a agregar el contenedor criptográfico. El asistente de migración migra correctamente el certificado TLS del servidor.

El Asistente de migración de directivas y tareas de la Consola de administración (MMC) migra todas las configuraciones a la solución Kaspersky Anti Targeted Attack Platform (EDR).

- Se crean tareas nuevas de Kaspersky Endpoint Security.

  Las tareas nuevas son copias de las tareas de Kaspersky Endpoint Agent para Kaspersky Endpoint Detection and Response y Kaspersky Sandbox. Al mismo tiempo, el Asistente deja las tareas de Kaspersky Endpoint Agent sin cambios.

Cómo migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en la Consola de administración (MMC) (solo para KATA [EDR]).

1. En la Consola de administración, elija el Servidor de administración y haga clic con el botón derecho para abrir el menú contextual.
2. Seleccione **Todas las tareas → Asistente de conversión por lotes de directivas y tareas**.

Se iniciará el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Elija la aplicación para la que necesita convertir directivas y tareas

En este paso, debe elegir Kaspersky Endpoint Security para Windows. Ir al paso siguiente.

Paso 2. Conversión de directivas

El Asistente de migración crea una nueva directiva de Kaspersky Endpoint Security a la que se migrará la configuración de la directiva de Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee transferir a la directiva de Kaspersky Endpoint Security. Ir al paso siguiente.

A continuación, el Asistente de migración comenzará a convertir las directivas. Durante la conversión de directivas, el Asistente de migración le solicita que acepte la Declaración de Kaspersky Security Network. Las nuevas directivas recibirán el nombre *<Nombre de la directiva> (convertida)*.

Paso 3. Conversión de tareas

Omita este paso. El asistente admite tareas para Kaspersky Endpoint Detection and Response y Kaspersky Sandbox. La gestión de estos componentes solo está disponible en Web Console. Ir al paso siguiente.

Paso 4: Fin del asistente

Finalice el asistente. Como resultado del asistente, se creará una nueva directiva de Kaspersky Endpoint Security.

Endpoint Detection and Response Agent (EDR Agent)

A partir de Kaspersky Endpoint Security 12.3 para Windows, la aplicación incluye la configuración de Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* es una aplicación que se instala en estaciones de trabajo y servidores individuales en la infraestructura de TI de la organización para dar soporte a las siguientes soluciones de Detection and Response de Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (a partir de la versión 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (a partir de la versión 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (a partir de la versión 12.11)

EDR Agent no admite la integración con la solución Kaspersky Endpoint Detection and Response Expert (cloud).

EDR Agent supervisa continuamente los procesos que se ejecutan en estos equipos, las conexiones de red abiertas y los archivos que se modifican. Los componentes de protección y control de la aplicación no están disponibles para EDR Agent.

EDR Agent es compatible con aplicaciones EPP de terceros. Esto le permite utilizar herramientas de seguridad de infraestructura de terceros junto con Detection and Response de Kaspersky.

Para implementar EDR Agent, el equipo debe tener instalado el Agente de red y debe haberse añadido a la consola de Kaspersky Security Center. Para habilitar la interacción de EDR Agent con Kaspersky Security Center, debe instalar el complemento de administración de Kaspersky Endpoint Security para Windows. Puede especificar la configuración de EDR Agent mediante una directiva de grupo. Para integrar EDR Agent, debe configurar la integración en las secciones de la directiva correspondiente.

Las siguientes aplicaciones de Kaspersky se deben instalar en la infraestructura para admitir las soluciones de Kaspersky Detection and Response:

	• Agente de red • EDR Agent
Endpoint	
	Complemento de administración de Kaspersky Endpoint Security para Windows
Kaspersky Security Center	
	
Soluciones de detección y respuesta: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Instalación de Instale EDR Agent

Kaspersky Endpoint Security en la configuración del Endpoint Detection and Response Agent (EDR Agent) para las soluciones de Kaspersky Detection and Response se instala de la misma manera.

EDR Agent se puede instalar en el equipo de una de las siguientes maneras:

- De forma remota utilizando Kaspersky Security Center.
- De forma local, utilizando el Asistente de configuración.
- Localmente en la línea de comandos (solo para KATA (EDR) y EDR Expert (on-premises)).

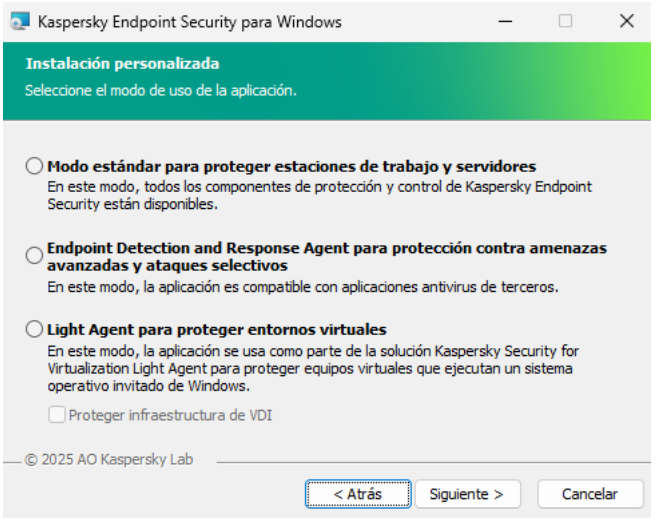
Para instalar EDR Agent, debe seleccionar la configuración adecuada en la configuración del paquete de instalación o en el Asistente de configuración.

Cómo instalar EDR Agent con el Asistente de configuración

1. Copie la carpeta del kit de distribución al equipo del usuario.
2. Ejecute setup_kes.exe.

   Se iniciará el Asistente de instalación.

Configuración de Kaspersky Endpoint Security



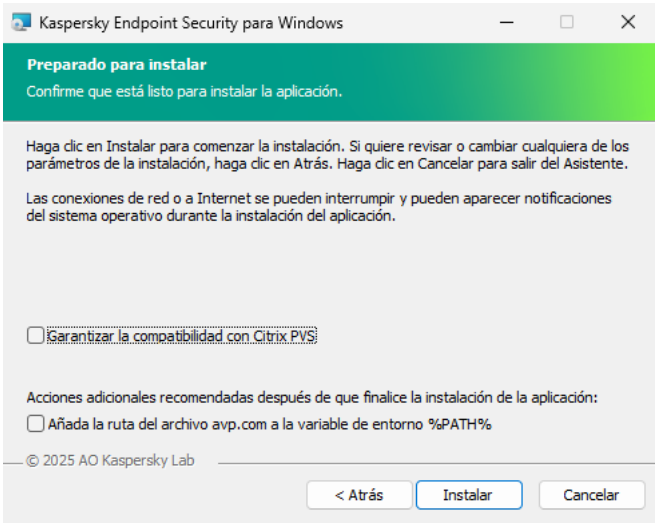
Elección de la configuración de la aplicación

Seleccione la configuración de **Endpoint Detection and Response Agent**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.

Los componentes de Kaspersky Endpoint Security

Seleccione los componentes que desee instalar. Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación. Para ello, tiene que ejecutar el Asistente de instalación de nuevo y elegir cambiar los componentes disponibles.

Configuración avanzada



Configuración de la instalación de la aplicación avanzada

Proteger el proceso de instalación de la aplicación. La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Windows Remote Desktop), se aconseja que desactive la protección del proceso de instalación.

Garantizar la compatibilidad con Citrix PVS. Puede habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual.

Añada la ruta del archivo avp.com a la variable de entorno %PATH%. Puede añadir la ruta de instalación a la variable %PATH% para un uso conveniente de la interfaz de línea de comandos.

Cómo instalar EDR Agent en la línea de comandos (solo para KATA (EDR) y EDR Expert (on-premises))

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.

2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.

3. Ejecute el siguiente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

o bien

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

Como resultado, la aplicación EDR Agent para la integración con Kaspersky Anti Targeted Attack Platform (EDR) o Kaspersky Endpoint Detection and Response Expert (on-premises) se instala en el equipo. Para confirmar que la aplicación está instalada y comprobar su configuración, use el comando `status`.

Cómo instalar EDR Agent usando la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione la carpeta **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

   Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.
3. Abra las propiedades del paquete de instalación.

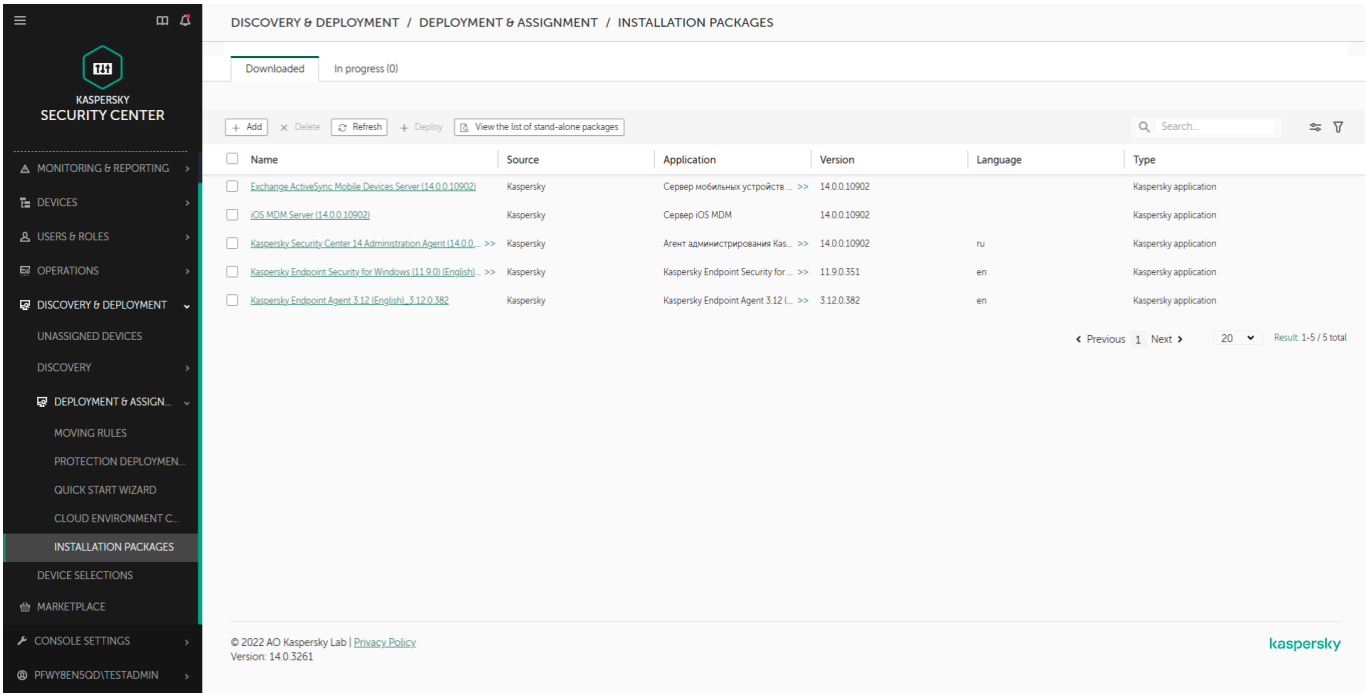
   Si necesario, cree un nuevo paquete de instalación.
4. Vaya a la sección **Componentes de protección**.
5. Seleccione la configuración de **Endpoint Detection and Response Agent para protección contra amenazas avanzadas y ataques selectivos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.
6. Seleccione los componentes que desee instalar.

   Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación.
7. Guarde los cambios.
8. Crear de una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que ha creado.

Cómo instalar EDR Agent usando Web Console

1. En la ventana principal de Web Console, seleccione **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.



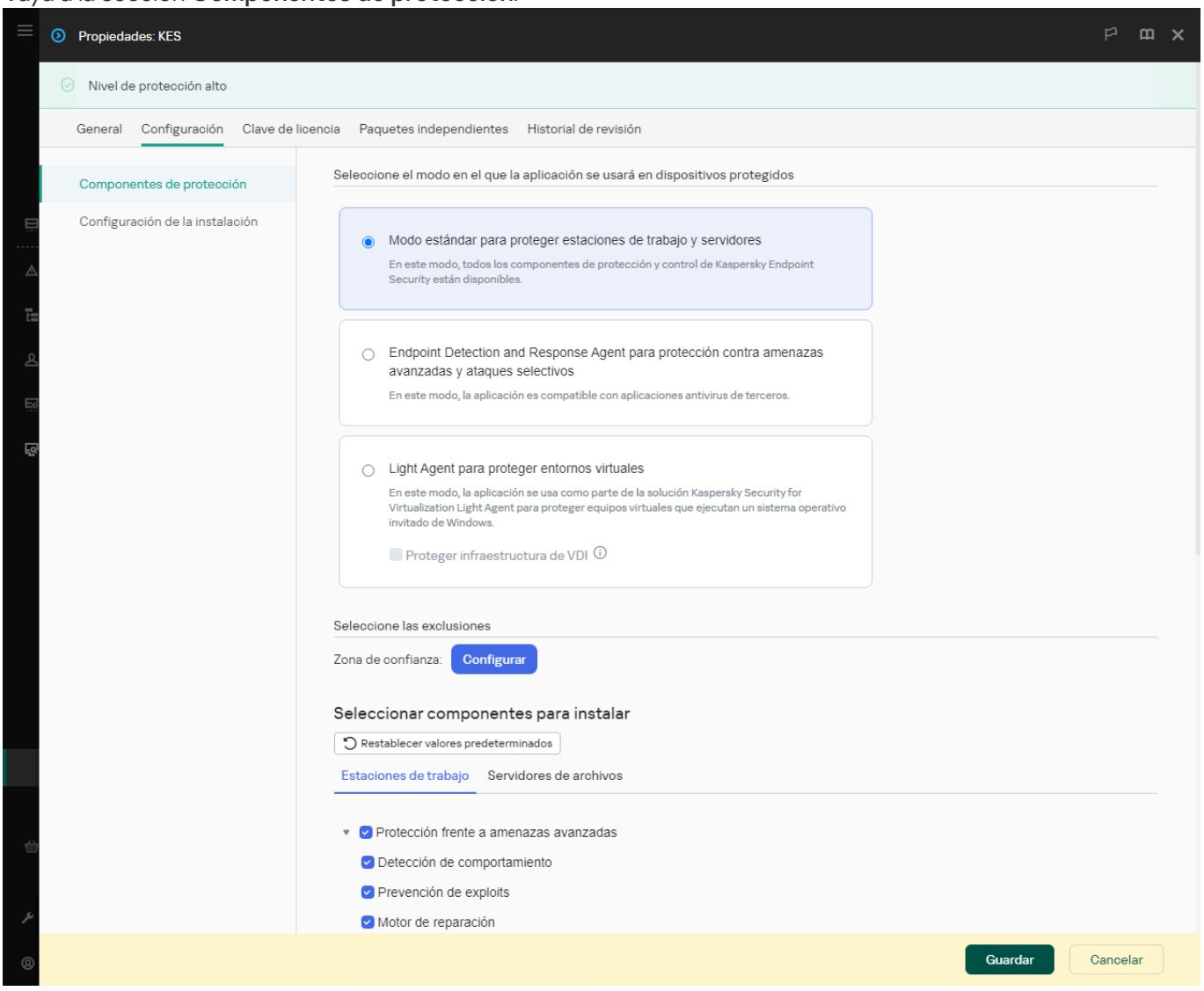
Lista de paquetes de instalación

2. Abra las propiedades del paquete de instalación.

   Si necesario, cree un nuevo paquete de instalación.

3. Seleccione la pestaña **Configuración**.

4. Vaya a la sección **Componentes de protección**.



Componentes incluidos en el paquete de instalación

5. Seleccione la configuración de **Endpoint Detection and Response Agent**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de detección y respuesta: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), y también KUMA. Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de Kaspersky Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.

6. Seleccione los componentes que desee instalar.

   Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación.

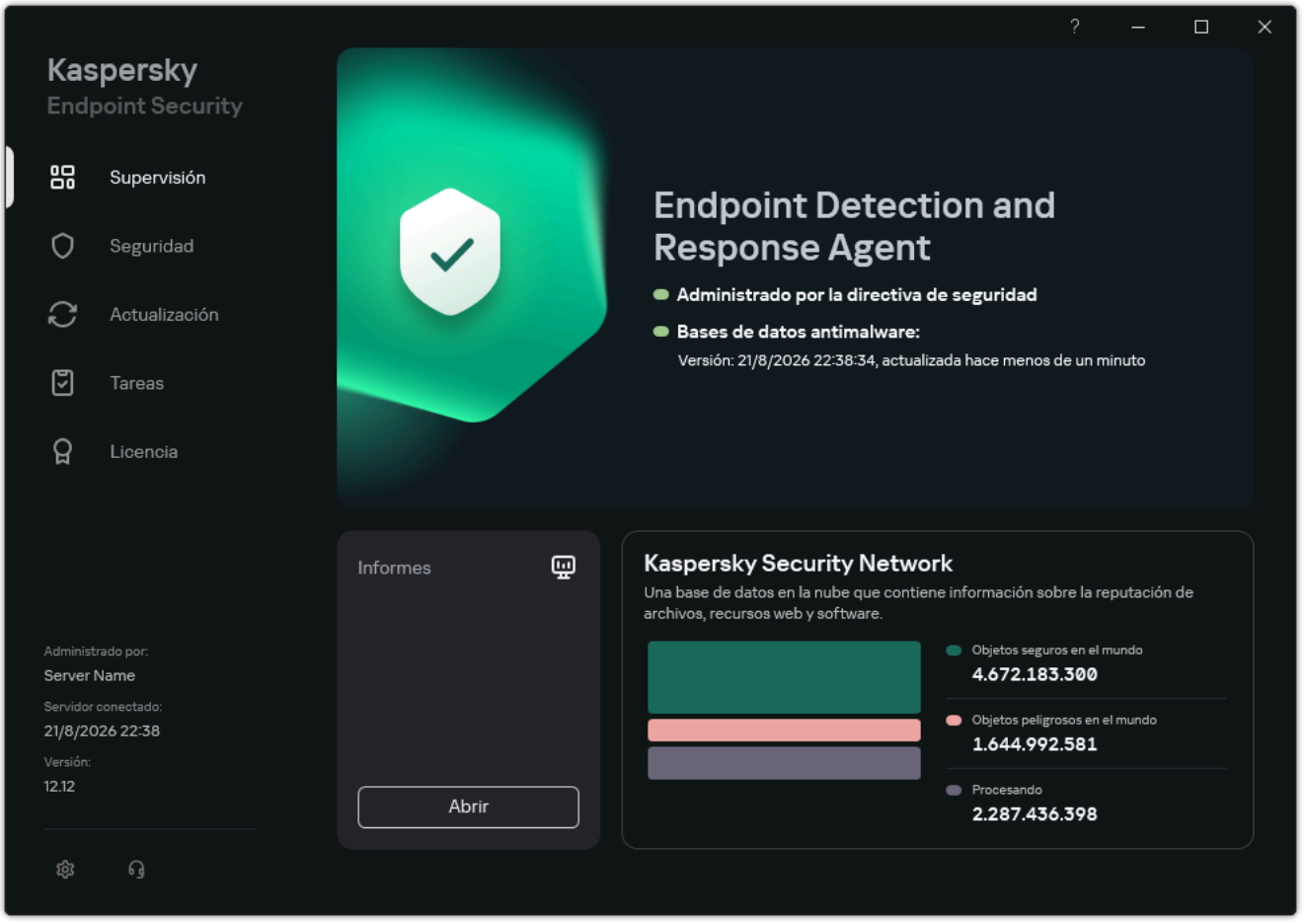
7. Guarde los cambios.

8. Crear de una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que ha creado.

Como resultado, EDR Agent se instala en el equipo del usuario. Puede utilizar la interfaz de la aplicación; aparece un icono de la aplicación en el área de notificaciones .

En Kaspersky Security Center, el equipo con la aplicación instalada en la configuración de EDR Agent tiene el estado *Crítico*: . El equipo tiene este estado porque falta el componente Protección frente a amenazas en archivos. No necesita realizar ninguna acción.

Si no ha podido instalar EDR Agent en un equipo con una aplicación EPP de terceros porque el instalador encontró software incompatible en el equipo, puede omitir la verificación de software incompatible.



Ventana principal de EDR Agent

Ahora debe configurar la integración con la solución Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) o Kaspersky Anti Targeted Attack (NDR). También puede especificar una configuración avanzada de la aplicación y, por ejemplo, crear una zona de confianza u ocultar la interfaz de la aplicación. Están disponibles las configuraciones en las siguientes secciones:

- Kaspersky Security Network
- Configuración de la aplicación
- Configuración de red
- Exclusiones
- Informes

- Interfaz
- Administrar configuración

Integración de EDR Agent con MDR

EDR Agent se instala en estaciones de trabajo y servidores en la infraestructura de TI de la organización. EDR Agent procesa datos y los envía a través de flujos de Kaspersky Security Network a Kaspersky Managed Detection and Response.

Para que Kaspersky Managed Detection and Response funcione con el Servidor de administración a través de Kaspersky Security Center Web Console, debe establecer una conexión nueva y segura, una *conexión en segundo plano*. Kaspersky Managed Detection and Response le solicita que establezca una conexión en segundo plano cuando despliega la solución. Asegúrese de que la conexión en segundo plano esté establecida.

Establecer una conexión en segundo plano en Web Console

1. En la ventana principal de Web Console, seleccione **Configuración** → **Integración**.
2. Vaya a la sección **Integración**.
3. Active la opción **Conexión en segundo plano para la integración Activada**.
4. Guarde los cambios.

La integración con Kaspersky Managed Detection and Response consta de los siguientes pasos:

1. **Instalar el componente Managed Detection and Response**

   Puede seleccionar el componente MDR durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

   > Para instalar el componente Managed Detection and Response sin reiniciar el equipo mediante la tarea *Cambiar componentes de la aplicación*, debe desactivar la opción **Comprobar si existen aplicaciones de terceros incompatibles** en la configuración de la tarea.

2. **Configuración de Kaspersky Private Security Network**

   > Omita este paso si utiliza Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configura automáticamente Kaspersky Private Security Network al instalar el complemento MDR.

   Kaspersky Private Security Network (KPSN) es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos.

   Cargue el archivo de configuración de Kaspersky Security Network en las propiedades del Servidor de administración. El archivo de configuración de Kaspersky Security Network se encuentra dentro del archivo comprimido ZIP del archivo de configuración de MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener detalles sobre la configuración de Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center. También puede cargar un archivo de configuración de Kaspersky Security Network en el equipo desde la línea de comandos (consulte las instrucciones a continuación).

Cómo configurar Kaspersky Private Security Network desde la línea de comandos

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

```
avp.com KSN /private <file name>
```

donde `<file name>` es el nombre del archivo de configuración que contiene la configuración de Kaspersky Private Security Network (formato de archivo PKCS7 o PEM).

Ejemplo:
`avp.com KSN /private C:\kpsn_config.pkcs7`

Como resultado, Kaspersky Endpoint Security utilizará Kaspersky Private Security Network para determinar la reputación de archivos, aplicaciones y sitios web. La sección **Kaspersky Security Network** de la configuración de la directiva mostrará el siguiente estado operativo: *Infraestructura: Kaspersky Private Security Network*.

Debe activar el modo de KSN ampliado para que funcione Managed Detection and Response.

3 Activar Kaspersky Managed Detection and Response

A partir de Kaspersky Endpoint Security para Windows 12.10, para activar la función Managed Detection and Response, como alternativa a una código de activación, también puede utilizar un archivo clave.

Debe comprar una licencia separada para MDR (complemento de Kaspersky Managed Detection and Response).

La funcionalidad estará disponible tras añadir una clave diferente para el complemento de Kaspersky Managed Detection and Response. La licencia para la funcionalidad independiente de Managed Detection and Response es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad MDR esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

4 Activación del componente Managed Detection and Response

Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (consulte las instrucciones a continuación). El archivo BLOB contiene el ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra dentro del archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener información detallada sobre un archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

A partir de Kaspersky Endpoint Security 12.6 para Windows, añadir un archivo BLOB es opcional para Kaspersky Managed Detection and Response sin inquilinos si tiene una licencia actual.

Cómo activar el componente Managed Detection and Response en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.

4. Seleccione la casilla **Managed Detection and Response (Industrial CyberSecurity)**.

5. En el bloque **Configuración**, haga clic en **Cargar** y seleccione el archivo BLOB recibido en Kaspersky Managed Detection and Response Console. El archivo tiene la extensión P7.

   De forma predeterminada, el usuario puede administrar la configuración de la aplicación ("candado" abierto). Para aplicar la directiva en equipos, cierre los candados .

6. Guarde los cambios.

Cómo activar el componente Managed Detection and Response en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.

5. Active la opción **Managed Detection and Response ACTIVADO**.

6. Haga clic en **Cargar** y seleccione el archivo BLOB que se obtuvo en Kaspersky Managed Detection and Response Console. El archivo tiene la extensión P7.

   De forma predeterminada, el usuario puede administrar la configuración de la directiva ("candado" abierto). Para aplicar la directiva en equipos, cierre los candados .

7. Guarde los cambios.

Cómo activar el componente Managed Detection and Response desde la línea de comandos

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.

2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

3. Ejecute el siguiente comando:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Configurar parámetros de la aplicación**.

Como resultado, Kaspersky Endpoint Security realizará una comprobación del archivo BLOB. La verificación del archivo BLOB incluye la verificación de la firma digital y el período de licencia. Si el archivo BLOB se verifica correctamente, Kaspersky Endpoint Security descargará el archivo y lo enviará al equipo durante la próxima sincronización con Kaspersky Security Center. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en informes de la interfaz local de Kaspersky Endpoint Security. El componente **Managed Detection and Response** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

5. **Configurar otros componentes de la aplicación para recibir telemetría**

   Debe activar los siguientes componentes para que Managed Detection and Response funcione:

   - Kaspersky Security Network (modo ampliado).
   - Detección de comportamiento.
   - Prevención de exploits.
   - Protección frente a amenazas web.
   - Protección frente a amenazas en el correo.
   - Protección frente a amenazas en archivos.
   - Protección frente a amenazas en la red.
   - Firewall.
   - Protección AMSI.
   - Análisis en segundo plano.

     1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
     2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

        Se abre la ventana de propiedades de la directiva.
     3. Seleccione la pestaña **Configuración de la aplicación**.
     4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.
     5. Active la opción **Managed Detection and Response ACTIVADO**.
     6. Guarde los cambios.

     1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
     2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
     3. En la ventana de la directiva, seleccione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
     4. Seleccione la casilla **Managed Detection and Response (Industrial CyberSecurity)**.
     5. Guarde los cambios.

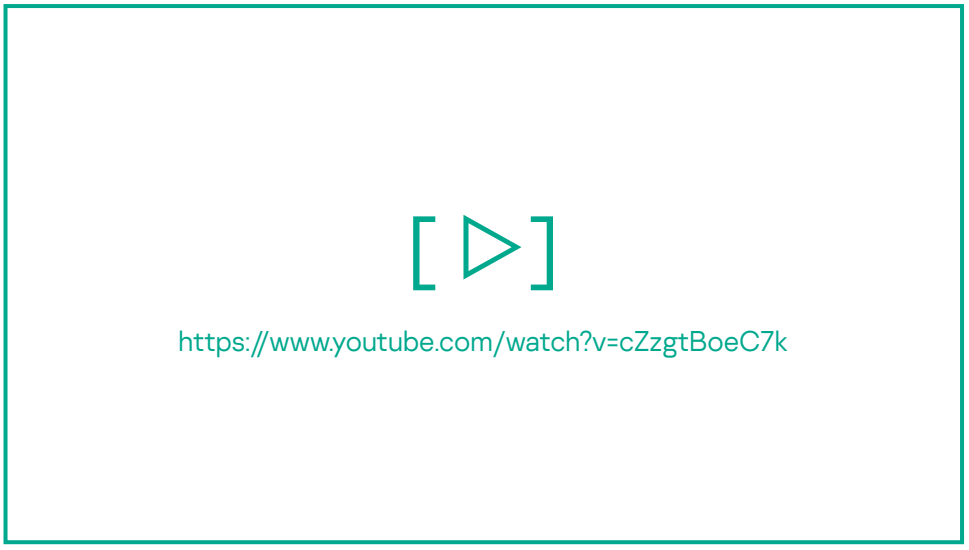
Integración de EDR Agent con EDR (KATA)

EDR Agent se instala en estaciones de trabajo y servidores en la infraestructura de TI de la organización. En estos equipos, EDR Agent supervisa continuamente procesos, conexiones de red abiertas y archivos que se modifican, y envía datos de supervisión al servidor con el componente de Central Node.

Para integrarse con EDR (KATA), debe añadir el componente Endpoint Detection and Response (KATA) y configurar EDR Agent.

Se deben cumplir con las siguientes condiciones para que Endpoint Detection and Response (KATA) funcione:

- Kaspersky Anti Targeted Attack Platform versiones 5.0-7.1.
- Kaspersky Security Center versión 14.2 o superior. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Endpoint Detection and Response (KATA).



https://www.youtube.com/watch?v=cZzgtBoeC7k

El proceso de integración con Endpoint Detection and Response (KATA) incluye los siguientes pasos:

1. **Activar Endpoint Detection and Response (KATA)**

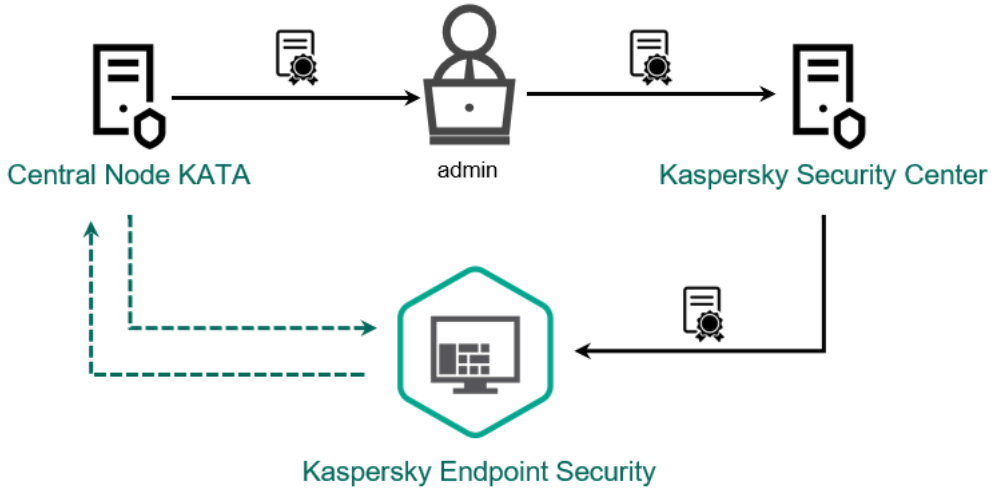
   Debe comprar una licencia separada para EDR (KATA) (complemento de Kaspersky Endpoint Detection and Response (KATA).

   La funcionalidad está disponible tras añadir una clave diferente para Kaspersky Endpoint Detection and Response (KATA). La licencia para la funcionalidad independiente de Endpoint Detection and Response (KATA) es la misma licencia que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad EDR (KATA) esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

2. **Conexión al Central Node**

Kaspersky Anti Targeted Attack Platform requiere establecer una conexión de confianza entre Kaspersky Endpoint Security y el componente de Central Node. Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). A continuación, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).



Agregar un certificado TLS a Kaspersky Endpoint Security

De manera predeterminada, Kaspersky Endpoint Security solo verifica el certificado TLS de Central Node. Para que la conexión sea más segura, también puede habilitar la verificación del equipo en Central Node (autenticación bidireccional). Para activar esta verificación, debe activar la autenticación bidireccional en la configuración de Central Node y Kaspersky Endpoint Security. Para usar la autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

Cómo conectar un equipo con Kaspersky Endpoint Security al Central Node mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Seleccione la casilla **Endpoint Detection and Response Expert (on-premises)**.
6. Haga clic en **Configuración de conexión a servidor**.
7. Configure la conexión del servidor:
   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente.
   - **Certificado TLS del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

- **Utilizar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

  El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

8. Haga clic en **Correcto**.
9. Agregar servidores de Central Node. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

   Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.
10. Si es necesario, configure la telemetría.
11. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo conectar un equipo con Kaspersky Endpoint Security al Central Node mediante Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.
5. Active la opción **Endpoint Detection and Response Expert (on-premises) activado**.
6. Para configurar EDR (KATA), seleccione **Endpoint Detection and Response Expert (versión 7.1 o anterior)** en la lista de soluciones.
7. Haga clic en **Configuración de conexión**.
8. Configure la conexión del servidor:

   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente.
   - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

- **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

  El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

9. Haga clic en **Aceptar**.
10. Agregar servidores de Central Node. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

    Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.
11. Si es necesario, configure la telemetría.
12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Como resultado, el equipo se agrega a la consola de Kaspersky Anti Targeted Attack Platform. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (on-premises)** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Integración de EDR Agent con NDR (KATA)

EDR Agent se instala en estaciones de trabajo y servidores en la infraestructura de TI de la organización. En estos equipos, EDR Agent supervisa continuamente procesos, conexiones de red abiertas y archivos que se modifican, y envía datos de supervisión al servidor con el componente de Central Node.

Para integrarse con NDR (KATA), debe añadir el componente Network Detection and Response (KATA) y configurar EDR Agent.

Se deben cumplir con las siguientes condiciones para que Network Detection and Response (KATA) funcione:

- Kaspersky Anti Targeted Attack Platform versión 7.0 o superior.
- Kaspersky Security Center versión 14.2 o superior. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Network Detection and Response (KATA).

https://www.youtube.com/watch?v=gd-rySv0ThQ

El proceso de integración con Network Detection and Response (KATA) incluye los siguientes pasos:

1. **Activar Network Detection and Response (KATA)**

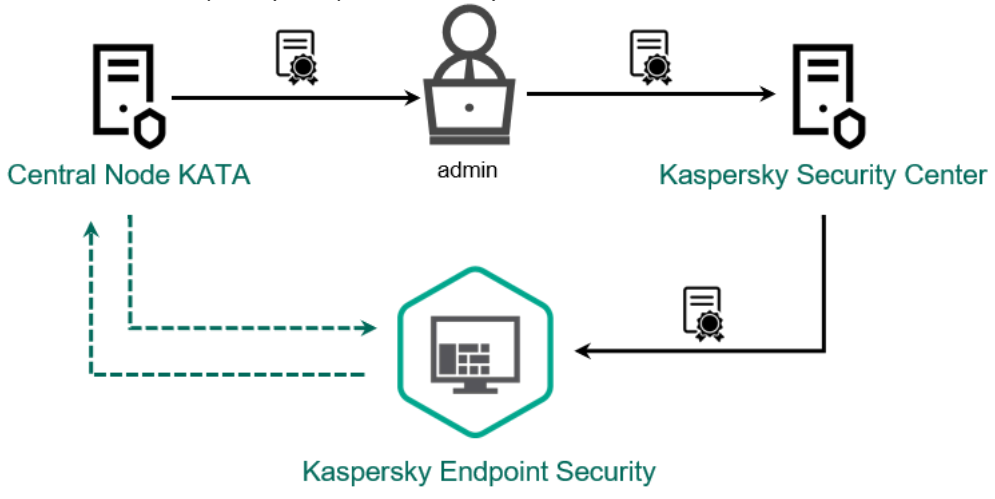
   Debe comprar una licencia separada para NDR (KATA) (complemento de Kaspersky Network Detection and Response (KATA).

   La funcionalidad está disponible tras añadir una clave diferente para Kaspersky Network Detection and Response (KATA). La licencia para la funcionalidad independiente de Network Detection and Response (KATA) es la misma licencia que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad NDR (KATA) esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

2. **Conexión al Central Node**

   Kaspersky Anti Targeted Attack Platform requiere establecer una conexión de confianza entre Kaspersky Endpoint Security y el componente de Central Node. Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). A continuación, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).



Agregar un certificado TLS a Kaspersky Endpoint Security

De manera predeterminada, Kaspersky Endpoint Security solo verifica el certificado TLS de Central Node. Para que la conexión sea más segura, también puede habilitar la verificación del equipo en Central Node (autenticación bidireccional). Para activar esta verificación, debe activar la autenticación bidireccional en la configuración de Central Node y Kaspersky Endpoint Security. Para usar la autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

Cómo conectar un equipo con Kaspersky Endpoint Security al Central Node mediante la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Detection and Response → Network Detection and Response (KATA)**.
4. Seleccione la casilla **Network Detection and Response (KATA)**.
5. Haga clic en **Configuración de conexión**.
6. Configure la conexión del servidor:
   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente.
   - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).
   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
7. Haga clic en **Aceptar**.
8. Agregar servidores de Central Node. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.
9. Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

10. Si es necesario, configure la telemetría.

11. Guarde los cambios.

Cómo conectar un equipo con Kaspersky Endpoint Security al Central Node mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Network Detection and Response (KATA)**.

5. Active la opción **Network Detection and Response (KATA) ACTIVADO**.

6. Haga clic en **Configuración de conexión**.

7. Configure la conexión del servidor:

   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente.

   - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

8. Haga clic en **Aceptar**.

9. Agregar servidores de Central Node. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

10. Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

11. Si es necesario, configure la telemetría.

12. Guarde los cambios.

Como resultado, el equipo se agrega a la consola de Kaspersky Anti Targeted Attack Platform. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Network Detection and Response (KATA)** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Integración de EDR Agent con EDR Expert (on-premises)

EDR Agent se instala en estaciones de trabajo y servidores en la infraestructura de TI de la organización. En estos equipos, EDR Agent supervisa continuamente procesos, conexiones de red abiertas y archivos que se modifican, y envía datos de supervisión al servidor con de EDR Expert (on-premises).

Para integrarse con EDR Expert (on-premises), debe añadir el componente Endpoint Detection and Response Expert (on-premises) y configurar EDR Agent.

El proceso de integración con Endpoint Detection and Response Expert (on-premises) incluye los siguientes pasos:

1. **Activar Endpoint Detection and Response Expert (on-premises)**

   Debe comprar una licencia separada para EDR Expert (on-premises) (complemento de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La funcionalidad está disponible tras añadir una clave diferente para Kaspersky Endpoint Detection and Response Expert (on-premises). La licencia para la funcionalidad independiente de Endpoint Detection and Response Expert (on-premises) es la misma que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad EDR Expert (on-premises) esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

2. **Conexión al servidor de recopilación de telemetría y al servidor de respuesta**

   Kaspersky Endpoint Detection and Response Expert (on-premises) requiere una conexión de confianza entre Kaspersky Endpoint Security y dos servidores:

   - Un *servidor de recopilación de telemetría* es un servidor que es parte de una solución SIEM que recopila, normaliza, correlaciona, analiza y almacena información sobre eventos que ocurren en el equipo.
   - A *servidor de respuesta* es un servidor para recibir y analizar datos, estudiar el comportamiento de los objetos y publicar los resultados de dichos estudios.

   Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). A continuación, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).

   De manera predeterminada, Kaspersky Endpoint Security solo verifica el certificado TLS de los servidores. Para que la conexión sea más segura, también puede habilitar la verificación del equipo en el servidor (autenticación bidireccional). Para activar esta verificación, debe activar la autenticación bidireccional en la configuración del servidor y Kaspersky Endpoint Security. Para usar la autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).

Cómo conectar un equipo con Kaspersky Endpoint Security a EDR Expert (on-premises) mediante Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response Expert (on-premises)**.
5. Active la opción **Endpoint Detection and Response Expert (on-premises) activado**.
6. Para configurar EDR Expert (on-premises), seleccione **Endpoint Detection and Response Expert (versión 8.0 o posterior)** en la lista de soluciones.
7. Configure la conexión de los *servidores de recopilación de telemetría*:

   a. En el bloque **Conexión a servidores de recogida de telemetría**, haga clic en el enlace **Configuración de conexión**.

   b. Configure la conexión de los servidores de recopilación de telemetría:

   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente.
   - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Tras configurar el servidor, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

d. Agregue servidores de recopilación de telemetría. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

Puede añadir varias direcciones de servidores de recopilación de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

e. Si es necesario, configure la telemetría.

8. Configure la conexión de los *servidores de respuesta*:

a. En el bloque **Conexión a servidores de respuesta**, configure el ajuste **Enviar solicitud de sincronización al servidor cada (min.)**. Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security recibe tareas de respuesta ante amenazas y envía los resultados de la tarea.

b. Haga clic en el enlace **Configuración de conexión**.

c. Configure la conexión con los servidores de respuesta:

- **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente.
- **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Tras configurar el servidor, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

  El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

d. Haga clic en **Aceptar**.

e. Añada servidores de respuesta. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

Puede añadir varias direcciones de servidor de respuesta. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Como resultado, el equipo se agrega a la plataforma abierta de administración única (OSMP). Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (on-premises)** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Compatibilidad con aplicaciones EPP de terceros

EDR Agent admite la funcionalidad de las soluciones de Kaspersky Detection and Response. Los componentes de protección y control no están disponibles para EDR Agent. Esta configuración permite instalar aplicaciones EPP de terceros e implementar soluciones de Kaspersky Detection and Response en la infraestructura de la organización.

EDR Agent es compatible con aplicaciones EPP de los siguientes proveedores:

- **Dr.Web**

  EDR Agent es compatible con Dr.Web Agent for Windows versión 13 y Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent es compatible con Dallas Lock 8.0-C versión 843.2.

  Para que EDR Agent se ejecute en un equipo que tenga instalado el software Dallas Lock, debe permitir la conexión a servicios externos de Kaspersky en la configuración del módulo Firewall.

- **Secret Net Studio**

  EDR Agent es compatible con Secret Net Studio versión 8.11 (20851).

  La aplicación no se puede instalar en un equipo donde se implementa Secret Net Studio con el componente antivirus. Para que la interoperabilidad sea posible, debe eliminar el componente antivirus de Secret Net Studio.

- **Trend Micro**

  EDR Agent es compatible con Trend Micro Vision One (incluida la versión 14.0.20731 de Security Agent).

  EDR Agent es compatible con Trend Micro Deep Security versión 20.0.3-18160 (incluido Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent es compatible con Sophos Intercept X versión 2024.1.2 (incluido Endpoint Agent) y Sophos Core Agent versión 2026.2.1.3.

- **Bitdefender**

  EDR Agent es compatible con Bitdefender Endpoint Security Tools versión 8.26.7.647.

- **ESET**

  EDR Agent es compatible con ESET Endpoint Security versión 13.0.2044.0 y ESET Management Agent versión 13.2.1189.0.

En equipos que ejecutan Windows 11 para Arm64, EDR Agent no es compatible con Bitdefender Endpoint Security Tools.

Las aplicaciones deben instalarse en el siguiente orden: primero, instale la aplicación EPP; a continuación, el Agente de red de Kaspersky Security Center; y luego, EDR Agent. Esto es necesario porque el instalador de la aplicación EPP puede detectar EDR Agent y el Agente de red como software incompatible y eliminarlos. El funcionamiento de EDR Agent y del Agente de red también debe verificarse después de actualizar la aplicación EPP de terceros, ya que su instalador puede volver a analizar el equipo en busca de software incompatible y eliminar las aplicaciones.

Si no ha podido instalar EDR Agent en un equipo con una aplicación EPP de terceros porque el instalador encontró software incompatible en el equipo, puede omitir la verificación de software incompatible.

Managed Detection and Response



Kaspersky Endpoint Security para Windows admite la integración con la solución Managed Detection and Response. La solución *Kaspersky Managed Detection and Response (MDR)* detecta y analiza automáticamente los incidentes de seguridad en su infraestructura. Para hacerlo, MDR utiliza datos de telemetría recibidos de endpoints y aprendizaje automático. MDR envía datos de incidentes a los expertos de Kaspersky. Luego, los expertos pueden procesar el incidente y, por ejemplo, añadir una nueva entrada a las bases de datos antivirus. De manera alternativa, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener información detallada sobre cómo funciona la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Configuraciones de Kaspersky Endpoint Security para integración con MDR

Las siguientes configuraciones se pueden utilizar para trabajar con MDR:

- **[KES+agente integrado]**. En esta configuración, Kaspersky Endpoint Security actúa como la aplicación que garantiza la seguridad del equipo y como la aplicación para trabajar con MDR.
- **[EPP de terceros +EDR Agent]**. En esta configuración, la seguridad de la infraestructura de TI la proporciona la aplicación Endpoint Protection Plataform (EPP) de terceros. La interacción con MDR la proporciona Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent (EDR Agent). En esta configuración, EDR Agent es compatible con aplicaciones EPP de terceros.

Integración del agente integrado con MDR

Para configurar la integración con Kaspersky Managed Detection and Response, debe activar el componente Managed Detection and Response y configurar Kaspersky Endpoint Security.

Para que Kaspersky Managed Detection and Response funcione con el Servidor de administración a través de Kaspersky Security Center Web Console, debe establecer una conexión nueva y segura, una *conexión en segundo plano*. Kaspersky Managed Detection and Response le solicita que establezca una conexión en segundo plano cuando despliega la solución. Asegúrese de que la conexión en segundo plano esté establecida.

Establecer una conexión en segundo plano en Web Console

1. En la ventana principal de Web Console, seleccione **Configuración → Integración**.
2. Vaya a la sección **Integración**.
3. Active la opción **Conexión en segundo plano para la integración Activada**.
4. Guarde los cambios.

La integración con Kaspersky Managed Detection and Response consta de los siguientes pasos:

1. **Instalar el componente Managed Detection and Response**

   Puede seleccionar el componente MDR durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

   > Para instalar el componente Managed Detection and Response sin reiniciar el equipo mediante la tarea *Cambiar componentes de la aplicación*, debe desactivar la opción **Comprobar si existen aplicaciones de terceros incompatibles** en la configuración de la tarea.

2. **Configuración de Kaspersky Private Security Network**

   > Omita este paso si utiliza Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configura automáticamente Kaspersky Private Security Network al instalar el complemento MDR.

   Kaspersky Private Security Network (KPSN) es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos.

   Cargue el archivo de configuración de Kaspersky Security Network en las propiedades del Servidor de administración. El archivo de configuración de Kaspersky Security Network se encuentra dentro del archivo comprimido ZIP del archivo de configuración de MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener detalles sobre la configuración de Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center. También puede cargar un archivo de configuración de Kaspersky Security Network en el equipo desde la línea de comandos (consulte las instrucciones a continuación).

   Cómo configurar Kaspersky Private Security Network desde la línea de comandos

   1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
   2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
   3. Ejecute el siguiente comando:

      ```
      avp.com KSN /private <file name>
      ```

      donde `<file name>` es el nombre del archivo de configuración que contiene la configuración de Kaspersky Private Security Network (formato de archivo PKCS7 o PEM).

Ejemplo:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Como resultado, Kaspersky Endpoint Security utilizará Kaspersky Private Security Network para determinar la reputación de archivos, aplicaciones y sitios web. La sección **Kaspersky Security Network** de la configuración de la directiva mostrará el siguiente estado operativo: *Infraestructura: Kaspersky Private Security Network*.

Debe activar el modo de KSN ampliado para que funcione Managed Detection and Response.

3 Activar Kaspersky Managed Detection and Response

A partir de Kaspersky Endpoint Security para Windows 12.10, para activar la función Managed Detection and Response, como alternativa a una código de activación, también puede utilizar un archivo clave.

Kaspersky Managed Detection and Response admite los siguientes métodos de licencia:

- La funcionalidad de Managed Detection and Response está incluida en la licencia de Kaspersky Endpoint Security para Windows.

  La funcionalidad estará disponible inmediatamente después de la activación de Kaspersky Endpoint Security para Windows.

- Se usa una licencia de MDR (complemento de Kaspersky Managed Detection and Response) independiente.

  La funcionalidad estará disponible tras añadir una clave diferente para el complemento de Kaspersky Managed Detection and Response. Como resultado, se añaden dos claves en el equipo: una para Kaspersky Endpoint Security y otra para Kaspersky Managed Detection and Response.

  La licencia para la funcionalidad independiente de Managed Detection and Response es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad MDR esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

4 Activación del componente Managed Detection and Response

Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (consulte las instrucciones a continuación). El archivo BLOB contiene el ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra dentro del archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener información detallada sobre un archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

A partir de Kaspersky Endpoint Security 12.6 para Windows, añadir un archivo BLOB es opcional para Kaspersky Managed Detection and Response sin inquilinos si tiene una licencia actual.

Cómo activar el componente Managed Detection and Response en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Seleccione la casilla **Managed Detection and Response (Industrial CyberSecurity)**.

5. En el bloque **Configuración**, haga clic en **Cargar** y seleccione el archivo BLOB recibido en Kaspersky Managed Detection and Response Console. El archivo tiene la extensión P7.

   De forma predeterminada, el usuario puede administrar la configuración de la aplicación ("candado" abierto). Para aplicar la directiva en equipos, cierre los candados .

6. Guarde los cambios.

Cómo activar el componente Managed Detection and Response en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.
5. Active la opción **Managed Detection and Response ACTIVADO**.
6. Haga clic en **Cargar** y seleccione el archivo BLOB que se obtuvo en Kaspersky Managed Detection and Response Console. El archivo tiene la extensión P7.

   De forma predeterminada, el usuario puede administrar la configuración de la directiva ("candado" abierto). Para aplicar la directiva en equipos, cierre los candados .

7. Guarde los cambios.

Cómo activar el componente Managed Detection and Response desde la línea de comandos

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Configurar parámetros de la aplicación**.

Como resultado, Kaspersky Endpoint Security realizará una comprobación del archivo BLOB. La verificación del archivo BLOB incluye la verificación de la firma digital y el período de licencia. Si el archivo BLOB se verifica correctamente, Kaspersky Endpoint Security descargará el archivo y lo enviará al equipo durante la próxima sincronización con Kaspersky Security Center. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en informes de la interfaz local de Kaspersky Endpoint Security. El componente **Managed Detection and Response** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

5 Configurar otros componentes de la aplicación para recibir telemetría

Debe activar los siguientes componentes para que Managed Detection and Response funcione:

- Kaspersky Security Network (modo ampliado).
- Detección de comportamiento.
- Prevención de exploits.
- Protección frente a amenazas web.
- Protección frente a amenazas en el correo.
- Protección frente a amenazas en archivos.
- Protección frente a amenazas en la red.
- Firewall.
- Protección AMSI.
- Análisis en segundo plano.

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.
5. Active la opción **Managed Detection and Response ACTIVADO**.
6. Guarde los cambios.

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Seleccione la casilla **Managed Detection and Response (Industrial CyberSecurity)**.
5. Guarde los cambios.

Guía de migración de KEA a KES para MDR

Kaspersky Endpoint Security para Windows incluye un agente integrado para la solución Kaspersky Managed Detection and Response. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con MDR. Kaspersky Endpoint Security realizará todas las funciones de Kaspersky Endpoint Agent.

Al desplegar Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Managed Detection and Response seguirá funcionando con Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 11.6.0 o superior.

Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar ambas aplicaciones en el mismo equipo.

Las siguientes condiciones se deben cumplir para que Kaspersky Endpoint Security funcione como parte de Kaspersky Managed Detection and Response:

- Kaspersky Security Center versión 13.2 o superior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Managed Detection and Response.
- Se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Para que MDR funcione con el Servidor de administración mediante Kaspersky Security Center Web Console, debe establecer una nueva conexión segura, una *conexión en segundo plano*.

Pasos para migrar la configuración de [KES+KEA] a [KES+agente integrado] para MDR

1. **Actualizar el Complemento de administración de Kaspersky Endpoint Security**

   El componente MDR se puede administrar con el Complemento de administración de Kaspersky Endpoint Security, versión 11.6 o superior. Según el tipo de consola de Kaspersky Security Center que esté utilizando, actualice el complemento de administración en la Consola de administración (MMC) o el complemento web en Web Console.

2. **Migrar directivas y tareas**

   Transfiera la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows. Están disponibles los siguientes opciones:

   - Un asistente para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Un asistente para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security solo funciona en Web Console.

     Cómo migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console

     En la ventana principal de Web Console, seleccione **Operaciones → Migración desde Kaspersky Endpoint Agent**.

     Esto ejecuta el asistente de migración de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Migración de directivas

El Asistente de migración crea una directiva nueva que combina las configuraciones de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee unir con la directiva de Kaspersky Endpoint Security. Haga clic en una directiva de Kaspersky Endpoint Agent para seleccionar la directiva de Kaspersky Endpoint Security con la que desea unir la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de tareas

El asistente de migración no admite tareas de MDR. Omita este paso.

Paso 3: Fin del asistente

Finalice el asistente. Como resultado del asistente, se creará una nueva directiva de Kaspersky Endpoint Security. La directiva une la configuración de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. La directiva se denomina *<nombre de la directiva de Kaspersky Endpoint Security> y <nombre de la directiva de Kaspersky Endpoint Agent>*. La directiva nueva tiene el estado *Inactiva*. Para continuar, cambie los estados de las directivas de Kaspersky Endpoint Agent y Kaspersky Endpoint Security a *Inactiva* y active la directiva nueva y combinada.

- Un asistente de conversión por lotes de directivas y tareas estándar. El asistente de conversión por lotes de directivas y tareas solo está disponible en la Consola de administración (MMC). Para obtener más detalles sobre el asistente de conversión por lotes de directivas y tareas, consulte la Ayuda de Kaspersky Security Center.

3. **Licencia de la funcionalidad MDR**

   Para activar Kaspersky Endpoint Security como parte de la solución Kaspersky Managed Detection and Response, necesita una licencia independiente para el complemento Kaspersky Managed Detection and Response. Puede añadir la clave con la tarea *Añadir clave*. Como resultado, se añadirán dos claves a la aplicación: *Kaspersky Endpoint Security* y *Kaspersky Managed Detection and Response*.

4. **Instalar o actualizar la aplicación Kaspersky Endpoint Security**

   Para migrar la funcionalidad MDR durante la instalación o actualización de una aplicación, se recomienda utilizar la tarea de instalación remota. Al crear una tarea de instalación remota, debe seleccionar el componente MDR en la configuración del paquete de instalación.

   También puede actualizar la aplicación con los siguientes métodos:

   - Usar el servicio de actualización de Kaspersky.
   - De forma local, utilizando el Asistente de instalación.

   Kaspersky Endpoint Security admite la selección automática de componentes al actualizar la aplicación en un equipo con la aplicación Kaspersky Endpoint Agent instalada. La selección automática de componentes depende de los permisos de la cuenta de usuario que está actualizando la aplicación.

   Si está actualizando Kaspersky Endpoint Security con el archivo EXE o MSI en la cuenta del sistema (SYSTEM), Kaspersky Endpoint Security obtiene acceso a las licencias actuales de las soluciones de Kaspersky. Por lo tanto, si el equipo tiene Kaspersky Endpoint Agent instalado y la solución MDR activada, el instalador de Kaspersky Endpoint Security configura automáticamente el conjunto de componentes y selecciona el componente MDR. Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina Kaspersky Endpoint Agent. La ejecución del instalador MSI con la cuenta del sistema (SYSTEM) se realiza normalmente cuando se actualiza a través del servicio de actualización de Kaspersky o cuando se despliega un paquete de instalación a través de Kaspersky Security Center.

   Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tendrá acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes basándose en un conjunto de componentes de Kaspersky Endpoint Agent. Tras esto, Kaspersky Endpoint Security pasa a utilizar el agente integrado y elimina Kaspersky Endpoint Agent.

Kaspersky Endpoint Security admite la actualización sin reiniciar el equipo. Puede seleccionar el modo de actualización de la aplicación en las propiedades de la directiva.

5. **Comprobación del funcionamiento de la aplicación**

   Si, tras instalar o actualizar la aplicación, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

   - Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.
   - Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, asegúrese de haber activado la funcionalidad de agente integrado.
   - Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

Endpoint Detection and Response

Kaspersky Endpoint Security para Windows incluye un agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante también "EDR Optimum"). A partir de la versión 11.8.0, Kaspersky Endpoint Security para Windows incluye un agente integrado para la solución Kaspersky Endpoint Detection and Response Expert (en adelante también "EDR Expert"). *Kaspersky Endpoint Detection and Response* es una variedad de soluciones para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de las soluciones combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware y ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre las soluciones, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

Herramientas de Inteligencia contra amenazas

Kaspersky Endpoint Detection and Response utiliza las siguientes herramientas Threat Intelligence:

- Integración con Kaspersky Threat Intelligence Portal, que contiene y muestra información sobre la reputación de los archivos y las direcciones web.
- Base de datos de amenazas de Kaspersky.
- La infraestructura de servicios de nube de Kaspersky Security Network (en lo sucesivo también denominada "KSN"), que proporciona acceso a información de reputación de software, sitios web y archivos en tiempo real de la base de conocimientos de Kaspersky. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de las aplicaciones de Kaspersky ante amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos.
- Tecnología Sandbox en la nube que le permite ejecutar archivos detectados en un entorno aislado y comprobar su reputación.

Principio de funcionamiento de la solución

Kaspersky Endpoint Detection and Response examina y analiza el desarrollo de amenazas e informa al *personal de seguridad* o al *Administrador* del posible ataque, para permitir una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana separada. Una *alerta* es un evento en la infraestructura de TI corporativa que la aplicación ha identificado como inusual o sospechoso, y que puede suponer una amenaza para la seguridad de dicha infraestructura. *Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

Compatibilidad con versiones anteriores de Kaspersky Endpoint Security

Si utiliza Kaspersky Endpoint Security 11.2.0–11.6.0 para la interoperabilidad con Kaspersky Endpoint Detection and Response Optimum, la aplicación incluye Kaspersky Endpoint Agent. Puede instalar Kaspersky Endpoint Agent junto con Kaspersky Endpoint Security. En Kaspersky Endpoint Security 11.9.0, el paquete de distribución de Kaspersky Endpoint Agent ya no forma parte del kit de distribución de Kaspersky Endpoint Security.

La solución Kaspersky Endpoint Detection and Response Expert no admite la interoperabilidad con Kaspersky Endpoint Agent. La solución Kaspersky Endpoint Detection and Response Expert usa Kaspersky Endpoint Security con un agente integrado (versión 11.8.0 o posteriores).

Integración del agente integrado con EDR Optimum/EDR Expert

Para configurar la integración con Kaspersky Managed Detection and Response, debe añadir el componente Endpoint Detection and Response Optimum o el componente Endpoint Detection and Response Expert (cloud) y configurar Kaspersky Endpoint Security.

Los componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) y Endpoint Detection and Response Expert (on-premises) no son compatibles entre sí.

Se deben cumplir con las siguientes condiciones para que Endpoint Detection and Response funcione:

- Kaspersky Security Center versión 13.2 o superior. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Endpoint Detection and Response.
- Complemento de administración de Kaspersky Endpoint Detection and Response.

  A partir de la versión 12.6 de Kaspersky Endpoint Security, la visualización de los detalles de la alerta se ha movido del complemento de administración de Kaspersky Endpoint Security al complemento de administración de EDR. El complemento de administración de EDR es un complemento único para trabajar con agentes en los sistemas operativos Windows, Mac y Linux. Ahora, al trabajar con EDR Optimum, necesitará el complemento de administración de Kaspersky Endpoint Security para crear tareas de respuesta a amenazas y el complemento de administración de EDR para ver los detalles de la alerta.

- El componente Endpoint Detection and Response Optimum, como parte de Kaspersky Endpoint Security, admite la interacción con la solución Kaspersky Endpoint Detection and Response Optimum 2.0. La interacción con Kaspersky Endpoint Detection and Response Optimum versión 1.0 no es compatible.
- EDR Optimum se puede administrar en Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console.

  EDR Expert solo se puede administrar mediante Kaspersky Security Center Cloud Console. No puede administrar esta funcionalidad mediante el uso de la Consola de administración (MMC).
- La aplicación está activada y la funcionalidad se incluye en la licencia.
- El componente Endpoint Detection and Response está activado.
- Los componentes de la aplicación de los que depende Endpoint Detection and Response están activados y en funcionamiento. Endpoint Detection and Response depende de los siguientes componentes:
  - Protección frente a amenazas en archivos.
  - Protección frente a amenazas web.
  - Protección frente a amenazas en el correo.
  - Prevención de exploits.
  - Detección de comportamiento.
  - Prevención de intrusiones en el host.
  - Motor de reparación.
  - Control de anomalías adaptativo.

El proceso de integración con Kaspersky Endpoint Detection and Response incluye los siguientes pasos:

1. **Instalar los componentes de Endpoint Detection and Response**

   Puede seleccionar el componente Endpoint Detection and Response Optimum o el componente Endpoint Detection and Response Expert (cloud) durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

   > Debe reiniciar el equipo para terminar de actualizar la aplicación con los componentes nuevos.

2. **Activar Kaspersky Endpoint Detection and Response**

   Puede comprar una licencia para uso de Kaspersky Endpoint Detection and Response de las siguientes maneras:

   - La funcionalidad de Endpoint Detection and Response está incluida en la licencia de Kaspersky Endpoint Security para Windows.

     La funcionalidad estará disponible inmediatamente después de la activación de Kaspersky Endpoint Security para Windows.

- Comprar una licencia separada para EDR Optimum o EDR Expert (complemento de Kaspersky Endpoint Detection and Response).

  La funcionalidad está disponible tras añadir una clave diferente para Kaspersky Endpoint Detection and Response. Como resultado, se añaden dos claves en el equipo: una para Kaspersky Endpoint Security y otra para Kaspersky Endpoint Detection and Response.

  La licencia para la funcionalidad independiente de Endpoint Detection and Response es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad EDR Optimum o EDR Expert esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

Para obtener más información sobre el Contrato de licencia de usuario final de EDR Optimum, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

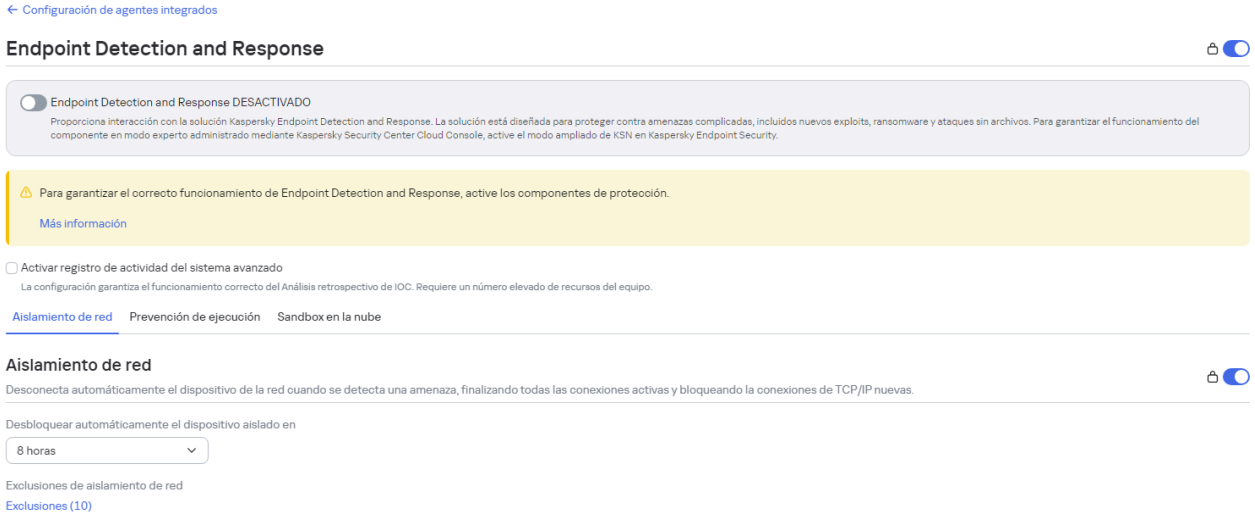
3 Activación de los componentes de Endpoint Detection and Response

Puede activar o desactivar el componente en la configuración de directivas de Kaspersky Endpoint Security para Windows.

Cómo activar o desactivar el componente Endpoint Detection and Response en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Active la opción **Endpoint Detection and Response ACTIVADO**.
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.



Configuración de la integración de EDR

El componente Kaspersky Endpoint Detection and Response está activado. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Optimum** o **Endpoint Detection and Response Expert (cloud)** se añade a la lista de componentes de Kaspersky Endpoint Security.

4 Activar la transferencia de datos al Servidor de administración

Para activar todas las funcionalidades de Endpoint Detection and Response, se debe activar la transferencia de los datos de los siguientes tipos de datos:

- Datos de archivos en cuarentena.

  Los datos se requieren para obtener información acerca de los archivos en cuarentena en un equipo a través de Web Console. Por ejemplo, puede descargar un archivo desde la cuarentena para analizarlo en Web Console.

- Datos de la cadena de desarrollo de la amenaza.

  Los datos son necesarios para obtener información en Web Console sobre las amenazas detectadas en un equipo. Puede ver los detalles de la alerta y realizar acciones de respuesta en Web Console.

Cómo activar la transferencia de datos al Servidor de administración en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Integración con KSC**.
5. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el enlace **Configuración avanzada**.
6. En la ventana que se abre, active la casilla:
   - **Acerca de los archivos en Cuarentena**.
   - **Acerca de una cadena de desarrollo de la amenaza**.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Analizar en busca de indicadores de compromiso (tarea estándar)

Un *Indicador de compromiso (IOC)* es un conjunto de datos sobre un objeto o actividad que indica el acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. La tarea de *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta a la amenaza.

Kaspersky Endpoint Security busca indicadores de compromiso utilizando archivos IOC. Los *archivos IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos IOC deben cumplir con el estándar OpenIOC.

Modo de ejecución de tareas Análisis de IOC

Kaspersky Endpoint Detection and Response le permite crear tareas de análisis de IOC estándar para detectar datos en peligro. La *tarea de análisis de IOC estándar* es una tarea grupal o local que se crea y configura manualmente en Web Console. Las tareas se ejecutan mediante archivos IOC preparados por el usuario. Si desea añadir un indicador de compromiso de forma manual, lea los requerimientos para archivos de IOC.

El archivo que puede descargar al hacer clic en el enlace a continuación contiene una tabla con la lista completa de términos de IOC del estándar de OpenIOC.

DESCARGAR EL ARCHIVO IOC_TERMS.XLSX

Kaspersky Endpoint Security también admite tareas de análisis de IOC independientes cuando la aplicación se utiliza como parte de la solución Kaspersky Sandbox.

Creación de archivo de IOC

A partir de Kaspersky Endpoint Security 12.10 para Windows, puede crear archivos de IOC directamente en la configuración de la tarea. Para crear un archivo de IOC, debe preparar un archivo TXT con una lista de indicadores de compromiso. Puede añadir listas de los siguientes objetos como indicadores de compromiso:

- Hash de archivo (MD5 / SHA256).

  La aplicación prepara un archivo de IOC con una cobertura de análisis FileItem/Md5sum o FileItem/Sha256sum.

- Direcciones IP (IPv4, IPv6).

  La aplicación prepara un archivo de IOC con una cobertura de análisis PortItem/RemoteIP.

- Nombres DNS.

  La aplicación prepara un archivo de IOC con una cobertura de análisis DnsEntryItem/RecordName.

Cómo crear un archivo de IOC en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Análisis de IOC**.

   Se abre la ventana propiedades de la tarea. Si es necesario, cree la tarea de **Análisis de IOC**.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Análisis de amenazas**.

5. Haga clic en **Redefinir los archivos IOC**.

6. Esto abre el formulario para crear un archivo de IOC:

   a. En **Origen de archivos de IOC**, seleccione **Generar a partir de archivo**.

   b. Escriba el nombre del archivo de IOC.

   c. Seleccione un archivo TXT con una lista de indicadores de compromiso.

   d. Seleccione el tipo de archivo de IOC: **Nombres de DNS**, **Hashes del archivo**, **Direcciones IP**.

   e. Haga clic en **Cargar**.

   Kaspersky Endpoint Security añade archivos de IOC a la colección de IOC. Si es necesario, puede excluir temporalmente los archivos de IOC de la cobertura de la tarea.

7. Guarde los cambios.

Crear una tarea Análisis de IOC

Puede crear tareas de *Análisis de IOC* manualmente:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

- Utilizar el Asistente de tareas.

La tarea de grupo *Análisis de IOC* no se puede ejecutar si la integración con Kaspersky Endpoint Detection and Response Expert (local) o Kaspersky Endpoint Detection and Response Expert (en la nube) está configurada en los equipos que se van a analizar. En este caso, recomendamos utilizar la acción de respuesta *Análisis de IOC* para buscar indicadores de compromiso. Para obtener más información, consulte la ayuda de Kaspersky Endpoint Detection and Response Expert (local).

Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.

Para crear una tarea Análisis de IOC:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Análisis de IOC**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Ir al paso siguiente.

   De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

   La cuenta del sistema (SYSTEM) no tiene permiso para ejecutar la tarea de *Análisis de IOC* en las unidades de red. Si desea ejecutar la tarea para una unidad de red, seleccione la cuenta de un usuario que tenga acceso a esa unidad.

   Para ejecutar tareas de análisis de IOC independientes en unidades de red, debe elegir manualmente la cuenta de usuario que tiene acceso a esa unidad en las propiedades de la tarea.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. Vaya a la sección **Análisis de amenazas**.

10. Cargue los archivos de IOC para buscar indicadores de compromiso.

    Después de cargar los archivos de IOC, la aplicación muestra información resumida sobre el archivo, incluida la lista de indicadores que no pasaron la comprobación. Después de cargar archivos de IOC, puede editar manualmente los archivos en el editor integrado directamente en las propiedades de la tarea. Kaspersky Endpoint Security admite la edición de archivos de IOC que cumplen con el estándar OpenIOC 1.1. No es posible modificar el contenido de los archivos IOC que cumplan con la versión 1.0 de OpenIOC.

    Kaspersky Endpoint Security añade archivos de IOC a la colección de IOC. Si es necesario, puede excluir temporalmente los archivos de IOC de la cobertura de la tarea.

    No se recomienda añadir ni eliminar archivos IOC después de ejecutar la tarea. Esto puede hacer que los resultados del análisis de IOC se muestren incorrectamente para ejecuciones anteriores de la tarea. Para buscar indicadores de compromiso por nuevos archivos IOC, se recomienda añadir nuevas tareas.

11. Si es necesario, active la casilla **Análisis Retrospectivo de IOC**. *Análisis de IOC retrospectivo* es un modo de la tarea *Análisis de IOC* en la que Kaspersky Endpoint Security analiza en busca de indicadores de compromiso utilizando datos durante un período de tiempo determinado. Este modo está diseñado para buscar indicadores de compromiso mediante la telemetría del equipo protegido, como la actividad de la red, los procesos, los archivos y otra telemetría. Kaspersky Endpoint Security analiza los datos en los registros del sistema operativo y del navegador en el equipo. El análisis de IOC retrospectivo analiza los registros de los siguientes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versión 79 o posterior).

12. Configure acciones al detectar un IOC:

    - **Aislar el dispositivo de la red**. Si se selecciona esta opción, Kaspersky Endpoint Security aísla el equipo de la red para evitar que la amenaza se propague. Puede configurar la duración del aislamiento en la configuración del componente Endpoint Detection and Response.

      Si esta casilla de verificación está desactivada, puede aislar el equipo de la red después de ejecutar la tarea manualmente. Si la tarea *Análisis de IOC* detecta un IOC, puede aislar el equipo de la red directamente desde el IOC (propiedades de la tarea *Análisis de IOC* → **Configuración de la aplicación** → **Resultados del Análisis de IOC**). Kaspersky Endpoint Security también permite administrar de inmediato configuraciones adicionales: período de desactivación del aislamiento de la red y exclusiones del aislamiento de la red.

    - **Mover la copia a la cuarentena, eliminar objeto**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.

      Si esta casilla de verificación está desactivada, puede poner en cuarentena el archivo manualmente después de ejecutar la tarea manualmente. Si la tarea *Análisis de IOC* detecta un archivo que puede poner en peligro los datos, puede poner en cuarentena este archivo directamente desde los resultados del análisis de IOC (**Configuración de la aplicación** → **Resultados del Análisis de IOC**). Como resultado, Kaspersky Endpoint Security inicia el asistente de creación de tareas con datos preestablecidos del archivo detectado. Solo necesita administrar la configuración de tareas adicional; por ejemplo, configurar la programación de tareas.

      Si es necesario, seleccione la casilla **Aplicar a objetos críticos del sistema**. Los System Critical Objects (SCO) incluyen archivos que el sistema operativo necesita para funcionar.

      > No recomendamos aplicar acciones a los archivos SCO. Esto puede provocar que el sistema operativo se vuelva inestable o no pueda iniciarse.

    - **Ejecutar análisis de áreas críticas**. Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.

13. Vaya a la sección **Avanzado**.

14. Seleccione los tipos de datos (documentos del IOC) que se deben analizar como parte de la tarea.

    > Kaspersky Endpoint Security selecciona tipos de datos (documentos de IOC) de manera automática para la tarea *Análisis de IOC* de acuerdo con el contenido de los archivos de IOC cargados. No se recomienda deseleccionar tipos de datos.

También puede configurar coberturas de análisis para los siguientes tipos de datos:

- **Archivos: FileItem**. Configure una cobertura de análisis de IOC en el equipo mediante coberturas preconfiguradas.

  De forma predeterminada, Kaspersky Endpoint Security analiza en busca de IOC solo en áreas importantes del equipo, como la carpeta de Descargas, el escritorio, la carpeta de archivos temporales del sistema operativo, etc. También puede añadir la cobertura del análisis de forma manual.

- **Registros de eventos de Windows - EventLogItem**. Introduzca el período en el cual se registran los eventos. También puede elegir qué registros de eventos de Windows se deben utilizar para realizar el análisis de IOC. De manera predeterminada, están seleccionados los siguientes registros de eventos: registro de eventos de la aplicación, registro de eventos del sistema y registro de eventos de seguridad.

  > Para el término de IOC EventLogItem\source, use el valor **Nombre del proveedor** del esquema XML del evento.

- **Registro de Windows - RegistryItem**. Configure la cobertura del análisis de IOC en el registro.

  De forma predeterminada, Kaspersky Endpoint Security analiza un grupo de claves de registro.

15. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.

16. Configure la programación de la tarea.

    > Wake-on-LAN no está disponible para esta tarea. Asegúrese de que el equipo esté encendido para ejecutar la tarea.

17. Guarde los cambios.

18. Active la casilla ubicada junto a la tarea.

19. Haga clic en **Iniciar**.

Como resultado, Kaspersky Endpoint Security ejecuta la búsqueda de indicadores de compromiso en el equipo. Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**. Puede ver la información acerca de los indicadores de compromiso detectados en las propiedades de la tarea: **Configuración de la aplicación** → **Resultados del Análisis de IOC**. En los resultados del análisis de IOC, también puede poner en cuarentena el archivo detectado o aislar el equipo de la red.

Kaspersky Endpoint Security busca duplicados entre los registros creados para el mismo archivo IOC y guarda solo registros únicos en los resultados de la tarea. Los duplicados son registros del mismo tipo que tienen los mismos valores de todos los campos comparados. La aplicación tampoco puede crear un registro si carece de un valor en uno o más campos (consulte la tabla a continuación).

Tipo	Campos comparados	Condición para no crear un registro
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Valor que falta en los campos FullPath, Md5sum, Sha256sum. • Valores perdidos del FullPath campo y valores idénticos de los campos Md5sum y Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Valor que falta de al menos uno de los siguientes campos: Hive, KeyPath o ValueName.
ProcessItem	• startTime • PID	Valores que faltan en los campos startTime o PID.

La ventana **Detalles de alerta** puede mostrar registros de RegistryItem con valores de campo idénticos. Dichos registros no son duplicados porque tienen diferentes valores del campo Texto, que no aparece en la interfaz.

Los resultados del análisis de IOC se conservan durante 30 días. Después de dicho período, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

Telemetría ampliada para Análisis de IOC

Recomendamos activar la telemetría ampliada en el equipo para el análisis de IOC retrospectivo. La telemetría ampliada mejora la precisión de la detección de IOC, pero utiliza más recursos del equipo.

La telemetría ampliada incluye el soporte de los siguientes términos adicionales:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem / Creado
- FileItem/Modified
- FileItem/Changed

- FileItem/Accessed
- FileItem/FileAttributes

Si la telemetría ampliada está desactivada, Kaspersky Endpoint Security puede rotar la información sobre los indicadores de compromiso detectados.

Para habilitar la telemetría ampliada:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la casilla **Activar registro de actividad del sistema avanzado**.
6. Guarde los cambios.

Mover archivo a la cuarentena

Al reaccionar ante amenazas, Kaspersky Endpoint Detection and Response puede crear tareas de *Mover archivo a Cuarentena*. Esto es necesario para minimizar las consecuencias de la amenaza. *Cuarentena* es un almacenamiento local especial en el equipo. El usuario puede poner en cuarentena archivos que considere peligrosos para el equipo. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la Cuarentena solo cuando se integra con soluciones de Kaspersky Detection and Response. En otros casos, Kaspersky Endpoint Security coloca el archivo relevante en Copia de seguridad. Para obtener información sobre cómo administrar la cuarentena como parte de las soluciones, consulte la Ayuda de Kaspersky Sandbox, la Ayuda de Kaspersky Endpoint Detection and Response Optimum, la Ayuda de Kaspersky Endpoint Detection and Response Expert, la Ayuda de Kaspersky Anti Targeted Attack Platform y la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises).

Puede crear tareas de *Mover archivo a Cuarentena* de las siguientes formas:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.
- Utilizar el Asistente de tareas.

  Debe introducir la ruta del archivo o el hash (SHA256 o MD5), o tanto la ruta del archivo como el hash del archivo.

- En la configuración de la tarea *Análisis de IOC*.

  Si la tarea *Análisis de IOC* detecta un archivo que puede poner en peligro los datos, puede poner en cuarentena este archivo directamente desde los resultados del análisis de IOC (**Configuración de la aplicación → Resultados del Análisis de IOC**). Como resultado, Kaspersky Endpoint Security inicia el asistente de creación de tareas con datos preestablecidos del archivo detectado. Solo necesita administrar la configuración de tareas adicional; por ejemplo, configurar la programación de tareas.

La tarea *Mover archivo a Cuarentena* tiene las siguientes limitaciones:

1. El tamaño del archivo no debe exceder los 100 MB.
2. No puede eliminar los archivos necesarios para el funcionamiento de Kaspersky Endpoint Security para Windows:
   - Archivos incluidos en el ámbito de la tecnología de Autodefensa de Kaspersky Endpoint Security para Windows
   - Archivos firmados digitalmente por Kaspersky
3. Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.
4. No puede analizar un objeto puesto en cuarentena como resultado de la tarea *Mover archivo a Cuarentena*.

Para crear una tarea Mover archivo a Cuarentena:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.
3. Configure los parámetros de la tarea:
   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.
   b. En la lista desplegable **Tipo de tarea**, seleccione **Mover archivo a Cuarentena**.
   c. En el campo **Nombre de la tarea**, escriba una descripción breve.
   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.
5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

   De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).
6. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. Si es necesario, active la casilla **Aplicar a objetos críticos del sistema**.

   Los System Critical Objects (SCO) incluyen archivos que el sistema operativo necesita para funcionar.

   > No recomendamos aplicar acciones a los archivos SCO. Esto puede provocar que el sistema operativo se vuelva inestable o no pueda iniciarse.

10. En la lista de archivos, haga clic en **Añadir**.

    Se inicia el asistente de adición de archivos.

11. Para añadir el archivo, debe introducir la ruta completa al mismo, o tanto el hash como la ruta.

    > Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se ha encontrado el archivo*.

12. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.

13. Configure la programación de la tarea.

    > Wake-on-LAN no está disponible para esta tarea. Asegúrese de que el equipo esté encendido para ejecutar la tarea.

14. Guarde los cambios.

15. Active la casilla ubicada junto a la tarea.

16. Haga clic en **Iniciar**.

    Como resultado, Kaspersky Endpoint Security mueve el archivo a Cuarentena.

Si el archivo está bloqueado por otro proceso, la tarea se muestra como Listo, pero el archivo en sí se pone en cuarentena solo después de reiniciar el equipo. Después de reiniciar el equipo, confirme que se eliminó el archivo.

Si el archivo está bloqueado por un proceso diferente, la tarea se muestra como *Completada*, pero el archivo en sí se pone en cuarentena solo después de reiniciar el equipo. Después de reiniciar el equipo, confirme que se eliminó el archivo.

La tarea de *Mover archivo a Cuarentena* puede finalizar con el error *Acceso denegado* si está intentando poner en cuarentena un archivo ejecutable que se está ejecutando actualmente. Cree una tarea de terminar proceso para el archivo y vuelva a intentarlo.

La tarea de *Mover archivo a Cuarentena* puede finalizar con el error *No hay espacio suficiente en el almacenamiento de Cuarentena* si está intentando poner en cuarentena un archivo demasiado grande. Vacíe la Cuarentena o aumente el tamaño de la Cuarentena. Luego, vuelva a intentarlo.

Puede restaurar un archivo de la cuarentena o vaciar la cuarentena mediante Web Console. Puede restaurar objetos localmente en el equipo mediante la línea de comandos.

Obtener archivo

Puede obtener archivos de los equipos de los usuarios. Por ejemplo, puede configurar la obtención de un archivo de registro de eventos creado por una aplicación de terceros. Como resultado de la ejecución de la tarea, una copia del archivo se guarda en Cuarentena. *Cuarentena* es un almacenamiento local especial en el equipo. Puede descargar este archivo de la cuarentena a su equipo mediante Web Console (**Operaciones** → **Repositorios** → **Cuarentena**). En el equipo del usuario, el archivo permanece en su carpeta original.

El tamaño del archivo no debe exceder los 2 GB.

Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.

Para crear una tarea Obtener archivo:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Obtener archivo**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

   De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.
9. En la lista de archivos, haga clic en **Añadir**.

   Se inicia el asistente de adición de archivos.
10. Para añadir el archivo, debe introducir la ruta completa al mismo, o tanto el hash como la ruta.

    Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se ha encontrado el archivo*.
11. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.
12. Configure la programación de la tarea.

    Wake-on-LAN no está disponible para esta tarea. Asegúrese de que el equipo esté encendido para ejecutar la tarea.
13. Guarde los cambios.
14. Active la casilla ubicada junto a la tarea.
15. Haga clic en **Iniciar**.

    Como resultado, Kaspersky Endpoint Security crea una copia del archivo y mueve esa copia a la Cuarentena. Puede descargar el archivo de la cuarentena en Web Console.

Eliminar el archivo

Puede eliminar archivos de forma remota mediante la tarea *Eliminar archivo*. Por ejemplo, puede eliminar un archivo de forma remota al responder a amenazas.

No puede eliminar los archivos necesarios para el funcionamiento de Kaspersky Endpoint Security para Windows:

- Archivos incluidos en el ámbito de la tecnología de Autodefensa de Kaspersky Endpoint Security para Windows
- Archivos firmados digitalmente por Kaspersky

Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.

Para crear una tarea Eliminar archivo:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Eliminar archivo**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

   De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. Para añadir el archivo, debe introducir la ruta completa al mismo, o tanto el hash como la ruta.

   Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se ha encontrado el archivo*.

10. Si es necesario, active la casilla **Aplicar a objetos críticos del sistema**.

    Los System Critical Objects (SCO) incluyen archivos que el sistema operativo necesita para funcionar.

    No recomendamos aplicar acciones a los archivos SCO. Esto puede provocar que el sistema operativo se vuelva inestable o no pueda iniciarse.

11. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.

12. Configure la programación de la tarea.

    Wake-on-LAN no está disponible para esta tarea. Asegúrese de que el equipo esté encendido para ejecutar la tarea.

13. Guarde los cambios.

14. Active la casilla ubicada junto a la tarea.

15. Haga clic en **Iniciar**.

    Como resultado, Kaspersky Endpoint Security elimina el archivo del equipo. Si el archivo está bloqueado por un proceso diferente, la tarea se muestra como *Listo*, pero el archivo en sí se elimina solo después de reiniciar el equipo. Después de reiniciar el equipo, confirme que se eliminó el archivo.

La tarea de *Eliminar archivo* puede finalizar con el error *Acceso denegado o no se encuentra el archivo* si está intentando eliminar un archivo ejecutable que se está ejecutando actualmente. Cree una tarea de terminar proceso para el archivo y vuelva a intentarlo.

Inicio del proceso

Puede ejecutar archivos de forma remota utilizando la tarea de *Inicio del proceso*. Por ejemplo, puede ejecutar de forma remota una utilidad que crea el archivo de configuración del equipo. Luego, puede utilizar la tarea *Obtener archivo* para recibir el archivo creado en Kaspersky Security Center Web Console.

Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.

Para crear una tarea Inicio del proceso:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Inicio del proceso**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

   De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.
8. Se abre la ventana propiedades de la tarea.
9. Seleccione la pestaña **Configuración de la aplicación**.
10. Introduzca el comando de inicio del proceso.

    Suponga que desea ejecutar una utilidad (`utility.exe`) que guarda la información sobre la configuración del equipo en un archivo llamado `conf.txt` en la carpeta actual (opción predeterminada): La utilidad está en la carpeta `C:\Users\admin\Diagnostic\`. Debe guardar el archivo de configuración en la carpeta `C:\Users\admin\Documents\Configuration`. Introduzca los siguientes valores:

    - **Comando ejecutable** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Argumentos de la línea de comandos (opcional)** – `/R conf.txt`
    - **Ruta de acceso a la carpeta de trabajo (opcional)** – `C:\Users\admin\Documents\Configuration`
11. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.
12. Configure la programación de la tarea.

    > Wake-on-LAN no está disponible para esta tarea. Asegúrese de que el equipo esté encendido para ejecutar la tarea.

13. Guarde los cambios.
14. Active la casilla ubicada junto a la tarea.
15. Haga clic en **Iniciar**.

    Como resultado, Kaspersky Endpoint Security ejecuta el comando en modo silencioso e inicia el proceso. Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados de la ejecución**.

Terminar proceso

Puede finalizar procesos de forma remota mediante la tarea *Terminar proceso*. Por ejemplo, puede finalizar de forma remota una utilidad de prueba de velocidad de Internet que se inició con la tarea *Ejecutar proceso*.

Si desea prohibir la ejecución de un archivo, puede configurar el componente de Prevención de ejecución. Puede prohibir la ejecución de archivos ejecutables, scripts, archivos de formato Office.

La tarea *Terminar proceso* tiene las siguientes limitaciones:

No puede finalizar los procesos de archivos necesarios para el funcionamiento de Kaspersky Endpoint Security para Windows:

- Archivos incluidos en el ámbito de la tecnología de Autodefensa de Kaspersky Endpoint Security para Windows
- Archivos firmados digitalmente por Kaspersky

Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.

Para crear una tarea Terminar proceso:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Añadir**.

   El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows 14.2**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Terminar proceso**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

   De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

   Se abre la ventana propiedades de la tarea.

8. Seleccione la pestaña **Configuración de la aplicación**.

9. Si es necesario, active la casilla **Aplicar a objetos críticos del sistema**.

   Los System Critical Objects (SCO) incluyen archivos que el sistema operativo necesita para funcionar.

   No recomendamos aplicar acciones a los archivos SCO. Esto puede provocar que el sistema operativo se vuelva inestable o no pueda iniciarse.

10. Para completar el proceso, debe seleccionar el archivo que desea terminar. Puede seleccionar el archivo de una de las siguientes formas:

    - Introduzca el nombre completo del archivo.
    - Introduzca el hash del archivo y la ruta al archivo.
    - Introduzca el PID del proceso (solo para tareas locales).
    - Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se ha encontrado el archivo*.

    Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se ha encontrado el archivo*.

11. En la ventana de propiedades de la tarea, elija la pestaña **Programación**.
12. Configure la programación de la tarea.

    Wake-on-LAN no está disponible para esta tarea. Asegúrese de que el equipo esté encendido para ejecutar la tarea.

13. Haga clic en **Guardar**.
14. Active la casilla ubicada junto a la tarea.
15. Haga clic en **Iniciar**.

    Como resultado, Kaspersky Endpoint Security finaliza el proceso en el equipo. Por ejemplo, si una aplicación GAME está en ejecución y finaliza el proceso game.exe, la aplicación se cierra sin guardar los datos. Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**.

Prevención de ejecución

La prevención de ejecución permite administrar la ejecución de archivos ejecutables y scripts, así como abrir archivos de formato Office. De esta manera, puede, por ejemplo, prevenir la ejecución de aplicaciones que considere inseguras. Como resultado, se puede detener la propagación de la amenaza. La prevención de ejecución es compatible con un conjunto de extensiones de archivos y un conjunto de intérpretes de script.

Regla de prevención de ejecución

La prevención de ejecución administra el acceso de usuarios a archivos con reglas de prevención de ejecución. *Regla de prevención de ejecución* es un conjunto de criterios que la aplicación tiene en cuenta al reaccionar a la ejecución de un objeto, por ejemplo, al bloquear la ejecución de un objeto. La aplicación identifica archivos por sus rutas o sumas de comprobación calculadas mediante algoritmos hash MD5 y SHA256.

Puede crear Reglas de prevención de ejecución:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

- Uso de una directiva de grupo o configuración de la aplicación local.

  Debe introducir la ruta o el hash del archivo (SHA256 o MD5), o bien la ruta de la carpeta y el hash del archivo.

También puede administrar la prevención de ejecución de forma local, mediante la línea de comandos.

Prevención de ejecución tiene las siguientes limitaciones:

1. Las reglas de prevención no incluyen archivos en CD ni imágenes ISO. La aplicación no bloquea la ejecución ni apertura de estos archivos.

2. No puede aplicar una regla de prevención a los archivos necesarios para el funcionamiento de Kaspersky Endpoint Security para Windows:

   - Archivos incluidos en el ámbito de la tecnología de Autodefensa de Kaspersky Endpoint Security para Windows

   - Archivos firmados digitalmente por Kaspersky

3. No se recomienda crear más de 5000 reglas de prevención de ejecución, ya que esto puede provocar inestabilidad en el sistema.

Modos de regla de prevención de ejecución

El componente de prevención de ejecución puede funcionar en dos modos:

- **Statistics only**

  En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de ejecutar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Windows y Kaspersky Security Center, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de forma predeterminada.

- **Active**

  En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Windows y en el registro de eventos de Kaspersky Security Center.

Administración de la prevención de ejecución

Puede configurar los ajustes del componente solo en Web Console.

Para prevenir la ejecución, haga lo siguiente:

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response**.
5. Seleccione la pestaña **Prevención de ejecución**.
6. Active la opción **Prevención de ejecución ACTIVADA**.
7. En el bloque **Acción al ejecutar o abrir un objeto prohibido**, seleccione el modo de funcionamiento del componente:

   - **Bloquear y añadir a registro de eventos**. En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Windows y en el registro de eventos de Kaspersky Security Center.

     Si es necesario, seleccione la casilla **Aplicar a objetos críticos del sistema**. Los System Critical Objects (SCO) incluyen archivos que el sistema operativo necesita para funcionar.

     No recomendamos aplicar acciones a los archivos SCO. Esto puede provocar que el sistema operativo se vuelva inestable o no pueda iniciarse.

   - **Añadir a registro de eventos**. En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de ejecutar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Windows y Kaspersky Security Center, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de forma predeterminada.
8. Crear una lista de reglas de prevención de ejecución:

   a. Haga clic en **Añadir**.

   b. Esto abre una ventana; en esta ventana, introduzca el nombre de la regla de prevención de ejecución (por ejemplo, *Aplicación A*).

   c. En la lista desplegable de **Tipo**, seleccione el objeto de que desee bloquear: **Archivo ejecutable**, **Script**, **Documento de Microsoft Office**.

   Si selecciona un tipo equivocado, Kaspersky Endpoint Security no bloquea el archivo ni el script.

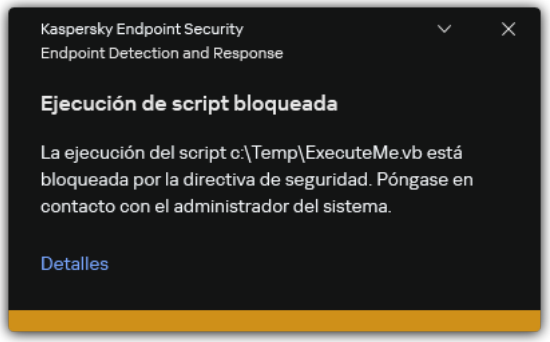
   d. Para añadir el archivo, debe introducir el hash del archivo (SHA256 o MD5), la ruta completa al archivo o el hash y la ruta de la carpeta.

Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, Kaspersky Endpoint Security no bloquea el archivo ni el script.

La prevención de ejecución es compatible con un conjunto de extensiones de archivos y un conjunto de intérpretes de script.

9. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security bloquea la ejecución de objetos: ejecución de archivos ejecutables y scripts, apertura de archivos de formato Office. Sin embargo, puede abrir un archivo de script en un editor de textos, incluso si no se puede ejecutar el script. Cuando se bloquea la ejecución de un objeto, Kaspersky Endpoint Security muestra una notificación estándar (ver la figura a continuación), si las notificaciones están habilitadas en la configuración de la aplicación.



Notificación de prevención de ejecución

Aislamiento de equipos de la red

El aislamiento de red permite aislar de forma automática un equipo de la red en respuesta a la detección de un indicador de compromiso (IOC). Este es el *modo automático*. Puede encender el Aislamiento de red de forma manual mientras investiga la amenaza detectada. Este es el *modo manual*.

Cuando el Aislamiento de red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones de red TCP/IP nuevas en el equipo, excepto las siguientes conexiones:

- Conexiones enumeradas en exclusiones de aislamiento de red.
- Conexiones iniciadas por los servicios de Kaspersky Endpoint Security.
- Conexiones iniciadas por el Agente de red de Kaspersky Security Center.
- Conexiones a la SVM y al Servidor de integración si la aplicación se está utilizando en modo Light Agent.
- Conexiones a KSN al integrar la aplicación con Kaspersky Managed Detection and Response.

Puede configurar los ajustes del componente solo en Web Console.

Modo de aislamiento de red automático

Puede configurar el Aislamiento de red para que se encienda de manera automática en respuesta a una detección de IOC. Puede configurar el modo de aislamiento de red automático con una directiva de grupo.

Cómo configurar el Aislamiento de red para que se encienda de forma automática en respuesta a una detección de IOC

1. En la ventana principal de Web Console, seleccione **Administración de activos → Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Análisis de IOC** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

   Si es necesario, cree la tarea de *Análisis de IOC*.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione la sección **Configuración de respuesta**.

5. En el bloque **Configurar acciones de respuestas al detectar un IOC**, seleccione **Alerta y respuesta** y marque la casilla **Aislar el dispositivo de la red**.

6. Guarde los cambios.

   Como resultado, cuando se detecta un IOC, la aplicación aísla el equipo de la red para prevenir que la amenaza se propague.

Puede configurar la desactivación automática del aislamiento de red tras un periodo determinado. De manera predeterminada, la aplicación apaga el Aislamiento de red cuando transcurren 8 horas desde que se encendió. También puede desactivar el aislamiento de red de forma manual (consulte las instrucciones a continuación). Después de apagar el Aislamiento de red, el equipo puede usar la red sin restricciones.

Cómo configurar el plazo para desactivar el aislamiento de red de un equipo en modo automático

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

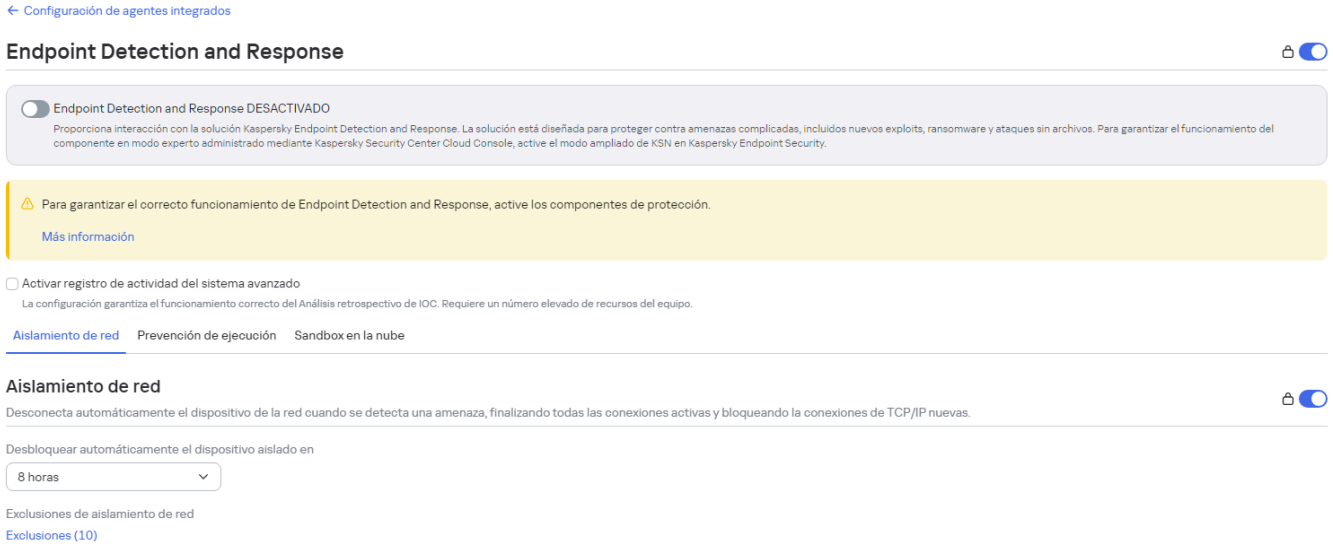
3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response**.

5. Seleccione la pestaña **Aislamiento de red**.

6. Seleccione el retraso para desactivar el aislamiento de la red.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.



Configuración de la integración de EDR

Modo de aislamiento de red manual

Puede encender y apagar el Aislamiento de red de forma manual. Puede configurar el modo de aislamiento de red manual mediante las propiedades del equipo en la consola de Kaspersky Security Center.

Puede encender el Aislamiento de red de la siguiente manera:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

- Uso de los ajustes locales de la aplicación.

- En la configuración de la tarea *Análisis de IOC*.

  Si la tarea *Análisis de IOC* detecta un IOC, puede aislar el equipo de la red directamente desde el IOC (propiedades de la tarea *Análisis de IOC* → **Configuración de la aplicación** → **Resultados del Análisis de IOC**). Kaspersky Endpoint Security también permite administrar de inmediato configuraciones adicionales: período de desactivación del aislamiento de la red y exclusiones del aislamiento de la red.

Cómo encender el Aislamiento de red de un equipo de forma manual

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.

2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.

   Se abren las propiedades del equipo.

3. Seleccione la pestaña **Aplicaciones**.

4. Haga clic en **Kaspersky Endpoint Security para Windows 14.2**.

   Se abre la configuración local de la aplicación.

5. Seleccione la pestaña **Configuración de la aplicación**.
6. Vaya a **Detection and Response → Endpoint Detection and Response**.
7. En el bloque **Aislamiento de red**, haga clic en **Aislar el equipo de la red**.

Puede configurar la desactivación automática del aislamiento de red tras un periodo determinado. De manera predeterminada, la aplicación apaga el Aislamiento de red cuando transcurren 8 horas desde que se encendió. Después de apagar el Aislamiento de red, el equipo puede usar la red sin restricciones.

Cómo configurar el plazo para desactivar el Aislamiento de red de un equipo en modo manual

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.
   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Tareas**.
   Esto mostrará la lista de tareas disponibles en el equipo.
4. Seleccione la tarea **Aislamiento de red**.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Esta acción abre una ventana. En ella, seleccione el plazo para desactivar el Aislamiento de red.
7. Guarde los cambios.

Cómo apagar el Aislamiento de red de un equipo de forma manual

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.
   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows 14.2**.
   Se abre la configuración local de la aplicación.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response**.
7. En el bloque **Aislamiento de red**, haga clic en **Desbloquear el equipo aislado de la red**.

También puede desactivar el Aislamiento de red de forma local mediante la línea de comandos.

A partir de Kaspersky Endpoint Security 12.10 para Windows, puede administrar el aislamiento de red en los detalles de la alerta. Además, en los detalles de la alerta puede especificar el período de tiempo de aislamiento de la red del equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

Exclusiones de aislamiento de red

Puede configurar Exclusiones de aislamiento de red. Las conexiones de red que coinciden con las reglas no se bloquean en el equipo cuando el aislamiento de red está activado.

Para configurar las Exclusiones de aislamiento de red, puede usar una lista de *perfiles de red estándar*. De forma predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones de forma manual (ver las instrucciones a continuación).

Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si el aislamiento de red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center o en los detalles de la alerta.

Una directiva activa no evita que se apliquen exclusiones al Aislamiento de red configurado en las propiedades del equipo, porque estos parámetros tienen situaciones de uso diferentes.

Cómo añadir una exclusión del Aislamiento de red en modo automático

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response**.
5. Seleccione la pestaña **Aislamiento de red**.
6. En el bloque **Exclusiones de aislamiento de red**, haga clic en **Exclusiones**.
7. Esto abre una ventana: aquí debe hacer clic en **Añadir → Añadir desde el perfil** y seleccionar los perfiles de red estándar para configurar las exclusiones.

   Las exclusiones del aislamiento de red desde el perfil se añaden a la lista de Exclusiones de aislamiento de red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de conexiones de red.
8. Si es necesario, añada una Exclusión de aislamiento de red de forma manual. Para hacerlo, en la ventana de la lista de exclusiones, haga clic en **Añadir → Añadir** y modifique la configuración de conexión de red de forma manual.
9. Guarde los cambios.

Cómo añadir una exclusión del Aislamiento de red en modo manual

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.

   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Tareas**.

   Esto mostrará la lista de tareas disponibles en el equipo.
4. Seleccione la tarea **Aislamiento de red**.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Esta acción abre una ventana. En ella, haga clic en **Exclusiones**.
7. Esto abre una ventana: aquí debe hacer clic en **Añadir desde el perfil** y seleccionar los perfiles de red estándar para configurar las exclusiones.

   Las exclusiones del aislamiento de red desde el perfil se añaden a la lista de Exclusiones de aislamiento de red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de conexiones de red.
8. Si es necesario, añada una Exclusión de aislamiento de red de forma manual. Para hacerlo, en la ventana de la lista de exclusiones, haga clic en **Añadir** y modifique la configuración de conexión de red de forma manual.
9. Guarde los cambios.

También puede ver la lista de Exclusiones de aislamiento de red de forma local mediante la línea de comandos. Para usar esta opción, es necesario que el equipo esté aislado.

A partir de Kaspersky Endpoint Security 12.10 para Windows, puede agregar las exclusiones de aislamiento de red en los detalles de la alerta. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

Sandbox en la nube

Sandbox en la nube es una tecnología que le permite detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Sandbox en la nube para su análisis. Sandbox en la nube ejecuta estos archivos en un entorno aislado para identificar actividad maliciosa y tomar una decisión sobre su reputación. A continuación, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Sandbox en la nube ha detectado un archivo malicioso, Kaspersky Endpoint Security realizará la acción adecuada para eliminar esta amenaza en todos los equipos donde se detecte este archivo.

Para que Sandbox en la nube funcione, debe activar el uso de Kaspersky Security Network.

Si está utilizando Kaspersky Security Network privada, la tecnología Sandbox en la nube no estará disponible.

La tecnología Sandbox en la nube se activa de manera permanente y está disponible para todos los usuarios de Kaspersky Security Network, más allá del tipo de licencia que usen. Si ya ha implementado la solución Endpoint Detection and Response Optimum, puede activar un contador independiente para las amenazas detectadas por Sandbox en la nube. Puede utilizar este contador para compilar estadísticas al analizar las amenazas detectadas. Kaspersky Endpoint Security indica la tecnología de detección de amenazas de Sandbox en la nube en *Informe de amenazas* en la consola de Kaspersky Security Center.



Contadores de amenazas

Para activar el contador de Sandbox en la nube:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la pestaña **Sandbox en la nube**.
6. Active la opción **Sandbox en la nube ACTIVADO**.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cuando existe una amenaza, Kaspersky Endpoint Security activa el contador de amenazas detectadas a través de Sandbox en la nube en la ventana principal de la aplicación, en **Tecnologías de detección de amenazas**. Kaspersky Endpoint Security también indicará la tecnología de detección de amenazas de Sandbox en el *Informe de amenazas* de la consola de Kaspersky Security Center.

Guía de migración de KEA a KES para EDR Optimum

Kaspersky Endpoint Security para Windows incluye un agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con EDR Optimum. Kaspersky Endpoint Security realizará todas las funciones de Kaspersky Endpoint Agent.

Al desplegar Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Endpoint Detection and Response Optimum seguirá funcionando con Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 11.7.0 o superior.

Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar ambas aplicaciones en el mismo equipo.

Se deben cumplir las siguientes condiciones para que Kaspersky Endpoint Security funcione como parte de Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum 2.0 o superior.
- Kaspersky Security Center versión 13.2 o superior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de EDR Optimum.
- EDR Optimum solo se puede administrar mediante Kaspersky Security Center Web Console.
- La transferencia de datos al Servidor de administración está activada. Los datos se requieren para obtener información acerca de los archivos en cuarentena en un equipo a través de Web Console.
- Se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Para que EDR Optimum trabaje con el Servidor de administración mediante Kaspersky Security Center Web Console, debe establecer una nueva conexión segura, una *conexión en segundo plano*.

Pasos para migrar la configuración de [KES+KEA] a [KES+agente integrado] para EDR Optimum

1. **Actualizar el complemento web de Kaspersky Endpoint Security**

   El componente EDR Optimum se puede administrar con el Complemento de administración de Kaspersky Endpoint Security, versión 11.7 o superior.

2. **Migrar directivas y tareas**

   Transfiera la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows. Para hacer esto, use el asistente para realizar la migración desde Kaspersky Endpoint Agent en Web Console.

   Cómo migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console

   En la ventana principal de Web Console, seleccione **Operaciones → Migración desde Kaspersky Endpoint Agent**.

Esto ejecuta el asistente de migración de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Migración de directivas

El Asistente de migración crea una directiva nueva que combina las configuraciones de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee unir con la directiva de Kaspersky Endpoint Security. Haga clic en una directiva de Kaspersky Endpoint Agent para seleccionar la directiva de Kaspersky Endpoint Security con la que desea unir la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de tareas

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desee crear para la directiva de Kaspersky Endpoint Security. Ir al paso siguiente.

Paso 3: Fin del asistente

Finalice el asistente. Como resultado, el asistente hace lo siguiente:

- Crea una directiva de Kaspersky Endpoint Security.

  La directiva une la configuración de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. La directiva se denomina *<nombre de la directiva de Kaspersky Endpoint Security> y <nombre de la directiva de Kaspersky Endpoint Agent>*. La directiva nueva tiene el estado *Inactiva*. Para continuar, cambie los estados de las directivas de Kaspersky Endpoint Agent y Kaspersky Endpoint Security a *Inactiva* y active la directiva nueva y combinada.

  Después de realizar la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, asegúrese de que la directiva nueva tenga configurada la funcionalidad para la transferencia de datos al Servidor de administración (datos del archivo en cuarentena y datos de la cadena de desarrollo de la amenaza). Los valores de parámetros de la transferencia de datos no se migran desde una directiva de Kaspersky Endpoint Agent.

- Se crean tareas nuevas de Kaspersky Endpoint Security.

  Las tareas nuevas son copias de las tareas de Kaspersky Endpoint Agent. Al mismo tiempo, el Asistente deja las tareas de Kaspersky Endpoint Agent sin cambios.

3 Licencia de la funcionalidad EDR Optimum

Si utiliza una licencia común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Agent, la funcionalidad EDR Optimum se activa de manera automática después de actualizar la aplicación a la versión 11.7.0 o superior. No necesita realizar ninguna otra acción.

Si utiliza una licencia independiente adicional de Kaspersky Endpoint Detection and Response Optimum para activar la funcionalidad EDR Optimum, debe asegurarse de que la clave de EDR Optimum se añada al repositorio de Kaspersky Security Center y de que la funcionalidad de distribución automática de claves de licencia esté activada. Después de actualizar la aplicación a la versión 11.7.0 o superior, la funcionalidad EDR Optimum se activa de manera automática.

Si utiliza una licencia de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Agent, y una licencia diferente para activar Kaspersky Endpoint Security para Windows, debe reemplazar la clave para Kaspersky Endpoint Security para Windows con la clave común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. Puede reemplazar la clave con la tarea *Añadir clave*.

4. **Instalar o actualizar la aplicación Kaspersky Endpoint Security**

Para migrar la funcionalidad EDR Optimum durante la instalación o actualización de una aplicación, se recomienda utilizar la tarea de instalación remota. Al crear una tarea de instalación remota, debe seleccionar el componente EDR Optimum en la configuración del paquete de instalación.

También puede actualizar la aplicación con los siguientes métodos:

- Usar el servicio de actualización de Kaspersky.
- De forma local, utilizando el Asistente de instalación.

Kaspersky Endpoint Security admite la selección automática de componentes al actualizar la aplicación en un equipo con la aplicación Kaspersky Endpoint Agent instalada. La selección automática de componentes depende de los permisos de la cuenta de usuario que está actualizando la aplicación.

Si está actualizando Kaspersky Endpoint Security con el archivo EXE o MSI en la cuenta del sistema (SYSTEM), Kaspersky Endpoint Security obtiene acceso a las licencias actuales de las soluciones de Kaspersky. Por lo tanto, si el equipo tiene, por ejemplo, Kaspersky Endpoint Agent instalado y la solución EDR Optimum activada, el instalador de Kaspersky Endpoint Security configura automáticamente el conjunto de componentes y selecciona el componente EDR Optimum. Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina Kaspersky Endpoint Agent. La ejecución del instalador MSI con la cuenta del sistema (SYSTEM) se realiza normalmente cuando se actualiza a través del servicio de actualización de Kaspersky o cuando se despliega un paquete de instalación a través de Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tendrá acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes según la configuración de Kaspersky Endpoint Agent. Tras esto, Kaspersky Endpoint Security pasa a utilizar el agente integrado y elimina Kaspersky Endpoint Agent.

Kaspersky Endpoint Security admite la actualización sin reiniciar el equipo. Puede seleccionar el modo de actualización de la aplicación en las propiedades de la directiva.

5. **Comprobación del funcionamiento de la aplicación**

Si, tras instalar o actualizar la aplicación, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.
- Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, asegúrese de haber activado la funcionalidad de agente integrado.
- Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

Kaspersky Sandbox



Kaspersky Endpoint Security para Windows incorpora un agente para la integración con Kaspersky Sandbox. El componente *Sandbox* detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Sandbox analiza el comportamiento de los objetos para detectar la actividad maliciosa y la actividad característica de los ataques dirigidos a la infraestructura de TI de la organización. Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Sandbox). Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Sandbox y la Ayuda de Kaspersky Anti Targeted Attack Platform.

Integración del agente integrado con Kaspersky Sandbox

Es necesario añadir el componente Sandbox para la integración con Kaspersky Sandbox. Puede seleccionar el componente Sandbox durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

Para utilizar el componente, se deben cumplir las siguientes condiciones:

- Kaspersky Security Center 13.2. Las versiones anteriores de Kaspersky Security Center no permiten crear tareas de análisis de IOC independientes para la respuesta a la amenaza.
- El componente solo se puede administrar mediante Web Console. No puede administrar este componente mediante la Consola de administración (MMC).
- La aplicación está activada y la funcionalidad se incluye en la licencia.
- La transferencia de datos al Servidor de administración está activada.

  Para utilizar todas las funcionalidades de Kaspersky Sandbox, asegúrese de que la transferencia de datos de archivos en cuarentena esté activada. Los datos se requieren para obtener información acerca de los archivos en cuarentena en un equipo a través de Web Console. Por ejemplo, puede descargar un archivo desde la cuarentena para analizarlo en Web Console.

  Cómo activar la transferencia de datos al Servidor de administración en Web Console

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general** → **Integración con KSC**.
  5. En el bloque **Transferencia de datos al Servidor de administración**, seleccione la casilla de verificación **Acerca de los archivos en Cuarentena**.
  6. Guarde los cambios.
- Se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración

Para que Kaspersky Sandbox trabaje con el Servidor de administración mediante Kaspersky Security Center Web Console, debe establecer una nueva conexión segura, una *conexión en segundo plano*. Para obtener información acerca de la integración de Kaspersky Security Center con otras soluciones de Kaspersky, consulte la Ayuda de Kaspersky Security Center.

Establecer una conexión en segundo plano en Web Console

1. En la ventana principal de Web Console, seleccione **Configuración** → **Integración**.
2. Vaya a la sección **Integración**.
3. Active la opción **Conexión en segundo plano para la integración Activada**.
4. Guarde los cambios.

Si no se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración, las tareas independientes de análisis de IOC no se pueden crear como parte de la Respuesta a la amenaza.

- Para configurar una conexión de confianza con el servidor Sandbox, debe preparar un certificado TLS. A continuación, debe añadir el certificado al equipo mediante el uso de una directiva. También debe añadir el certificado al servidor Sandbox.

  La autenticación bidireccional mediante un contenedor criptográfico no está disponible para Kaspersky Sandbox.

  Puede añadir un certificado TLS en Web Console o localmente mediante la línea de comandos.

- El componente Kaspersky Sandbox está activado.
- Los componentes de la aplicación que garantizan el funcionamiento de Sandbox están activados y operativos. Los siguientes componentes garantizan el funcionamiento de Sandbox:
  - Protección frente a amenazas en archivos.
  - Prevención de intrusiones en el host.
  - Firewall.
  - Protección AMSI.
  - Análisis en segundo plano.

Para activar o desactivar la integración con Kaspersky Sandbox, haga lo siguiente:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Sandbox**.
5. Utilice interruptor **Integración con Sandbox ACTIVADA** para activar o desactivar el componente.

6. En el bloque **Modo de integración**, seleccione el modo de funcionamiento del componente: **Kaspersky Sandbox**.

7. Haga clic en el enlace **Configuración de conexión**.

   Esto abre la ventana de configuración de la conexión del servidor de Sandbox.

8. En el bloque **Certificado TLS del servidor**, haga clic en **Cargar** y seleccione el archivo de certificado TLS.

   Kaspersky Endpoint Security solo puede tener un certificado TLS para un servidor de Sandbox. Si ha añadido un certificado TLS anteriormente, ese certificado se revoca. Solo se utiliza el último certificado añadido.

9. Configure las opciones de conexiones avanzadas para los servidores de Sandbox:

   - **Tiempo de espera (mseg)**. Tiempo de espera de conexión para el servidor Sandbox. Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de espera de conexión del servidor si su velocidad de conexión es baja o si la conexión es inestable. El tiempo de espera recomendado para las solicitudes es de 0,5 segundos o menos.

   - **Cola de peticiones**. Tamaño de la carpeta de cola de solicitudes. Al enviar varios objetos para su análisis en Sandbox, Kaspersky Endpoint Security crea una cola de solicitudes. De forma predeterminada, el tamaño de la carpeta de cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Sandbox deja de añadir nuevas solicitudes a la cola y envía el evento correspondiente a Kaspersky Security Center. Puede configurar el tamaño de la carpeta de cola de solicitudes en función de la configuración de su servidor.

10. En el bloque **Conexión a servidores Sandbox**, haga clic en el botón **Añadir**.

11. Esto abre una ventana en la que debe introducir la dirección del servidor de Sandbox (IPv4, IPv6, DNS) y el puerto.

    Para obtener detalles sobre la implementación de imágenes virtuales y la configuración de los servidores de Sandbox, consulte la Ayuda de Kaspersky Sandbox.

12. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security comprueba el certificado TLS. Si el certificado se comprueba correctamente, Kaspersky Endpoint Security carga el archivo del certificado en el equipo durante la próxima sincronización con Kaspersky Security Center. Si ha añadido dos certificados TLS, Kaspersky Sandbox utilizará el último certificado añadido para establecer una conexión de confianza. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Sandbox** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Puede activar o desactivar la integración con Kaspersky Sandbox en Web Console o localmente a través de la línea de comandos.

Kaspersky Endpoint Security guarda información sobre el funcionamiento del componente Kaspersky Sandbox en un informe. El informe también contiene información sobre errores. Si recibe un mensaje de error con un formato de descripción `Error code: XXX` (por ejemplo, `0xa67b01f4`), póngase en contacto con el Soporte técnico.

Analizar en busca de indicadores de compromiso (tarea independiente)

Un *Indicador de compromiso (IOC)* es un conjunto de datos sobre un objeto o actividad que indica el acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. La tarea de *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta a la amenaza.

Kaspersky Endpoint Security busca indicadores de compromiso utilizando archivos IOC. Los *archivos IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos IOC deben cumplir con el estándar OpenIOC. Kaspersky Endpoint Security genera automáticamente archivos IOC para Kaspersky Sandbox.

Modo de ejecución de tareas Análisis de IOC

La aplicación crea tareas de análisis de IOC independientes para Kaspersky Sandbox. La *tarea de análisis de IOC independiente* es una tarea de grupo que se crea automáticamente al reaccionar a una amenaza detectada por Kaspersky Sandbox. Kaspersky Endpoint Security genera automáticamente el archivo de IOC. Los archivos IOC personalizados no son compatibles. Las tareas se eliminan automáticamente 30 días después del momento de creación. Para obtener más detalles sobre las tareas de análisis de IOC independientes, consulte la Ayuda de Kaspersky Sandbox.

Configuración de la tarea Análisis de IOC

Kaspersky Sandbox puede crear y ejecutar tareas de *Análisis de IOC* de forma automática cuando reacciona a amenazas.

Puede configurar los ajustes solo en Web Console.

Necesita Kaspersky Security Center 13.2 para que las tareas de análisis de IOC independientes de Kaspersky Sandbox funcionen.

Para cambiar la configuración de la tarea de la tarea Análisis de IOC:

1. En la ventana principal de Web Console, seleccione **Tareas**.

   Se abre la lista de tareas.

2. Seleccione la tarea **Análisis de IOC** de Kaspersky Endpoint Security.

   Se abre la ventana propiedades de la tarea.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Configuración del Análisis de IOC**.

5. Configure acciones al detectar un IOC:

   - **Mover la copia a la cuarentena, eliminar objeto**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.

   - **Ejecutar análisis de áreas críticas**. Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.

   - **Ejecutar solo cuando el equipo está inactivo**. Inicio pospuesto de la tarea cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.

6. Guarde los cambios.

Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**. Puede ver la información acerca de los indicadores de compromiso detectados en las propiedades de la tarea: **Configuración de la aplicación → Resultados del Análisis de IOC**.

Los resultados del análisis de IOC se conservan durante 30 días. Después de dicho período, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

Guía de migración de KEA a KES para Kaspersky Sandbox

Kaspersky Endpoint Security para Windows incorpora un agente para la solución Kaspersky Sandbox. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con Kaspersky Sandbox. Kaspersky Endpoint Security realizará todas las funciones de Kaspersky Endpoint Agent.

Al desplegar Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Sandbox seguirá funcionando con Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 11.7.0 o superior.

Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar ambas aplicaciones en el mismo equipo.

Se deben cumplir las siguientes condiciones para que Kaspersky Endpoint Security funcione como parte de Kaspersky Sandbox:

- Kaspersky Sandbox versión 2.0 o superior.
- Kaspersky Security Center versión 13.2 o superior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Kaspersky Sandbox.
- Kaspersky Sandbox solo se puede administrar mediante Kaspersky Security Center Web Console.

- La transferencia de datos al Servidor de administración está activada. Los datos se requieren para obtener información acerca de los archivos en cuarentena en un equipo a través de Web Console.
- Se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Para que Kaspersky Sandbox trabaje con el Servidor de administración mediante Kaspersky Security Center Web Console, debe establecer una nueva conexión segura, una *conexión en segundo plano*.

Pasos para migrar la configuración de [KES+KEA] a [KES+agente integrado] para Kaspersky Sandbox

1. **Actualizar el complemento web de Kaspersky Endpoint Security**

   El componente Kaspersky Sandbox se puede administrar con el complemento web de Kaspersky Endpoint Security, versión 11.7.0 o superior.

2. **Migrar directivas y tareas**

   Transfiera la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows. Para hacer esto, use el asistente para realizar la migración desde Kaspersky Endpoint Agent en Web Console.

   Cómo migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console

   En la ventana principal de Web Console, seleccione **Operaciones → Migración desde Kaspersky Endpoint Agent**.

   Esto ejecuta el asistente de migración de directivas y tareas. Siga las instrucciones del Asistente.

   Paso 1. Migración de directivas

   El Asistente de migración crea una directiva nueva que combina las configuraciones de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee unir con la directiva de Kaspersky Endpoint Security. Haga clic en una directiva de Kaspersky Endpoint Agent para seleccionar la directiva de Kaspersky Endpoint Security con la que desea unir la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

   Paso 2. Migración de tareas

   El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desee crear para la directiva de Kaspersky Endpoint Security. Ir al paso siguiente.

   Paso 3: Fin del asistente

   Finalice el asistente. Como resultado, el asistente hace lo siguiente:

   - Crea una directiva de Kaspersky Endpoint Security.

La directiva une la configuración de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. La directiva se denomina *<nombre de la directiva de Kaspersky Endpoint Security> y <nombre de la directiva de Kaspersky Endpoint Agent>*. La directiva nueva tiene el estado *Inactiva*. Para continuar, cambie los estados de las directivas de Kaspersky Endpoint Agent y Kaspersky Endpoint Security a *Inactiva* y active la directiva nueva y combinada.

Después de realizar la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, asegúrese de que la directiva nueva tenga configurada la funcionalidad para la transferencia de datos al Servidor de administración (datos del archivo en cuarentena y datos de la cadena de desarrollo de la amenaza). Los valores de parámetros de la transferencia de datos no se migran desde una directiva de Kaspersky Endpoint Agent.

- Se crean tareas nuevas de Kaspersky Endpoint Security.

  Las tareas nuevas son copias de las tareas de Kaspersky Endpoint Agent. Al mismo tiempo, el Asistente deja las tareas de Kaspersky Endpoint Agent sin cambios.

3 Licencia de la funcionalidad de Kaspersky Sandbox

Para activar Kaspersky Endpoint Security como parte de la solución Kaspersky Sandbox, necesita una licencia independiente para el complemento Kaspersky Sandbox. Puede añadir la clave con la tarea *Añadir clave*. Como resultado, se añadirán dos claves a la aplicación: *Kaspersky Endpoint Security* y *Kaspersky Sandbox*.

4 Instalar o actualizar la aplicación Kaspersky Endpoint Security

Para migrar la funcionalidad de Kaspersky Sandbox durante la instalación o actualización de una aplicación, se recomienda utilizar la tarea de instalación remota. Al crear una tarea de instalación remota, debe seleccionar el componente Kaspersky Sandbox en la configuración del paquete de instalación.

También puede actualizar la aplicación con los siguientes métodos:

- Usar el servicio de actualización de Kaspersky.
- De forma local, utilizando el Asistente de instalación.

Kaspersky Endpoint Security admite la selección automática de componentes al actualizar la aplicación en un equipo con la aplicación Kaspersky Endpoint Agent instalada. La selección automática de componentes depende de los permisos de la cuenta de usuario que está actualizando la aplicación.

Si está actualizando Kaspersky Endpoint Security con el archivo EXE o MSI en la cuenta del sistema (SYSTEM), Kaspersky Endpoint Security obtiene acceso a las licencias actuales de las soluciones de Kaspersky. Por lo tanto, si el equipo tiene, por ejemplo, Kaspersky Endpoint Agent instalado y la solución Kaspersky Sandbox activada, el instalador de Kaspersky Endpoint Security configura automáticamente el conjunto de componentes y selecciona el componente Kaspersky Sandbox. Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina Kaspersky Endpoint Agent. La ejecución del instalador MSI con la cuenta del sistema (SYSTEM) se realiza normalmente cuando se actualiza a través del servicio de actualización de Kaspersky o cuando se despliega un paquete de instalación a través de Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tendrá acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes según la configuración de Kaspersky Endpoint Agent. Tras esto, Kaspersky Endpoint Security pasa a utilizar el agente integrado y elimina Kaspersky Endpoint Agent.

Kaspersky Endpoint Security admite la actualización sin reiniciar el equipo. Puede seleccionar el modo de actualización de la aplicación en las propiedades de la directiva.

5 Comprobación del funcionamiento de la aplicación

Si, tras instalar o actualizar la aplicación, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.
- Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, asegúrese de haber activado la funcionalidad de agente integrado.
- Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security para Windows permite trabajar con la solución Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* es una solución diseñada para detener a tiempo amenazas sofisticadas, como ataques dirigidos, amenazas persistentes avanzadas (APT) y ataques de día cero, entre otras. Kaspersky Anti Targeted Attack Platform incluye tres unidades funcionales:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Puede comprar todas las unidades funcionales o unidades funcionales individuales por separado. Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform. La aplicación incluye agentes integrados para componentes EDR y NDR. La aplicación también permite trabajar con el componente Sandbox que forma parte de KATA.

Herramientas de Inteligencia contra amenazas

Kaspersky Endpoint Detection and Response utiliza las siguientes herramientas Threat Intelligence:

- Integración con Kaspersky Threat Intelligence Portal, que contiene y muestra información sobre la reputación de los archivos y las direcciones web.
- Base de datos de amenazas de Kaspersky.
- La infraestructura de servicios de nube de Kaspersky Security Network (en lo sucesivo también denominada "KSN"), que proporciona acceso a información de reputación de software, sitios web y archivos en tiempo real de la base de conocimientos de Kaspersky. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de las aplicaciones de Kaspersky ante amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos.

Principio de funcionamiento de la solución

Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y supervisa continuamente los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos en el equipo (datos de telemetría) se envía al servidor de Kaspersky Anti Targeted Attack Platform. En este caso, Kaspersky Endpoint Security también envía información al servidor de Kaspersky Anti Targeted Attack Platform sobre las amenazas descubiertas por la aplicación, así como información sobre los resultados del procesamiento de estas amenazas.

La integración de EDR (KATA) y NDR (KATA) se configura en la consola de Kaspersky Security Center. A continuación, el agente integrado se administra mediante la consola de Kaspersky Anti Targeted Attack Platform, incluida la ejecución de tareas, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Configuraciones de Kaspersky Endpoint Security para trabajar con EDR / NDR (KATA)

Se pueden utilizar las siguientes configuraciones para trabajar con EDR / NDR (KATA):

- **[KES+agente integrado]**. En esta configuración, Kaspersky Endpoint Security actúa como la aplicación que garantiza la seguridad del equipo y como la aplicación para trabajar con EDR / NDR (KATA). El agente integrado para EDR (KATA) está disponible en Kaspersky Endpoint Security 12.1 para Windows o posterior. El agente integrado para NDR (KATA) está disponible en Kaspersky Endpoint Security 12.7 para Windows o posterior.

- **[EPP de terceros +EDR Agent]**. En esta configuración, la seguridad de la infraestructura de TI la proporciona la aplicación Endpoint Protection Plataform (EPP) de terceros. La interacción con EDR / NDR (KATA) la proporciona Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent (EDR Agent). En esta configuración, EDR Agent es compatible con aplicaciones EPP de terceros. EDR Agent para EDR (KATA) está disponible en Kaspersky Endpoint Security 12.3 para Windows o posterior. EDR Agent para NDR (KATA) está disponible en Kaspersky Endpoint Security 12.7 para Windows o posterior.

Compatibilidad con versiones anteriores de Kaspersky Endpoint Security

Si utiliza Kaspersky Endpoint Security 11.2.0–11.8.0 para la interoperabilidad con Kaspersky Anti Targeted Attack Platform (EDR), la aplicación incluye Kaspersky Endpoint Agent. Puede instalar Kaspersky Endpoint Agent junto con Kaspersky Endpoint Security.

Si utiliza Kaspersky Endpoint Security 11.9.0 – 12.0, debe instalar Kaspersky Endpoint Agent por separado porque, a partir de Kaspersky Endpoint Security 11.9.0, el paquete de distribución de Kaspersky Endpoint Agent ya no forma parte del kit de distribución de Kaspersky Endpoint Security.

Integración del agente integrado con EDR / NDR (KATA)

Para la integración con EDR/NDR (KATA), debe añadir el componente relevante: Endpoint Detection and Response (KATA) o Network Detection and Response (KATA). Puede seleccionar componentes de integración con EDR / NDR (KATA) durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

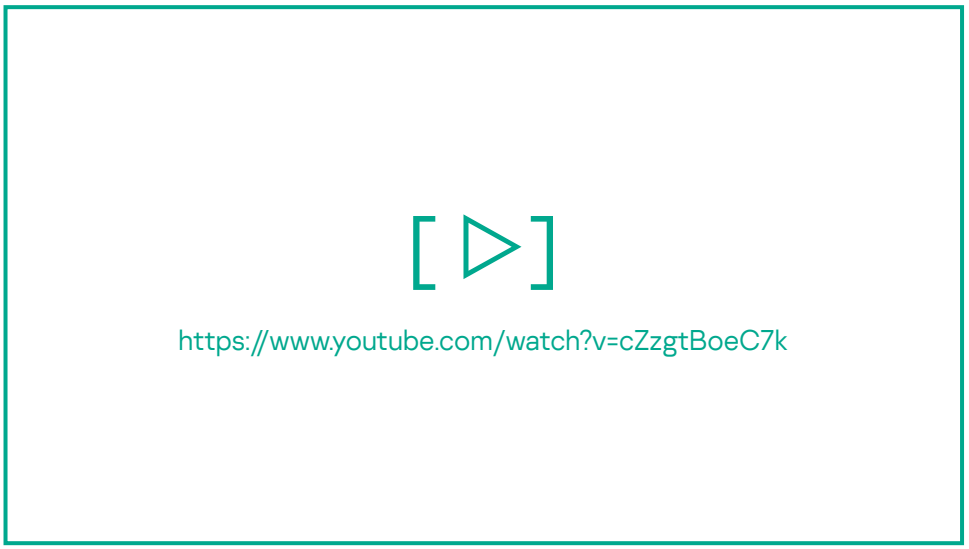
A partir de la versión 12.11 de Kaspersky Endpoint Security para Windows, se ha cambiado el nombre del componente EDR (KATA) a **Endpoint Detection and Response Expert (versión 8.0 o posterior)**. En esta versión de la aplicación, el componente es compatible con Kaspersky Anti Targeted Attack Platform 7.1 y versiones anteriores, así como con Kaspersky Endpoint Detection and Response Expert (on-premises).

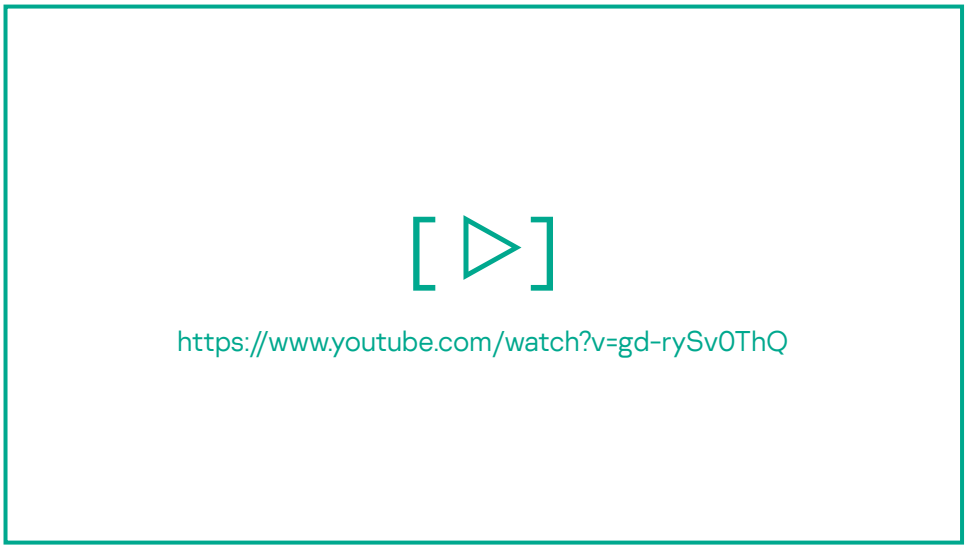
Los componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) y Endpoint Detection and Response Expert (on-premises) no son compatibles entre sí.

Para utilizar EDR / NDR (KATA), se deben cumplir las siguientes condiciones:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform versiones 5.0-7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform versión 7.0 o superior.
- EDR (KATA): Kaspersky Endpoint Security para Windows 12.1 o posterior. Para obtener más detalles sobre la compatibilidad de KATA con diferentes versiones de Kaspersky Endpoint Security, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security para Windows 12.7 o posterior.
- Kaspersky Security Center versión 14.2 o superior. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de integración de EDR / NDR (KATA).
- La aplicación está activada y la funcionalidad se incluye en la licencia.
- Los componentes Endpoint Detection and Response (KATA) y Network Detection and Response (KATA) están activados.
- Los componentes de la aplicación que garantizan el funcionamiento de EDR / NDR (KATA) están activados y operativos. Los siguientes componentes garantizan el funcionamiento de EDR / NDR (KATA):
  - Protección frente a amenazas en archivos.
  - Protección frente a amenazas web.
  - Protección frente a amenazas en el correo.
  - Prevención de exploits.
  - Detección de comportamiento.
  - Prevención de intrusiones en el host.
  - Protección AMSI.

- Análisis en segundo plano.
- Kaspersky Security Network.





El proceso de integración con Endpoint Detection and Response (KATA) incluye los siguientes pasos:

1. **Instalación de los componentes Endpoint Detection and Response (KATA) y Network Detection and Response (KATA)**

   Puede seleccionar los componentes EDR (KATA) y NDR (KATA) durante la instalación o la actualización, así como utilizar la tarea *Cambiar componentes de la aplicación*.

   > Debe reiniciar el equipo para terminar de actualizar la aplicación con los componentes nuevos.

2. **Activación de Endpoint Detection and Response (KATA) y Network Detection and Response (KATA)**

   Debe comprar una licencia independiente para EDR (KATA) y NDR (KATA) (por ejemplo, complemento de Kaspersky Endpoint Detection and Response [KATA]).

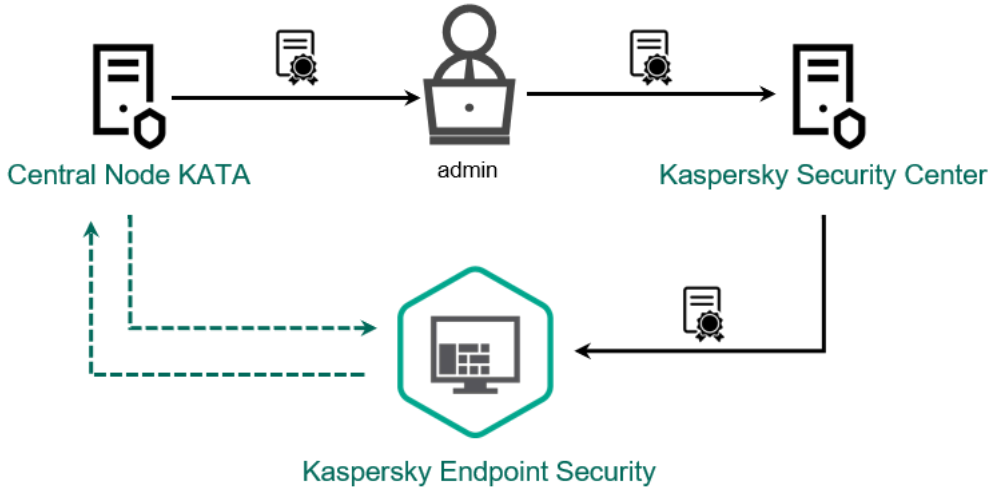
   La funcionalidad estará disponible tras añadir una clave independiente que cubra la funcionalidad EDR (KATA) y NDR (KATA). Como resultado, se añaden varias claves en el equipo: una clave para Kaspersky Endpoint Security, y claves para Kaspersky Endpoint Detection and Response (KATA) y Network Detection and Response (KATA).

   La licencia para la funcionalidad independiente de EDR (KATA) y NDR (KATA) es la misma licencia que la de Kaspersky Endpoint Security.

   Asegúrese de que tanto la funcionalidad de EDR (KATA) como de NDR (KATA) estén incluidas en la licencia y en ejecución en la interfaz local de la aplicación.

3 Conexión al Central Node

Kaspersky Anti Targeted Attack Platform requiere establecer una conexión de confianza entre Kaspersky Endpoint Security y el componente de Central Node. Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). A continuación, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).



Agregar un certificado TLS a Kaspersky Endpoint Security

De manera predeterminada, Kaspersky Endpoint Security solo verifica el certificado TLS de Central Node. Para que la conexión sea más segura, también puede habilitar la verificación del equipo en Central Node (autenticación bidireccional). Para activar esta verificación, debe activar la autenticación bidireccional en la configuración de Central Node y Kaspersky Endpoint Security. Para usar la autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

Cómo conectar un equipo con Kaspersky Endpoint Security al Central Node mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Detection and Response** y el componente que desea configurar: **Endpoint Detection and Response Expert (on-premises)** o **Network Detection and Response (KATA)**.
5. Seleccione la casilla de verificación correspondiente: **Endpoint Detection and Response Expert (versión 7.1 o anterior)** o **Network Detection and Response (KATA)**.
6. Haga clic en **Configuración de conexión a servidor**.

7. Configure la conexión del servidor:

   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente.

   - **Certificado TLS del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

   - **Utilizar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

8. Haga clic en **Correcto**.

9. Agregar servidores de Central Node. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

   Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

10. Si es necesario, configure la telemetría.

11. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo conectar un equipo con Kaspersky Endpoint Security al Central Node mediante Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Configuración de agentes integrados** y seleccione el componente que desea configurar: **Endpoint Detection and Response Expert (on-premises)** o **Network Detection and Response (KATA)**.

5. Active el interruptor correspondiente: **Endpoint Detection and Response Expert (on-premises) activado** o **Network Detection and Response (KATA) ACTIVADO**.

6. Para configurar EDR (KATA), seleccione **Endpoint Detection and Response Expert (versión 7.1 o anterior)** en la lista de soluciones.

7. Haga clic en **Configuración de conexión**.

8. Configure la conexión del servidor:

   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente.

   - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform).

   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

9. Haga clic en **Aceptar**.

10. Agregar servidores de Central Node. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

    Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

11. Si es necesario, configure la telemetría.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

También puede añadir un certificado TLS localmente mediante la línea de comandos.

Como resultado, el equipo se agrega a la consola de Kaspersky Anti Targeted Attack Platform. Compruebe el estado operativo de los componentes consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de los componentes en los informes de la interfaz local de Kaspersky Endpoint Security. Los componentes **Endpoint Detection and Response Expert (versión 8.0 o posterior)** y **Network Detection and Response (KATA)** se añadirán a la lista de componentes de Kaspersky Endpoint Security.

Puede comprobar el estado de los componentes en la consola de Kaspersky Security Center en las propiedades del equipo, en la sección **Componentes**. Tenga en cuenta lo siguiente al comprobar el estado del componente en la consola. Si el componente no está instalado y la funcionalidad no está cubierta por su licencia, la consola muestra el estado **No compatible con la licencia** en lugar de **No instalado**.

A partir de Kaspersky Endpoint Security 12.6 para Windows, puede supervisar el estado del componente EDR (KATA) en la Consola de administración de Kaspersky Security Center (MMC). El estado actual del componente se muestra en las propiedades del equipo en la columna **Estado de Endpoint Server** (*En ejecución*, *Iniciando*, *Detenido*, *En pausa*, *Fallo*, *Desconocido*). Web Console no muestra el estado del Endpoint Sensor.

Configuración de la telemetría de EDR (KATA)

Telemetría es una lista de eventos que han ocurrido en el equipo protegido. Kaspersky Endpoint Security analiza los datos de telemetría y los envía a Kaspersky Anti Targeted Attack Platform durante la sincronización. Los eventos de telemetría llegan al servidor de manera casi continua. Kaspersky Endpoint Security inicia la sincronización con el servidor cuando se cumple alguna de las siguientes condiciones:

- Se ha agotado el intervalo de sincronización.
- El número de eventos en el búfer sobrepasa el límite superior.

Por lo tanto, de forma predeterminada, la aplicación se sincroniza cada 30 segundos o cada vez que el búfer contiene 1024 eventos. Puede configurar el comportamiento de sincronización en la directiva de Kaspersky Endpoint Security y seleccionar los valores óptimos para que coincidan con la carga de su red (consulte las instrucciones a continuación).

Si no hay conexión entre Kaspersky Endpoint Security y el servidor, la aplicación pone en cola nuevos eventos. Cuando se restablece la conexión, Kaspersky Endpoint Security envía los eventos en cola al servidor en el orden correcto. Para evitar sobrecargar el servidor, Kaspersky Endpoint Security puede omitir algunos eventos. Para activar esta función, puede optimizar la configuración de transmisión de eventos, por ejemplo, para establecer un valor máximo de eventos por hora (consulte las instrucciones que aparecen más adelante).

Si usa Kaspersky Anti Targeted Attack Platform junto con otra solución que también use telemetría, puede desactivar la telemetría para KATA (EDR) (consulte las instrucciones que aparecen más adelante). Esto le permite optimizar la carga del servidor para estas soluciones. Por ejemplo, si tiene implementados la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Threat Response en KATA (EDR).

Cómo configurar la telemetría en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Detection and Response** y el componente que desea configurar: **Endpoint Detection and Response Expert (on-premises)** o **Network Detection and Response (KATA)**.
5. Configure el ajuste **Enviar solicitud de sincronización al servidor de KATA cada (min)**. Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre la configuración y las tareas de la aplicación modificada.
6. Asegúrese de que la casilla de verificación **Enviar telemetría a KATA** esté seleccionada.
7. Si es necesario, configure la sincronización con la configuración del servidor en el bloque **Configuración de transmisión de datos**:
   - **Retraso máximo de transmisión de eventos (seg)**. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.
   - **Número máximo de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos.

8. Si es necesario, active la casilla **Activar la limitación de solicitudes** casilla en el bloque **Limitación de solicitudes**.

   Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos.

9. Configure los ajustes de optimización para enviar eventos al servidor:

   - **Número máximo de eventos por hora**. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora.

   - **Porcentaje de exceso de límite del evento**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.

10. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar la telemetría en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.

5. Para configurar EDR (KATA), seleccione **Endpoint Detection and Response Expert (versión 7.1 o anterior)** en la lista de soluciones.

6. Asegúrese de que la casilla de verificación **Enviar telemetría a servidores de KATA** está seleccionada en el bloque **Configuración de transmisión de datos**.

7. Configure el ajuste **Enviar solicitud de sincronización al servidor cada (min.)**. Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre la configuración y las tareas de la aplicación modificada.

8. Asegúrese de que la casilla de verificación **Enviar telemetría a servidores de KATA** esté seleccionada.

9. Si es necesario, configure la sincronización con la configuración del servidor en el bloque **Configuración de transmisión de datos**:

   - **Retraso máximo de transmisión de eventos (seg)**. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.

   - **Número máximo de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos.

10. Si es necesario, active la casilla **Activar la limitación de solicitudes** casilla en el bloque **Limitación de solicitudes**.

    Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos.

11. Configure los ajustes de optimización para enviar eventos al servidor:

    - **Número máximo de eventos por hora**. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora.

    - **Porcentaje de exceso de límite del evento**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Integración KATA** → **Exclusiones de telemetría**.

5. En **Configuración de transmisión de datos**, seleccione la casilla **Usar exclusiones**.

6. Haga clic en **Agregar** y configure las exclusiones:

   Los criterios se combinan con el operador lógico *AND*.

   - **Ruta**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. Para que la exclusión funcione, se debe especificar la ruta al archivo.

   - **Línea de comandos**. Comando utilizado para ejecutar el objeto.

   - **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo).

     Para obtener más información sobre el recurso VersionInfo, visite el sitio web de Microsoft.

   - **Nombre del archivo original**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo).

   - **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo).

- **MD5**. Hash MD5 del archivo.
- **SHA256**. Hash SHA256 del archivo.
- **Tipos de evento**. Para que la exclusión funcione, debe seleccionar al menos un tipo de evento.

7. Guarde los cambios.

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Tareas**.
   Se abre la lista de tareas.
2. Haga clic en **Nueva tarea**.

El Asistente de tareas comienza. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

1. Seleccione **Kaspersky Endpoint Security para Windows (14.2)** → **Revertir actualización**.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se realizará la tarea. Están disponibles los siguientes opciones:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos detectados por el Servidor de Administración en la red que tengan el estado *dispositivos no asignados*. Los dispositivos específicos pueden incluir tanto dispositivos incluidos en grupos de administración, como dispositivos no asignados.
- Especifique manualmente las direcciones de dispositivos o importe sus direcciones de una lista. Puede especificar nombre NetBIOS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Configurar una planificación de inicio de tarea

Configure la planificación de la tarea; por ejemplo, manualmente.

Paso 4. Definir el nombre de la tarea

Introduzca un nombre para la tarea.

Paso 7. Conclusión de la creación de tareas

Finalice el asistente. Si es necesario, active la casilla **Ejecutar la tarea después de que finalice el asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Exclusiones de telemetría de EDR (KATA)

Para mejorar el rendimiento y optimizar la transmisión de datos al servidor de telemetría, puede configurar las exclusiones de telemetría. Por ejemplo, puede elegir no enviar datos de comunicaciones de red de aplicaciones individuales.

Cómo crear una exclusión de telemetría en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
4. En el bloque **Configuración de telemetría → Telemetría de EDR (KATA) / NDR (KATA)**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, configure las exclusiones de telemetría (consulte la tabla a continuación).

   La aplicación combina condiciones de exclusión con el operador lógico AND. Para crear una regla, debe especificar un valor en el campo **Ruta completa** y seleccionar al menos un tipo de evento en la lista **Usar para los siguientes tipos de evento**.
6. Guarde los cambios.

Cómo crear una exclusión de telemetría en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de EDR (KATA) / NDR (KATA)**.
6. En la ventana que se abre, configure las exclusiones de telemetría (consulte la tabla a continuación).

   La aplicación combina condiciones de exclusión con el operador lógico AND. Para crear una regla, debe especificar un valor en el campo **Ruta completa** y seleccionar al menos un tipo de evento.
7. Guarde los cambios.

Parámetros de exclusión de telemetría

Parámetro	Descripción
Procesos excluidos	**Optimizar el tamaño de la telemetría para envío**. Kaspersky Endpoint Security permite optimizar la cantidad de datos transmitidos y excluir eventos con determinados códigos de la telemetría: código 102 (comunicaciones básicas) y 8 (actividad de red del proceso) para el protocolo Microsoft SMB, el servicio WinRM y el proceso klnagent.exe del Agente de red, así como información ampliada sobre los tipos de paquetes de red para todo tipo de protocolos de red. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo. **Usar para los siguientes tipos de evento**: • **Modificación del archivo**. • **Eventos de red**. • **Proceso: entrada interactiva en la consola**. • **Módulo cargado**. • **Registro modificado**. • **Registros de DNS**. • **Acceso al proceso**. • **Inyección de código**. • **Consulta de WMI**. • **Canal**. • **LDAP**. • **AMSI**.
Comunicaciones de red excluidas	**Nombre de la regla**. **Dirección**. **Protocolo**. **Socket raw**. **Número de protocolo**. **Certificado TLS**. **Puerto o rango local**. **Puerto o rango remoto**. **Dirección local**. La dirección de red del equipo para el que Kaspersky Endpoint Security excluye la telemetría del tráfico de red. **Dirección remota**. La dirección de red del equipo para el que Kaspersky Endpoint Security excluye la telemetría del tráfico de red. Solo el formato IPv4 es compatible con las direcciones IP. **Aplicaciones**. Lista de archivos ejecutables de aplicaciones para las que Kaspersky Endpoint Security excluye la telemetría EDR del tráfico de red.

Parámetro	Descripción
Operaciones excluidas con archivos	**Nombre de la regla**. **Nombre o máscara de archivo**. Nombre o máscara de un archivo o carpeta; Kaspersky Endpoint Security aplica la regla de exclusión cuando se accede a este archivo o carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara. **Tipo de operación**. **Ruta anterior**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.
Operaciones de DNS excluidas	**Nombre de la regla**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo. **DNS**: • **Dirección IP del servidor DNS**. • **Opciones de consulta**. • **Estado**. • **Nombre de dominio**. • **ID de tipo de configuración**. • **Datos de respuesta**.

Parámetro	Descripción
Operaciones de LDAP excluidas	**Nombre de la regla**. **Alcance de la búsqueda de LDAP**. **Filtro**. **Nombre distinguido para la búsqueda de objetos LDAP**. **Atributos de objeto**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.
Consultas de acceso a procesos excluidos	**Nombre de la regla**. **Tipo de operación**. **Se ha solicitado acceso al proceso**. **Llamar a rastreo de pila**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso**, **Proceso principal**, **Archivo del proceso de destino**, **Manejar en el proceso de origen** y **Manejar en el proceso de destino**. • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Especifique criterios de activación de reglas y los tipos de evento para los que usar esta regla**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo). • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.

Parámetro	Descripción
Inyecciones de código excluidas	**Nombre de la regla**. **Método de acceso**. **Llamar a pila**. **Línea de comandos modificada**. **Dirección de inyección**. **Nombre de DLL inyectado**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.
Consultas de WMI excluidas	**Nombre de la regla**. **Tipo de operación de WMI**. **Consulta remota**. **Nombre de un equipo que ha ejecutado un comando WMI**. **Cuenta de usuario de WMI**. **Comando WMI ejecutado**. **Espacio de nombre de WMI**. **Filtro de consumidor de evento de WMI**. **Nombre del consumidor de evento de WMI creado**. **Código fuente de un consumidor de evento de WMI**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.

Parámetro	Descripción
Operaciones excluidas con canales	**Nombre de la regla**. **Nombre del canal**. **Tipo de operación**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.
Cambios en el registro excluidos	**Nombre de la regla**. **Tipo de operación**. **Ruta**. **Nombre del valor**. **Valor**. **Nombre completo de un archivo de registro**. Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa al archivo, incluidos el nombre y la extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo) VersionInfo. • **Nombre original del archivo**. Valor del parámetro OriginalFilename de un recurso RT_VERSION (VersionInfo). • **Versión**. Valor del parámetro FileVersion de un recurso RT_VERSION (VersionInfo). • **Sumas de comprobación del archivo**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará automáticamente los campos del archivo seleccionado. En los sistemas operativos de 64 bits, debe ingresar manualmente los parámetros de la versión de 64 bits del archivo ejecutable de un proceso desde la carpeta `C:\windows\system32` porque la aplicación completa los campos de parámetros del archivo ejecutable con datos de las propiedades de la versión de 32 bits del mismo archivo ejecutable en la carpeta `C:\windows\syswow64`. Por ejemplo, si selecciona `C:\windows\system32\cmd.exe`, el complemento muestra los parámetros de `C:\windows\syswow64\cmd.exe`. Tal comportamiento está dictado por peculiaridades del sistema operativo.
Operaciones excluidas con dispositivos	**Nombre de la regla**. **Tipo de dispositivo**. **ID de dispositivo**. **Nombre del dispositivo**.

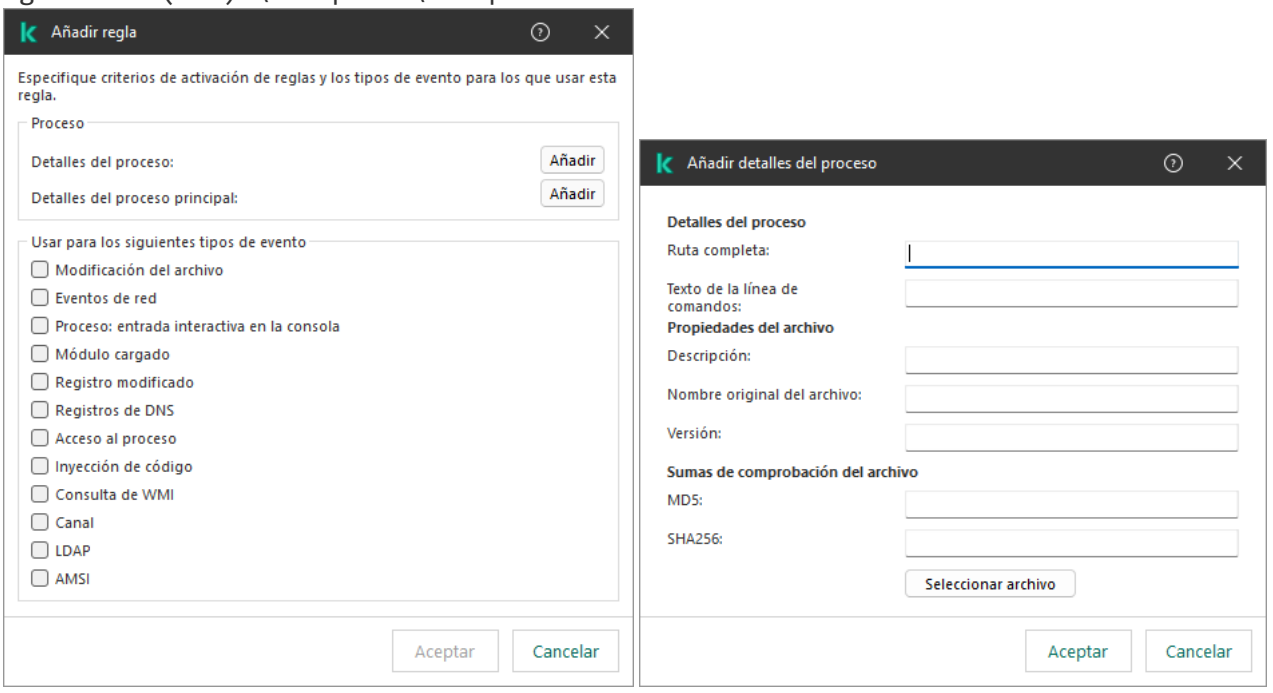
Ejemplo 1. Procesos excluidos

Para excluir eventos de aplicaciones (procesos) de terceros de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Procesos excluidos** y añada el archivo ejecutable de la aplicación.

Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND.

Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. Por ejemplo:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Excluir un proceso

Ejemplo 1. Modificación de archivos

Si edita con frecuencia scripts en la aplicación Notepad++ y desea excluir los eventos de modificación de los scripts correspondientes, añada el archivo ejecutable de Notepad++ a las exclusiones de telemetría.

Especifique la configuración de la siguiente manera:

- **Ruta completa**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Usar para los siguientes tipos de evento**: Modificación del archivo.

Ejemplo 2. Eventos de red

Si usa la aplicación WinSCP para administrar archivos en un servidor remoto y desea excluir eventos de red, añada el archivo ejecutable de WinSCP a las exclusiones de telemetría.

Especifique la configuración de la siguiente manera:

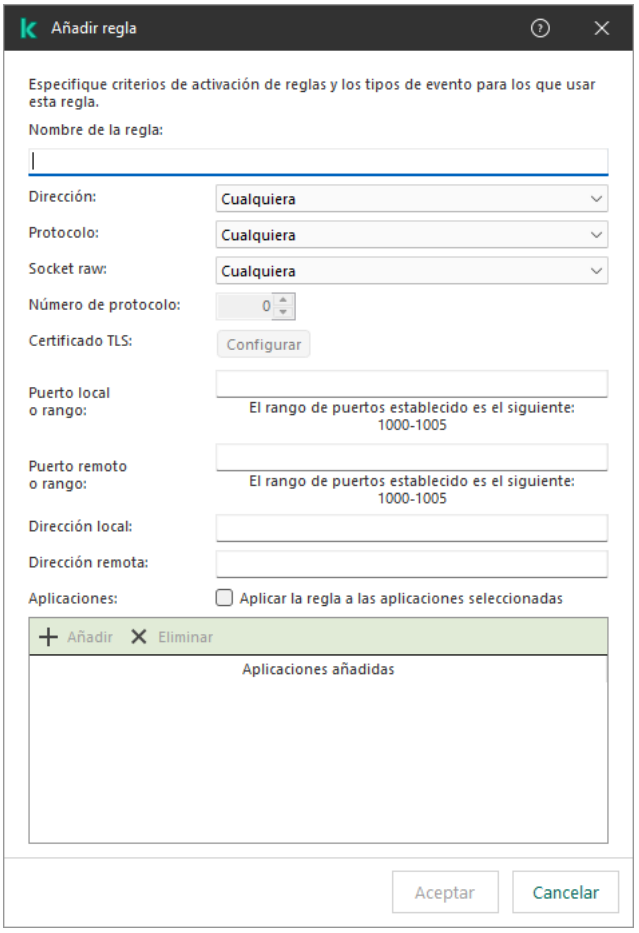
- **Ruta completa**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (opcional).
- **Usar para los siguientes tipos de evento**: Eventos de red.

Ejemplo 2. Comunicaciones de red excluidas

Para excluir eventos de conexión del servicio remoto de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Comunicaciones de red excluidas** y añada la configuración de conexión: protocolo, puerto, dirección, dirección IP, certificado TLS y otros.

Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND.

No puede especificar una dirección de subred (por ejemplo, 10.28.0.0/24). La aplicación solo permite especificar una dirección IP (por ejemplo, 10.28.0.105).



Exclusión de comunicaciones de red

Si utiliza un servidor web corporativo y desea excluir eventos del navegador al conectarse a ese servidor web, añada la dirección IP del servidor y el archivo ejecutable del navegador a las exclusiones de telemetría.

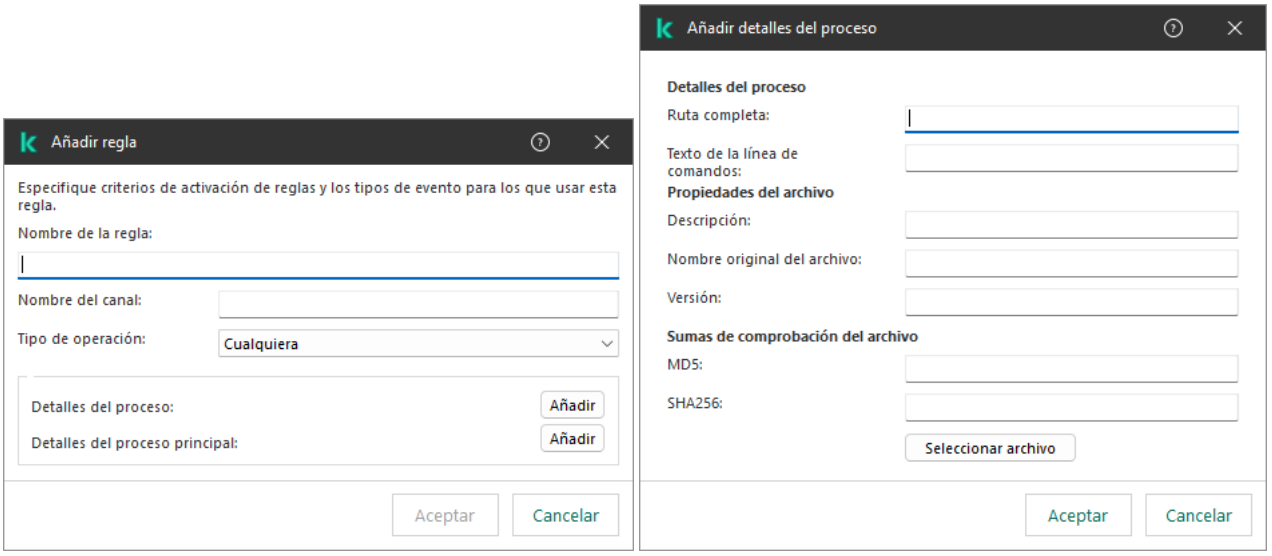
Especifique la configuración de la siguiente manera:

- **Protocolo**: TCP.
- **Puerto o rango remoto**: 443.
- **Dirección remota**: 10.28.0.105.
- **Aplicaciones**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Ejemplo 3. Operaciones de archivo excluidas

Para excluir eventos que implican operaciones con archivos de confianza de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Operaciones excluidas con archivos** y añada el archivo de confianza.

Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND.



Operaciones de archivo excluidas

Si una aplicación escribe en un registro y desea excluir los eventos de modificación del archivo de registro, añada el archivo de registro y el archivo ejecutable de la aplicación de la telemetría.

Especifique la configuración de la siguiente manera:

- **Nombre o máscara de archivo**: `C:\Apache24\logs\error.log`.
- **Tipo de operación**: Modificación del archivo.
- **Ruta completa**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Ejemplo 4. Modificaciones de registro excluidas

Para excluir eventos de modificación del registro de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Cambios en el registro excluidos** y añada una clave de registro.

Kaspersky Endpoint Security combina criterios de activación de reglas con un operador lógico AND.

Si una aplicación modifica con frecuencia sus valores de registro y desea excluir estos eventos de modificación del registro de la telemetría, añada la clave del registro y el archivo ejecutable de la aplicación a las exclusiones de telemetría.

Especifique la configuración de la siguiente manera:

- **Tipo de operación**: Modificar.
- **Ruta**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Ruta completa**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform incluye el componente Sandbox (KATA Sandbox). *Sandbox* es una tecnología que le permite detectar amenazas avanzadas en un equipo. Sandbox analiza el comportamiento de los objetos para detectar la actividad maliciosa y la actividad característica de los ataques dirigidos a la infraestructura de TI de la organización. Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Sandbox). Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

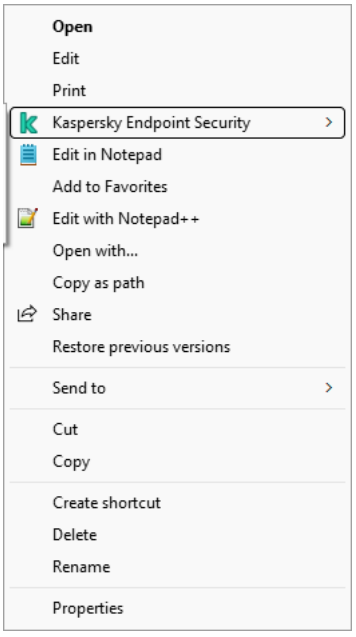
Para activar KATA Sandbox, necesita una clave de licencia que incluya la funcionalidad KATA o KEDR. Para obtener información acerca de las funcionalidades disponibles, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

KATA Sandbox permite analizar archivos en los siguientes modos:

- *Manualmente*. El usuario envía manualmente el archivo para su análisis desde el menú contextual (**Enviar a Sandbox**). Al enviar un archivo a Sandbox, la aplicación también analiza el archivo utilizando bases de datos antivirus.
- *Automáticamente*. La aplicación detecta objetos automáticamente y los envía a Sandbox para su análisis.

Después de que el archivo se envíe a Sandbox, el usuario puede acceder al archivo. Kaspersky Endpoint Security registra el evento correspondiente y lo envía a Kaspersky Security Center y a la consola de Kaspersky Anti Targeted Attack Platform. Si Sandbox detecta actividad maliciosa, Kaspersky Endpoint Security realiza una acción de Threat Response automáticamente (por ejemplo, elimina el objeto e inicia un Análisis de áreas críticas).

Para que KATA Sandbox funcione en modo manual, se debe implementar Kaspersky Anti Targeted Attack Platform 7.0 o posterior. Para que KATA Sandbox funcione en modo automático, se debe implementar Kaspersky Anti Targeted Attack Platform 8.0 o posterior.



Escaneo en KATA Sandbox desde el menú contextual

Integración del agente integrado con KATA Sandbox

Es necesario añadir el componente Sandbox para la integración con KATA Sandbox. Puede seleccionar el componente Sandbox durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

Para enviar archivos para su análisis, debe activar la integración con KATA Sandbox y añadir un servidor de Central Node que se despliega dentro de la solución. El componente solo se puede administrar mediante Kaspersky Security Center Web Console. No puede administrar este componente mediante la Consola de administración (MMC).

Para activar o desactivar la integración con KATA Sandbox, haga lo siguiente:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Sandbox**.
5. Utilice interruptor **Integración con Sandbox ACTIVADA** para activar o desactivar el componente.

6. Seleccione el modo de funcionamiento KATA Sandbox:

   - **Manual**. El usuario envía manualmente el archivo para su análisis desde el menú contextual (**Enviar a Sandbox**).
   - **Automático**. La aplicación detecta objetos automáticamente y los envía a Sandbox para su análisis.
   - **Combinado**.

7. Haga clic en el enlace **Configuración de conexión**.

8. Configurar los parámetros de conexión del servidor de Central Node.

   - **Tiempo de espera (mseg)**. Tiempo de espera de conexión para el servidor de Central Node. Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de espera de conexión del servidor si su velocidad de conexión es baja o si la conexión es inestable. El tiempo de espera recomendado para las solicitudes es de 0,5 segundos o menos.
   - **Cola de peticiones**. Tamaño de la carpeta de cola de solicitudes. Al enviar varios objetos para su análisis en Sandbox, Kaspersky Endpoint Security crea una cola de solicitudes. De forma predeterminada, el tamaño de la carpeta de cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Sandbox deja de añadir nuevas solicitudes a la cola y envía el evento correspondiente a Kaspersky Security Center. Puede configurar el tamaño de la carpeta de cola de solicitudes en función de la configuración de su servidor.
   - **Certificado TLS del servidor**. Para configurar una conexión de confianza con el servidor de Central Node, debe preparar un certificado TLS. A continuación, debe añadir el certificado al equipo mediante el uso de una directiva. También debe añadir el certificado al servidor de Central Node.
   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

9. En el bloque **Conexión a servidores Sandbox**, haga clic en el botón **Añadir**.

10. Esto abre una ventana en la que debe introducir la dirección del servidor del nodo central (IPv4, IPv6, DNS) y el puerto.

    Para obtener detalles sobre la implementación de imágenes virtuales y la configuración de los servidores del nodo central, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

11. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Como resultado, el componente Sandbox se activa. Compruebe el estado operativo del componente consultando el *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Sandbox** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Configuración de acciones de respuesta a amenazas

Si Sandbox detecta actividad maliciosa, Kaspersky Endpoint Security realiza una acción de Threat Response automáticamente (por ejemplo, elimina el objeto e inicia un Análisis de áreas críticas).

Para configurar acciones de Threat Response:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Sandbox**.
5. Seleccione la acción correspondiente en el bloque **Acción al detectar una amenaza**:

   - **Mover la copia a la cuarentena, eliminar objeto**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.
   - **Ejecutar análisis de áreas críticas**. Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.
   - **Crear tarea de Análisis de IOC**. Si se selecciona esta opción, Kaspersky Endpoint Security crea la tarea *Análisis de IOC automáticamente (tarea de análisis de IOC autónoma)*. Para esta tarea, puede configurar el modo de ejecución, la cobertura del análisis y la acción al detectar un IOC (*Mover la copia a la cuarentena, eliminar objeto* o *Ejecutar análisis de áreas críticas*). Para modificar otros parámetros de la tarea *Análisis de IOC*, vaya a la configuración de la tarea.
6. Si es necesario, configure los parámetros de la tarea *Análisis de IOC* en el bloque **Cobertura del Análisis de IOC**.

   - **Áreas críticas de archivos**. Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC solo en áreas críticas de archivos del equipo: memoria del núcleo y sectores de arranque.
   - **Áreas de archivos en la unidad de sistema del equipo**. Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC en la unidad de sistema del equipo.

7. Si es necesario, configure los parámetros de la tarea *Análisis de IOC* en el bloque **Ejecute la tarea de Análisis de IOC**.

   - **Manual**. Modo de ejecución en el que puede ejecutar la tarea *Análisis de IOC* manualmente en el momento que sea conveniente para usted.
   - **Automático**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea *Análisis de IOC* automáticamente después de detectar una amenaza.
   - **Ejecutar solo cuando el equipo está inactivo**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea *Análisis de IOC* si el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security pausa la tarea. Esto significa que la tarea puede tardar varios días en completarse.

8. Configure los parámetros de la tarea avanzados para *Análisis de IOC*.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Guía de migración de KEA a KES para EDR (KATA)

A partir de la versión 12.1, Kaspersky Endpoint Security para Windows incluye un agente integrado para administrar el componente Kaspersky Endpoint Detection and Response como parte de la solución Kaspersky Anti Targeted Attack Platform. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con EDR (KATA). Kaspersky Endpoint Security realizará todas las funciones de Kaspersky Endpoint Agent. La carga en los servidores de Kaspersky Anti Targeted Attack Platform seguirá siendo la misma.

Al desplegar Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Anti Targeted Attack Platform (EDR) seguirá funcionando con Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 12.1 o superior.

> Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar ambas aplicaciones en el mismo equipo.

Se deben cumplir las siguientes condiciones para que Kaspersky Endpoint Security funcione como parte de Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform versión 5.0 o superior.
- Kaspersky Security Center versión 14.2 o superior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Endpoint Detection and Response (KATA).

Pasos para migrar la configuración de [KES+KEA] a [KES+agente integrado] para EDR (KATA)

1. **Actualizar el Complemento de administración de Kaspersky Endpoint Security**

   El componente EDR (KATA) se puede administrar con el Complemento de administración de Kaspersky Endpoint Security, versión 12.1 o superior. Según el tipo de consola de Kaspersky Security Center que esté utilizando, actualice el complemento de administración en la Consola de administración (MMC) o el complemento web en Web Console.

2. **Migrar directivas y tareas**

Transfiera la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows. Están disponibles los siguientes opciones:

- Un asistente para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Un asistente para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security solo funciona en Web Console.

  Cómo migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console

  En la ventana principal de Web Console, seleccione **Operaciones** → **Migración desde Kaspersky Endpoint Agent**.

  Esto ejecuta el asistente de migración de directivas y tareas. Siga las instrucciones del Asistente.

  Paso 1. Migración de directivas

  El Asistente de migración crea una directiva nueva que combina las configuraciones de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee unir con la directiva de Kaspersky Endpoint Security. Haga clic en una directiva de Kaspersky Endpoint Agent para seleccionar la directiva de Kaspersky Endpoint Security con la que desea unir la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

  Paso 2. Migración de tareas

  El asistente de migración no admite tareas de EDR (KATA). Omita este paso.

  Paso 3: Fin del asistente

  Finalice el asistente. Como resultado del asistente, se creará una nueva directiva de Kaspersky Endpoint Security. La directiva une la configuración de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. La directiva se denomina *<nombre de la directiva de Kaspersky Endpoint Security> y <nombre de la directiva de Kaspersky Endpoint Agent>*. La directiva nueva tiene el estado *Inactiva*. Para continuar, cambie los estados de las directivas de Kaspersky Endpoint Agent y Kaspersky Endpoint Security a *Inactiva* y active la directiva nueva y combinada.

  El asistente de migración de Web Console omite las siguientes configuraciones de directivas y no las migra:

  - Prohibición de modificar la configuración **Configuración de conexión** ("candado").

    De forma predeterminada, la configuración se puede modificar (el "candado" está abierto). Por lo tanto, la configuración no se aplica en el equipo. Debe prohibir la modificación de la configuración y cerrar el "candado".

  - Contenedor criptográfico.

    Si está utilizando la autenticación bidireccional para conectarse a los servidores del Nodo Central, debe volver a agregar el contenedor criptográfico.

Como el Asistente de migración no migra esta configuración, es posible que encuentre errores al conectar el equipo a los servidores de Central Node. Para corregir los errores, debe ir a las propiedades de la directiva y configurar los ajustes de conexión.

- Un asistente de conversión por lotes de directivas y tareas estándar. El asistente de conversión por lotes de directivas y tareas solo está disponible en la Consola de administración (MMC). Para obtener más detalles sobre el asistente de conversión por lotes de directivas y tareas, consulte la Ayuda de Kaspersky Security Center.

Para asegurarse de que Kaspersky Endpoint Security funciona correctamente en los servidores, se recomienda agregar archivos importantes para el funcionamiento del servidor a la zona de confianza. Para servidores SQL, debe agregar archivos de base de datos MDF y LDF. Para servidores de Microsoft Exchange, debe agregar archivos CHK, EDB, JRS, LOG y JSL. Puede usar máscaras; por ejemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores.

Las exclusiones de telemetría de EDR no migran de la directiva de Kaspersky Endpoint Agent a la directiva de Kaspersky Endpoint Security. Kaspersky Endpoint Security tiene sus propias herramientas de exclusión: aplicaciones de confianza. El funcionamiento de Kaspersky Endpoint Security está optimizado para que la ausencia de exclusiones de telemetría de EDR individuales no provoquen una carga adicional en el equipo en comparación con Kaspersky Endpoint Agent. Kaspersky Endpoint Security usa telemetría no solo para EDR (KATA), sino también para el funcionamiento de los componentes de protección de la aplicación. Por tanto, no es necesario transferir exclusiones de telemetría de EDR individuales. Si experimenta una disminución del rendimiento del equipo, compruebe el funcionamiento de la aplicación (consulte el paso 7 Comprobación del rendimiento).

3 Licencia de la funcionalidad EDR (KATA)

Para activar Kaspersky Endpoint Security como parte de la solución Kaspersky Anti Targeted Attack Platform, necesita una licencia independiente para el complemento Kaspersky Endpoint Detection and Response (KATA). Puede añadir la clave con la tarea *Añadir clave*. Como resultado, se añadirán dos claves a la aplicación: *Kaspersky Endpoint Security* y *Kaspersky Endpoint Detection and Response (KATA)*.

La licencia del complemento Kaspersky Endpoint Detection and Response (KATA) en equipos con funciones EDR Optimum o EDR Expert previamente activadas implica las siguientes consideraciones especiales:

- Si está utilizando un *archivo clave* para la licencia de Kaspersky Endpoint Security con las funciones EDR Optimum o EDR Expert, no puede añadir una clave aparte para el complemento Kaspersky Endpoint Detection and Response (KATA). Puede pasar a usar un código de activación para la licencia o ponerse en contacto con su proveedor de servicios para obtener un nuevo archivo clave para activar las funciones de Kaspersky Endpoint Security y EDR. El proveedor de servicios proporcionará uno o más archivos clave para la licencia.

- Si está utilizando un *archivo clave* para la licencia de Kaspersky Endpoint Security sin las funciones EDR Optimum o EDR Expert, puede añadir una clave aparte para el complemento Kaspersky Endpoint Detection and Response (KATA) sin tener que volver a emitir los archivos clave.

- Si está utilizando un *código de activación* para la concesión de licencias, el servidor de activación de Kaspersky volverá a emitir automáticamente las claves y las funciones de EDR (KATA) estarán disponibles automáticamente. En este caso, EDR Optimum y EDR Expert estarán desactivadas.

- Kaspersky Endpoint Security le permite agregar hasta dos claves activas: clave de Kaspersky Endpoint Security y clave de tipo complemento. También puede agregar hasta dos claves de reserva. Una clave de reserva de Kaspersky Endpoint Security y una clave de reserva de tipo complemento.

4. **Instalar o actualizar la aplicación Kaspersky Endpoint Security**

   Para migrar la funcionalidad EDR (KATA) durante la instalación o actualización de una aplicación, se recomienda utilizar la tarea de instalación remota. Al crear una tarea de instalación remota, debe seleccionar el componente EDR (KATA) en la configuración del paquete de instalación.

   También puede actualizar la aplicación con los siguientes métodos:

   - Usar el servicio de actualización de Kaspersky.

   - De forma local, utilizando el Asistente de instalación.

   Kaspersky Endpoint Security admite la selección automática de componentes al actualizar la aplicación en un equipo con la aplicación Kaspersky Endpoint Agent instalada. La selección automática de componentes depende de los permisos de la cuenta de usuario que está actualizando la aplicación.

   Si está actualizando Kaspersky Endpoint Security con el archivo EXE o MSI en la cuenta del sistema (SYSTEM), Kaspersky Endpoint Security obtiene acceso a las licencias actuales de las soluciones de Kaspersky. Por lo tanto, si el equipo tiene Kaspersky Endpoint Agent instalado y la solución EDR (KATA) activada, el instalador de Kaspersky Endpoint Security configura automáticamente el conjunto de componentes y selecciona el componente EDR (KATA). Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina Kaspersky Endpoint Agent. La ejecución del instalador MSI con la cuenta del sistema (SYSTEM) se realiza normalmente cuando se actualiza a través del servicio de actualización de Kaspersky o cuando se despliega un paquete de instalación a través de Kaspersky Security Center.

   Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tendrá acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes basándose en un conjunto de componentes de Kaspersky Endpoint Agent. Tras esto, Kaspersky Endpoint Security pasa a utilizar el agente integrado y elimina Kaspersky Endpoint Agent.

   > Kaspersky Endpoint Security admite la actualización sin reiniciar el equipo. Puede seleccionar el modo de actualización de la aplicación en las propiedades de la directiva.

5. **Comprobación del funcionamiento de la aplicación**

   Si, tras instalar o actualizar la aplicación, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

   - Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.

   - Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, asegúrese de haber activado la funcionalidad de agente integrado.

   - Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

6. **Comprobación de la conexión al servidor de Kaspersky Anti Targeted Attack Platform**

Compruebe la conexión al servidor de Kaspersky Anti Targeted Attack Platform. Para ello:

1. Compruebe que dispone de un certificado válido.
2. Compruebe los ajustes de conexión del servidor.
3. Compruebe el registro de eventos.

   Si se establece una conexión al servidor, la aplicación envía el evento *Conexión correcta al servidor de EDR Expert*. Si no hay ningún evento de conexión correcto y no hay eventos con errores de conexión, compruebe la configuración del registro de eventos y active el envío de eventos para Endpoint Detection and Response (KATA).

El estado de conexión del servidor no afecta al estado del equipo en la consola de Kaspersky Security Center. Por tanto, si no hay conexión al servidor, el equipo sigue pudiendo tener el estado *Aceptar*. Compruebe el registro de eventos para verificar la conexión al servidor.

7 Comprobación del rendimiento

Si el rendimiento del equipo se ha ralentizado después de instalar o actualizar una aplicación, puede optimizar la transferencia de datos. Para ello:

1. Desactive el componente EDR (KATA) y verifique que la degradación del rendimiento se deba a EDR (KATA).
2. Para aplicaciones de confianza, desactive la recopilación de telemetría en las operaciones de entrada de la consola (activada de forma predeterminada).
3. Agregue aplicaciones que reduzcan el rendimiento del equipo a la lista de aplicaciones de confianza.
4. Póngase en contacto con el soporte técnico de Kaspersky. Los expertos de soporte le ayudarán a configurar el filtrado de telemetría en Kaspersky Anti Targeted Attack Platform. Esto reducirá la cantidad de tráfico. Si el rendimiento de su equipo se ve afectado por una determinada aplicación, adjunte el paquete de distribución de esa aplicación a la solicitud.

Endpoint Detection and Response Expert (on-premises)



Kaspersky Endpoint Security para Windows admite la integración con las soluciones de Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* es una solución de ciberseguridad empresarial que incluye aplicaciones de Kaspersky que permiten a una organización defenderse contra la mayoría de los tipos de ciberriesgos y cubrir los escenarios de propagación de amenazas más importantes. Los componentes de EDR Expert (on-premises) se implementan en la plataforma abierta de administración única (OSMP). Esta plataforma ejecuta escenarios multiplataforma en una única interfaz y permite integrar aplicaciones de Kaspersky con aplicaciones de terceros en un sistema de seguridad completo.

Uno de los elementos centrales de la solución es *SIEM*. SIEM rastrea los eventos que provienen de todos los componentes y los correlaciona entre sí mediante reglas definidas por el proveedor y el usuario. EDR Expert (on-premises) analiza los registros y la telemetría recibidos de la infraestructura corporativa para detectar ataques automáticamente y permite investigar incidentes utilizando un gráfico de investigación unificado que combina todos los eventos recopilados en EDR Expert (on-premises), incluidos eventos de aplicaciones de Kaspersky y productos de seguridad de la información de terceros.

Para responder a incidentes avanzados, EDR Expert (on-premises) utiliza escenarios predefinidos y definidos por el usuario. También puede usar acciones de respuesta de aplicaciones de terceros y escenarios de respuesta que involucren varias aplicaciones.

Herramientas de Inteligencia contra amenazas

Kaspersky Endpoint Detection and Response utiliza las siguientes herramientas Threat Intelligence:

- Integración con Kaspersky Threat Intelligence Portal, que contiene y muestra información sobre la reputación de los archivos y las direcciones web.
- Base de datos de amenazas de Kaspersky.
- La infraestructura de servicios de nube de Kaspersky Security Network (en lo sucesivo también denominada "KSN"), que proporciona acceso a información de reputación de software, sitios web y archivos en tiempo real de la base de conocimientos de Kaspersky. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de las aplicaciones de Kaspersky ante amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos.

Principio de funcionamiento de la solución

Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y supervisa continuamente los procesos, las conexiones de red abiertas y los archivos que se modifican.

Cuando se instala en modo estándar en la infraestructura de VDI, Kaspersky Endpoint Security admite la integración con EDR Expert (on-premises). Sin embargo, no se garantiza la operatividad del resto de funcionalidades de la aplicación. Para proteger las máquinas virtuales en la infraestructura de VDI, recomendamos utilizar Kaspersky Endpoint Security en modo de Light Agent.

La información sobre los eventos en el equipo (telemetría) se envía al servidor de EDR Expert (on-premises). En este caso, Kaspersky Endpoint Security también envía información sobre las amenazas descubiertas por la aplicación, así como información sobre los resultados del procesamiento de estas amenazas a los servidores de recopilación de telemetría.

La integración de EDR Expert (on-premises) se configura en la consola de Kaspersky Security Center. A continuación, el agente integrado se administra mediante la plataforma abierta de administración única (OSMP), incluida la ejecución de tareas, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Configuraciones de Kaspersky Endpoint Security para trabajar con EDR Expert (on-premises)

Se pueden utilizar las siguientes configuraciones para trabajar con EDR Expert (on-premises):

- **[KES+agente integrado]**. En esta configuración, Kaspersky Endpoint Security actúa como la aplicación que garantiza la seguridad del equipo y como la aplicación para trabajar con EDR Expert (on-premises). El agente integrado para EDR Expert (on-premises) está disponible en Kaspersky Endpoint Security 12.11 para Windows o posterior.

- **[EPP de terceros +EDR Agent]**. En esta configuración, la seguridad de la infraestructura de TI la proporciona la aplicación Endpoint Protection Platform (EPP) de terceros. La interacción con EDR Expert (on-premises) la proporciona Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent (EDR Agent). En esta configuración, EDR Agent es compatible con aplicaciones EPP de terceros. EDR Agent para EDR Expert (on-premises) está disponible en Kaspersky Endpoint Security 12.11 para Windows o posterior.

Integración del agente integrado con EDR Expert (on-premises)

Para integrarse con la solución Kaspersky Endpoint Detection and Response Expert (on-premises), debe añadir el componente Endpoint Detection and Response Expert (on-premises) y configurar Kaspersky Endpoint Security.

Los componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) y Endpoint Detection and Response Expert (on-premises) no son compatibles entre sí.

Se deben cumplir con las siguientes condiciones para que Endpoint Detection and Response Expert (on-premises) funcione:

- La OSMP (Open Single Management Platform) está instalada.
- La aplicación está activada y la funcionalidad se incluye en la licencia.
- El componente Endpoint Detection and Response Expert (on-premises) está activado.
- Los componentes de la aplicación que garantizan el funcionamiento de EDR Expert (on-premises) están activados y operativos. Los siguientes componentes garantizan el funcionamiento de EDR Expert (on-premises):
  - Protección frente a amenazas en archivos.
  - Protección frente a amenazas web.
  - Protección frente a amenazas en el correo.
  - Prevención de exploits.
  - Detección de comportamiento.
  - Prevención de intrusiones en el host.

- Motor de reparación.
- Control de anomalías adaptativo.

La configuración de la integración de EDR Expert (on-premises) implica los siguientes pasos:

1. **Instalación del componente EDR Expert (on-premises)**

   Puede seleccionar el componente EDR Expert (on-premises) durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

   > Debe reiniciar el equipo para terminar de actualizar la aplicación con el nuevo componente.

2. **Activar Endpoint Detection and Response Expert (on-premises)**

   Debe comprar una licencia separada para EDR Expert (on-premises) (complemento de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La funcionalidad está disponible tras añadir una clave diferente para Kaspersky Endpoint Detection and Response Expert (on-premises). Como resultado, se añaden dos claves en el equipo: una para Kaspersky Endpoint Security y una para Kaspersky Endpoint Detection and Response Expert (on-premises).

   La licencia para la funcionalidad independiente de Endpoint Detection and Response Expert (on-premises) es la misma que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad EDR Expert (on-premises) esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

3. **Conexión al servidor de recopilación de telemetría y al servidor de respuesta**

   Kaspersky Endpoint Detection and Response Expert (on-premises) requiere una conexión de confianza entre Kaspersky Endpoint Security y dos servidores:

   - Un *servidor de recopilación de telemetría* es un servidor que es parte de una solución SIEM que recopila, normaliza, correlaciona, analiza y almacena información sobre eventos que ocurren en el equipo.
   - A *servidor de respuesta* es un servidor para recibir y analizar datos, estudiar el comportamiento de los objetos y publicar los resultados de dichos estudios.

   Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). A continuación, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).

   De manera predeterminada, Kaspersky Endpoint Security solo verifica el certificado TLS de los servidores. Para que la conexión sea más segura, también puede habilitar la verificación del equipo en el servidor (autenticación bidireccional). Para activar esta verificación, debe activar la autenticación bidireccional en la configuración del servidor y Kaspersky Endpoint Security. Para usar la autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Cómo conectar un equipo con Kaspersky Endpoint Security a EDR Expert (on-premises) mediante Web Console

   1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
   2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

      Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response Expert (on-premises)**.

5. Active la opción **Endpoint Detection and Response Expert (on-premises) activado**.

6. Para configurar EDR Expert (on-premises), seleccione **Endpoint Detection and Response Expert (versión 8.0 o posterior)** en la lista de soluciones.

7. Configure la conexión de los *servidores de recopilación de telemetría*:

   a. En el bloque **Conexión a servidores de recogida de telemetría**, haga clic en el enlace **Configuración de conexión**.

   b. Configure la conexión de los servidores de recopilación de telemetría:

   - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente.

   - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Tras configurar el servidor, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

   d. Agregue servidores de recopilación de telemetría. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

      Puede añadir varias direcciones de servidores de recopilación de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

   e. Si es necesario, configure la telemetría.

8. Configure la conexión de los *servidores de respuesta*:

   a. En el bloque **Conexión a servidores de respuesta**, configure el ajuste **Enviar solicitud de sincronización al servidor cada (min.)**. Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security recibe tareas de respuesta ante amenazas y envía los resultados de la tarea.

   b. Haga clic en el enlace **Configuración de conexión**.

   c. Configure la conexión con los servidores de respuesta:

      - **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente.

      - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Tras configurar el servidor, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.

        El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   d. Haga clic en **Aceptar**.

   e. Añada servidores de respuesta. Para hacer esto, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

      Puede añadir varias direcciones de servidor de respuesta. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Puede comprobar el estado del componente mediante *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (on-premises)** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Configuración de parámetros de telemetría de EDR Expert (on-premises)

Telemetría es una lista de eventos que han ocurrido en el equipo protegido. Kaspersky Endpoint Security analiza los datos de telemetría y los envía a los servidores de recopilación de telemetría durante la sincronización. Para obtener más información sobre los eventos de telemetría transmitidos, consulte la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises).

Los eventos de telemetría llegan al servidor de manera casi continua. Kaspersky Endpoint Security inicia la sincronización con el servidor cuando se cumple alguna de las siguientes condiciones:

- Se ha agotado el intervalo de sincronización.
- El número de eventos en el búfer sobrepasa el límite superior.

Por lo tanto, de forma predeterminada, la aplicación se sincroniza cada 30 segundos o cada vez que el búfer contiene 1024 eventos. Puede configurar el comportamiento de sincronización en la directiva de Kaspersky Endpoint Security y seleccionar los valores óptimos para que coincidan con la carga de su red (consulte las instrucciones a continuación).

Si no hay conexión entre Kaspersky Endpoint Security y el servidor, la aplicación pone en cola nuevos eventos. Cuando se restablece la conexión, Kaspersky Endpoint Security envía los eventos en cola al servidor en el orden correcto. Para evitar sobrecargar el servidor, Kaspersky Endpoint Security puede omitir algunos eventos. Para activar esta función, puede optimizar la configuración de transmisión de eventos, por ejemplo, para establecer un valor máximo de eventos por hora (consulte las instrucciones que aparecen más adelante).

Para configurar la telemetría, siga estos pasos:

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.
5. Para configurar EDR Expert (on-premises), seleccione **Endpoint Detection and Response Expert (versión 8.0 o posterior)** en la lista de soluciones.
6. Asegúrese de que la casilla de verificación **Enviar telemetría a servidores de recogida de telemetría** está seleccionada en el bloque **Configuración de transmisión de datos**.
7. Si es necesario, active la casilla **Enviar telemetría solo con IOA**. *Indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que puede indicar un ataque dirigido. La aplicación compara el comportamiento en curso en el sistema con estas reglas y registra los eventos que son indicativos de un ataque dirigido. La aplicación utiliza la tecnología de *análisis de transmisión*, que permite el seguimiento en tiempo real de dichos eventos.

8. Si es necesario, configure la sincronización con la configuración del servidor en el bloque **Configuración de transmisión de datos**:

   - **Retraso máximo de transmisión de eventos (seg)**. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.

   - **Número máximo de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos.

9. Si es necesario, desactive la casilla **Activar la limitación de solicitudes** en el bloque **Limitación de solicitudes**.

   Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. Esta opción está activada de forma predeterminada.

10. Configure los ajustes de optimización para enviar eventos al servidor:

    - **Número máximo de eventos por hora**. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60.000 eventos por hora.

    - **Porcentaje de exceso de límite del evento**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.

11. En el bloque **Conexión a servidores de respuesta**, introduzca un valor para el parámetro **Enviar solicitud de sincronización al servidor cada (min.)**.

12. Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre la configuración y las tareas de la aplicación modificada.

13. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Configuración de telemetría de EDR Expert (on-premises)

Para mejorar el rendimiento y optimizar la transmisión de datos al servidor de recopilación de telemetría, puede añadir las exclusiones de telemetría. Por ejemplo, puede elegir no enviar datos de comunicaciones de red de aplicaciones individuales.

> Usar demasiadas reglas puede aumentar la carga sobre el servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos añadir solo las reglas necesarias.

Para crear una exclusión de telemetría en Web Console y Cloud Console:

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de EDR Expert (on-premises)**.
6. En el bloque **Exclusiones generales**, haga clic en el botón **Añadir**.
   Se abre la ventana **Añadir regla de exclusión**.
7. Si es necesario, cambie el estado de la regla. De manera predeterminada, la regla está activada.
8. Introduzca un nombre para la regla.
9. Seleccione la acción que se realizará cuando se active la regla:
   - **No recopilar**. El evento filtrado se excluirá de la telemetría enviada.
   - **Excluir IOA**. El evento de activación de la regla IOA se excluirá de la telemetría enviada.
10. Si la opción **Excluir IOA** está seleccionada, especifique las reglas de IOA que se añadirán a las exclusiones:
    - **Excluir todo**. Cuando se cumpla la condición especificada, la aplicación excluirá de la telemetría los eventos generados según todas las reglas de IOA.
    - **Excluir por GUID**. Especifique el GUID de la regla de IOA. Puede especificar varios GUID mediante el uso de `,`. Para obtener más detalles sobre las reglas de la IOA, consulte la Ayuda de EDR Expert (on-premises).
11. Especifique la condición de filtrado:
    a. Seleccione el nombre del campo que se utilizará para el filtrado.
    b. Seleccione un operador (consulte la tabla que aparece a continuación) y especifique el valor con el que se comparará el valor del campo del evento.

Lista de operadores condicionales

Operador	Descripción
<	Si el valor del campo es menor que el valor especificado en la condición, el evento no pasará el filtro.
≤	Si el valor del campo es menor o igual que el valor especificado en la condición, el evento no pasará el filtro.
=	Si el valor del campo es igual al valor especificado en la condición, el evento no pasará el filtro.
≥	Si el valor del campo es mayor o igual que el valor especificado en la condición, el evento no pasará el filtro.
>	Si el valor del campo es mayor que el valor especificado en la condición, el evento no pasará el filtro.
≠	Si el valor del campo no es igual al valor especificado en la condición, el evento no pasará el filtro.
es como	Si el valor del campo coincide con la máscara especificada en la condición, el evento no pasará el filtro. La aplicación admite los caracteres `*` y `?` al introducir una máscara:
no es como	Si el valor del campo no coincide con la máscara especificada en la condición, el evento no pasará el filtro. La aplicación admite los caracteres `*` y `?` al introducir una máscara:
uno de	Si el valor del campo coincide con uno de los valores de la lista especificada en la condición, el evento se considera filtrado.
ninguno de	Si el valor del campo no coincide con ninguno de los valores de la lista especificada en la condición, el evento se considera filtrado.
es como uno de	Si el valor del campo coincide con una de las máscaras especificadas en la condición, el evento no pasará el filtro. La aplicación admite los caracteres * y ? al introducir una máscara.

Operador	Descripción
no es como uno de	Si el valor del campo no coincide con ninguna de las máscaras especificadas en la condición, el evento no pasará el filtro. La aplicación admite los caracteres * y ? al introducir una máscara.
existe	Si el campo especificado en la condición está presente en el evento, el evento no pasará el filtro.
no existe	Si el campo especificado en la condición no está presente en el evento, el evento no pasará el filtro.
contiene	Si el valor especificado en la condición está presente en el valor del campo, el evento no pasará el filtro.
es igual a	Si el valor del campo es igual al valor especificado en la condición, el evento no pasará el filtro. El análisis no distingue entre mayúsculas y minúsculas.
en lo referente a bits Y	Si el resultado de la operación bit a bit AND (&) entre el valor del campo y el valor especificado en la condición es 1, el evento no pasará el filtro.

12. Si es necesario, puede crear criterios de filtro complejos añadiendo varias condiciones y grupos de condiciones de filtro. También puede añadir condiciones anidadas y grupos de condiciones a un grupo de condiciones. Puede utilizar los siguientes operadores:

    - **Y** significa que el filtro selecciona eventos que cumplen todas las condiciones especificadas.
    - **O** significa que el filtro selecciona eventos que cumplen una de las condiciones especificadas.
    - **NO** (para usar este operador, seleccione la opción **Añadir NO antes**) significa que el filtro selecciona eventos que no cumplen ninguna de las condiciones especificadas.

    Las condiciones y los grupos de condiciones de primer nivel se combinan con el operador **Y**.

13. Si su equipo ejecuta la plataforma abierta de administración única (OSMP), puede analizar la regla de filtrado que ha creado. Para ejecutar el análisis, haga clic en el botón **Comprobar regla**.

    En la ventana que se abre aparecerá una tabla de eventos filtrados por la regla creada. Para obtener más detalles, consulte la Ayuda de EDR Expert (on-premises).

14. Si es necesario, en **Todos los tipos de evento**, añada exclusiones de telemetría por tipo de evento.

    a. Haga clic en el nombre del tipo de evento.

    b. En la ventana que se abre, haga clic en el botón **Configurar manualmente**.

    c. Si es necesario, configure la transmisión de telemetría para el tipo de evento seleccionado usando el interruptor **Enviar evento**. De forma predeterminada, la transmisión de telemetría está activada para todos los tipos de eventos.

    d. En el bloque **Reglas de exclusión**, haga clic en el botón **Añadir**.

    Se abre la ventana **Añadir regla de exclusión**.

    e. Realice las acciones descritas en los pasos 7 a 13 para cada regla que añada.

15. Para algunos tipos de eventos también puede añadir reglas de inclusión para expandir la telemetría recopilada:

    a. En el bloque **Reglas de inclusión**, haga clic en el botón **Añadir**.

    Se abre la ventana **Añadir reglas de inclusión**.

    b. Introduzca un nombre para la regla.

    c. En **Condición**, introduzca valores para los campos que aparecen. El tipo de campos disponibles depende del evento seleccionado.

Las reglas de exclusión tienen prioridad sobre las reglas de inclusión.

16. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Exportación e importación de filtros de eventos de EDR Expert (on-premises)

Puede exportar la lista de exclusiones a un archivo JSON. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad ID de eventos. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de filtros de eventos o para migrar la lista a un servidor diferente.

Usar demasiadas reglas puede aumentar la carga sobre el servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos añadir solo las reglas necesarias.

Cómo exportar e importar filtros de eventos en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
5. En el bloque **Configuración de telemetría → Telemetría de EDR Expert (on-premises)**, haga clic en el botón **Configuración**.
6. Para exportar los filtros de eventos:
   a. Haga clic en **Exportar**.
      En la ventana que se abre, especifique el nombre del archivo JSON al que desee exportar los filtros de eventos y seleccione la carpeta en la que desee guardar este archivo.
   b. Guarde el archivo.
      Kaspersky Endpoint Security exporta los filtros de eventos al archivo JSON.
7. Para importar los filtros de eventos:
   a. Haga clic en **Importar**.
   b. En la ventana que se abre, seleccione el archivo JSON del que importar los filtros de eventos.
   c. Abra el archivo.
      Si ya existen reglas de filtrado de eventos en el equipo, Kaspersky Endpoint Security las reemplaza al importar.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo exportar e importar filtros de eventos en la consola web

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de EDR Expert (on-premises)**.
6. Para exportar los filtros de eventos:
   a. Haga clic en **Exportar**.
   b. En la ventana que se abre, especifique el nombre del archivo JSON al que desee exportar los filtros de eventos y seleccione la carpeta en la que desee guardar este archivo.
   c. Guarde el archivo.

      Kaspersky Endpoint Security exporta los filtros de eventos al archivo JSON.
7. Para importar los filtros de eventos:
   a. Haga clic en **Importar**.
   b. En la ventana que se abre, seleccione el archivo JSON del que importar los filtros de eventos.
   c. Seleccione cómo desea que se importen las reglas de filtrado de eventos: añadiéndolas a reglas existentes o descartando las reglas existentes y reemplazándolas por otras nuevas.
   d. Abra el archivo.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

También puede exportar o importar filtros de eventos en la línea de comandos.

Consideraciones especiales al usar perfiles de política para configurar la integración con EDR Expert (on-premises) y EDR (KATA)

Para configurar la integración con EDR (KATA) para determinados grupos de administración y con EDR Expert (on-premises) para otros como parte de una única directiva, deberá usar perfiles de política. Debe configurar la integración con EDR (KATA) en las propiedades de la directiva, y la integración con EDR Expert (on-premises) para los grupos de administración seleccionados debe configurarse en las propiedades del perfil de política.

El uso de perfiles de política para configurar la integración con EDR Expert (on-premises) tiene las siguientes limitaciones:

- Si configura la integración con EDR Expert (on-premises) en las propiedades de la directiva, esta configuración se aplicará a todos los grupos de administración; no se aplicará la configuración de integración de los perfiles de política.
- Al usar perfiles de política para configurar la integración con EDR Expert (on-premises), no puede usar la Consola de administración (MMC) para administrar directivas. Cuando abra las propiedades de la directiva en la Consola de administración, la configuración de integración de EDR Expert (on-premises) en los perfiles de política se sobrescribirá con la configuración de la directiva, lo que provocará que el componente funcione incorrectamente. Deberá restablecer la configuración del componente Endpoint Detection and Response Expert (on-premises) de acuerdo con las instrucciones siguientes.
- Al usar perfiles de política para configurar la integración con EDR Expert (on-premises), no puede usar directivas secundarias.

Si ya tiene una directiva configurada en una versión anterior del complemento web, debe restablecer la configuración del componente Endpoint Detection and Response Expert (on-premises) para aplicar la configuración de integración con EDR Expert (on-premises) a los dispositivos administrados desde los perfiles de política.

Para restablecer la configuración del componente:

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.
5. Cambie el modo de funcionamiento de **Endpoint Detection and Response Expert (versión 7.1 o anterior)** a **Modo Endpoint Detection and Response Expert (versión 8.0 o anterior)**.
6. Vuelva a **Endpoint Detection and Response Expert (versión 7.1 o anterior)**.
7. Guarde los cambios.

Endpoint Detection and Response Expert (cloud)

La integración de Kaspersky Endpoint Security con Kaspersky Endpoint Detection and Response Expert (cloud) no está disponible temporalmente. Se prevé que esta funcionalidad sea compatible a finales de 2026. Mantenga un registro de nuestras Notas de la versión para estar al tanto de las actualizaciones de la aplicación y las nuevas funciones.



Kaspersky Endpoint Security admite la integración con la solución Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* es una solución de ciberseguridad empresarial en la nube que incluye aplicaciones de Kaspersky que permiten a una organización defenderse contra la mayoría de los tipos de ciberriesgos y cubrir los escenarios de propagación de amenazas más importantes. Los componentes de EDR Expert (cloud) se implementan en Open Single Management Platform (OSMP). Esta plataforma ejecuta escenarios multiplataforma en una única interfaz y permite integrar aplicaciones de Kaspersky con aplicaciones de terceros en un sistema de seguridad completo.

Uno de los elementos centrales de la solución es *SIEM*. SIEM rastrea los eventos que provienen de todos los componentes y los correlaciona entre sí mediante reglas definidas por el proveedor y el usuario. EDR Expert (cloud) analiza los registros y la telemetría recibidos de la infraestructura corporativa para detectar ataques automáticamente y permite investigar incidentes utilizando un gráfico de investigación unificado que combina todos los eventos recopilados en EDR Expert (cloud), incluidos eventos de aplicaciones de Kaspersky y productos de seguridad de la información de terceros.

Para responder a incidentes avanzados, EDR Expert (cloud) utiliza escenarios predefinidos y definidos por el usuario. También puede usar acciones de respuesta de aplicaciones de terceros y escenarios de respuesta que involucren varias aplicaciones.

Herramientas de Inteligencia contra amenazas

Kaspersky Endpoint Detection and Response utiliza las siguientes herramientas Threat Intelligence:

- Integración con Kaspersky Threat Intelligence Portal, que contiene y muestra información sobre la reputación de los archivos y las direcciones web.
- Base de datos de amenazas de Kaspersky.
- La infraestructura de servicios de nube de Kaspersky Security Network (en lo sucesivo también denominada "KSN"), que proporciona acceso a información de reputación de software, sitios web y archivos en tiempo real de la base de conocimientos de Kaspersky. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de las aplicaciones de Kaspersky ante amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos.

Principio de funcionamiento de la solución

Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y supervisa continuamente los procesos, las conexiones de red abiertas y los archivos que se modifican.

La información sobre los eventos en el equipo (telemetría) se envía al servidor de EDR Expert (cloud). En este caso, Kaspersky Endpoint Security también envía información sobre las amenazas descubiertas por la aplicación, así como información sobre los resultados del procesamiento de estas amenazas a los servidores de recopilación de telemetría.

La integración de EDR Expert (cloud) se configura en la consola de Kaspersky Security Center. A continuación, el agente integrado se administra mediante la plataforma abierta de administración única (OSMP), incluida la ejecución de tareas, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Integración del agente integrado con EDR Expert (cloud)

Para configurar la integración con la solución Kaspersky Endpoint Detection and Response (cloud), debe instalar el componente Endpoint Detection and Response Expert (cloud) y configurar Kaspersky Endpoint Security.

Los componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) y Endpoint Detection and Response Expert (on-premises) no son compatibles entre sí.

Condiciones de funcionamiento de EDR Expert (cloud)

Para que EDR Expert (cloud) funcione, se deben cumplir las siguientes condiciones:

- La infraestructura de Kaspersky Endpoint Detection and Response Expert (cloud) está disponible en su región. Para obtener información sobre la disponibilidad de la infraestructura de EDR Expert (cloud) en su región, póngase en contacto con el soporte técnico.
- La OSMP (Open Single Management Platform) está instalada.
- Kaspersky Endpoint Security instalado en modo estándar.
- La aplicación Kaspersky Endpoint Security está activada y la funcionalidad se incluye en la licencia.
- Ha aceptado los términos del Contrato de procesamiento de datos de Kaspersky Endpoint Detection and Response Expert (cloud).
- Endpoint Detection and Response Expert (cloud): el componente está activado.
- Los componentes de la aplicación que garantizan el funcionamiento de EDR Expert (cloud) están activados y operativos:
  - Protección frente a amenazas en archivos.
  - Protección frente a amenazas web.
  - Protección frente a amenazas en el correo.
  - Prevención de exploits.
  - Detección de comportamiento.
  - Prevención de intrusiones en el host.
  - Motor de reparación.
  - Control de anomalías adaptativo.

Pasos para la integración con EDR Expert (cloud)

La configuración de la integración de EDR Expert (cloud) implica los siguientes pasos:

1. **Instalar el componente Endpoint Detection and Response Expert (cloud)**

   Puede seleccionar el componente Endpoint Detection and Response Expert (cloud) durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

   > Debe reiniciar el equipo para terminar de actualizar la aplicación con el nuevo componente.

2. **Activar Kaspersky Endpoint Detection and Response Expert (cloud)**

Debe comprar una licencia independiente para Kaspersky Endpoint Detection and Response Expert (cloud).

La funcionalidad está disponible tras añadir una clave diferente para Kaspersky Endpoint Detection and Response Expert (cloud). Como resultado, se añaden dos claves en el equipo: una para Kaspersky Endpoint Security y una para Kaspersky Endpoint Detection and Response Expert (cloud).

La licencia para la funcionalidad independiente de Endpoint Detection and Response Expert (cloud) es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad EDR Expert (cloud) esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

3. **Conexión al servidor de recopilación de telemetría y al servidor de respuesta**

Kaspersky Endpoint Detection and Response Expert (cloud) requiere una conexión de confianza entre Kaspersky Endpoint Security y dos servidores:

- Un *servidor de recopilación de telemetría* es un servidor que es parte de una solución SIEM que recopila, normaliza, correlaciona, analiza y almacena información sobre eventos que ocurren en el equipo.
- A *servidor de respuesta* es un servidor para recibir y analizar datos, estudiar el comportamiento de los objetos y publicar los resultados de dichos estudios.

Cómo conectar un equipo con Kaspersky Endpoint Security a EDR Expert (cloud) mediante Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (cloud)**.
5. Habilite el componente usando el interruptor **Endpoint Detection and Response Expert (cloud) DESACTIVADO**.
6. Si la directiva actual es una directiva secundaria y la directiva principal prohíbe los cambios en la configuración de integración de EDR Expert (cloud) ("candado" cerrado), puede configurar la herencia de configuración en la sección **Herencia**:
   - **Heredar configuración de conexión de la directiva** (valor predeterminado). La configuración de conexión se heredará de la directiva principal. No podrá editar la configuración.
   - **Usar configuración de conexión personalizada**. Puede configurar los parámetros de la conexión manualmente.
7. La pestaña **Servidor de respuesta** muestra el nombre de dominio completo y el puerto del servidor de respuesta, que se recuperan automáticamente. Si la directiva de seguridad de su infraestructura no le permite conectarse directamente a los servidores de EDR Expert (cloud), puede configurar una conexión a través de un túnel TCP:
   a. Seleccione la casilla **Usar un túnel TCP para respuesta**.
   b. Especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al túnel.
8. Si es necesario, establezca la frecuencia de envío de solicitudes de sincronización al servidor en el campo **Enviar solicitud de sincronización al servidor cada (min.)**. Durante la sincronización, Kaspersky Endpoint Security recibe tareas de respuesta ante amenazas y envía los resultados de la tarea.

9. Vaya a la pestaña **Servidor de recogida de telemetría**.

10. Configure los ajustes de conexión del servidor de recopilación de telemetría:

    a. Haga clic en el enlace **Modificar**.

    b. En la ventana que se abre, seleccione el servidor de recopilación de telemetría en la lista. El recopilador de KUMA sirve como servidor de recopilación de telemetría en EDR Expert (cloud). Para obtener más información, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform.

    Si se produce un error al conectarse al servidor de recopilación de telemetría, seleccione otro servidor. Si no puede conectarse al servidor de recopilación de telemetría, póngase en contacto con Soporte técnico.

    c. Si es necesario, puede configurar una conexión al servidor de recopilación de telemetría a través de un túnel TCP, igual que para el servidor de respuesta.

11. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Puede comprobar el estado del componente mediante *Informe sobre el estado de los componentes de la aplicación*. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (cloud)** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Configuración de parámetros de telemetría de EDR Expert (cloud)

Telemetría es una lista de eventos que han ocurrido en el equipo protegido. Kaspersky Endpoint Security analiza los datos de telemetría y los envía a los servidores de recopilación de telemetría durante la sincronización. Los eventos de telemetría llegan al servidor de manera casi continua. Kaspersky Endpoint Security inicia la sincronización con el servidor cuando se cumple alguna de las siguientes condiciones:

- Se ha agotado el intervalo de sincronización.
- El número de eventos en el búfer sobrepasa el límite superior.

Por lo tanto, de forma predeterminada, la aplicación se sincroniza cada 30 segundos o cada vez que el búfer contiene 1024 eventos. Puede configurar el comportamiento de sincronización en la directiva de Kaspersky Endpoint Security y seleccionar los valores óptimos para que coincidan con la carga de su red (consulte las instrucciones a continuación).

Si no hay conexión entre Kaspersky Endpoint Security y el servidor, la aplicación pone en cola nuevos eventos. Cuando se restablece la conexión, Kaspersky Endpoint Security envía los eventos en cola al servidor en el orden correcto. Para evitar sobrecargar el servidor, Kaspersky Endpoint Security puede omitir algunos eventos. Para activar esta función, puede optimizar la configuración de transmisión de eventos, por ejemplo, para establecer un valor máximo de eventos por hora (consulte las instrucciones que aparecen más adelante).

Para configurar la telemetría, siga estos pasos:

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados → Endpoint Detection and Response Expert (cloud)**.

5. En la ventana que se abre, seleccione la ficha **Configuración de transmisión de datos**.

6. Asegúrese de que la casilla de verificación **Enviar telemetría ACTIVADO** esté seleccionada.

7. Si es necesario, active la funcionalidad **Enviar telemetría solo con IOA**. *Indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que puede indicar un ataque dirigido. La aplicación compara el comportamiento en curso en el sistema con estas reglas y registra los eventos que son indicativos de un ataque dirigido. La aplicación utiliza la tecnología de *análisis de transmisión*, que permite el seguimiento en tiempo real de dichos eventos. De forma predeterminada, la función está desactivada.

8. Si es necesario, configure la sincronización del servidor:

   - **Retraso máximo de transmisión de eventos (seg)**. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.

   - **Número máximo de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos.

9. Vaya a la pestaña **Limitación de solicitudes**.

10. Si es necesario, desactive la limitación de solicitudes mediante el botón de alternancia **Limitación de solicitudes ACTIVADA**.

    Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. Esta opción está activada de forma predeterminada.

11. Configure los ajustes de optimización para enviar eventos al servidor:

    - **Número máximo de eventos por hora**. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora.

    - **Porcentaje de exceso de límite del evento (%)**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.

12. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Exclusiones de telemetría de EDR Expert (cloud)

Para mejorar el rendimiento y optimizar la transmisión de datos al servidor de recopilación de telemetría, puede añadir las exclusiones de telemetría. Por ejemplo, puede elegir no enviar datos de comunicaciones de red de aplicaciones individuales.

> Usar demasiadas reglas puede aumentar la carga sobre el servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos añadir solo las reglas necesarias.

Para crear una exclusión de telemetría en Web Console y Cloud Console:

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de EDR Expert (cloud)**.
6. En el bloque **Exclusiones generales**, haga clic en el botón **Añadir**.
   Se abre la ventana **Añadir regla de exclusión**.
7. Si es necesario, cambie el estado de la regla. De manera predeterminada, la regla está activada.
8. Introduzca un nombre para la regla.
9. Seleccione la acción que se realizará cuando se active la regla:
   - **No recopilar**. El evento filtrado se excluirá de la telemetría enviada.
   - **Excluir IOA**. El evento de activación de la regla IOA se excluirá de la telemetría enviada.
10. Si la opción **Excluir IOA** está seleccionada, especifique las reglas de IOA que se añadirán a las exclusiones:
    - **Excluir todo**. Cuando se cumpla la condición especificada, la aplicación excluirá de la telemetría los eventos generados según todas las reglas de IOA.
    - **Excluir por GUID**. Especifique el GUID de la regla de IOA. Puede especificar varios GUID mediante el uso de `,`. Para obtener más detalles sobre las reglas de la IOA, consulte la Ayuda de EDR Expert (cloud).
11. Especifique la condición de filtrado:
    a. Seleccione el nombre del campo que se utilizará para el filtrado.
    b. Seleccione un operador (consulte la tabla que aparece a continuación) y especifique el valor con el que se comparará el valor del campo del evento.

Lista de operadores condicionales

Operador	Descripción
<	Si el valor del campo es menor que el valor especificado en la condición, el evento no pasará el filtro.
≤	Si el valor del campo es menor o igual que el valor especificado en la condición, el evento no pasará el filtro.
=	Si el valor del campo es igual al valor especificado en la condición, el evento no pasará el filtro.
≥	Si el valor del campo es mayor o igual que el valor especificado en la condición, el evento no pasará el filtro.
>	Si el valor del campo es mayor que el valor especificado en la condición, el evento no pasará el filtro.
≠	Si el valor del campo no es igual al valor especificado en la condición, el evento no pasará el filtro.
es como	Si el valor del campo coincide con la máscara especificada en la condición, el evento no pasará el filtro. La aplicación admite los caracteres `*` y `?` al introducir una máscara:
no es como	Si el valor del campo no coincide con la máscara especificada en la condición, el evento no pasará el filtro. La aplicación admite los caracteres `*` y `?` al introducir una máscara:
uno de	Si el valor del campo coincide con uno de los valores de la lista especificada en la condición, el evento se considera filtrado.
ninguno de	Si el valor del campo no coincide con ninguno de los valores de la lista especificada en la condición, el evento se considera filtrado.
es como uno de	Si el valor del campo coincide con una de las máscaras especificadas en la condición, el evento no pasará el filtro. La aplicación admite los caracteres * y ? al introducir una máscara.
no es como uno de	Si el valor del campo no coincide con ninguna de las máscaras especificadas en la condición, el evento no pasará el filtro. La aplicación admite los caracteres * y ? al introducir una máscara.
existe	Si el campo especificado en la condición está presente en el evento, el evento no pasará el filtro.
no existe	Si el campo especificado en la condición no está presente en el evento, el evento no pasará el filtro.
contiene	Si el valor especificado en la condición está presente en el valor del campo, el evento no pasará el filtro.
es igual a	Si el valor del campo es igual al valor especificado en la condición, el evento no pasará el filtro. El análisis no distingue entre mayúsculas y minúsculas.
en lo referente a bits Y	Si el resultado de la operación bit a bit AND (&) entre el valor del campo y el valor especificado en la condición es 1, el evento no pasará el filtro.

12. Si es necesario, puede crear criterios de filtro complejos añadiendo varias condiciones y grupos de condiciones de filtro. También puede añadir condiciones anidadas y grupos de condiciones a un grupo de condiciones. Puede utilizar los siguientes operadores:

    - **Y** significa que el filtro selecciona eventos que cumplen todas las condiciones especificadas.
    - **O** significa que el filtro selecciona eventos que cumplen una de las condiciones especificadas.
    - **NO** (para usar este operador, seleccione la opción **Añadir NO antes**) significa que el filtro selecciona eventos que no cumplen ninguna de las condiciones especificadas.

    Las condiciones y los grupos de condiciones de primer nivel se combinan con el operador **Y**.

13. Para analizar la regla de filtrado creada, haga clic en el botón **Comprobar regla**.

    En la ventana que se abre aparecerá una tabla de eventos filtrados por la regla creada. Para obtener más detalles, consulte la Ayuda de EDR Expert (cloud).

14. Si es necesario, en **Todos los tipos de evento**, añada exclusiones de telemetría por tipo de evento.

    a. Haga clic en el nombre del tipo de evento.

    b. En la ventana que se abre, haga clic en el botón **Configurar manualmente**.

c. Si es necesario, configure la transmisión de telemetría para el tipo de evento seleccionado usando el interruptor **Enviar evento**. De forma predeterminada, la transmisión de telemetría está activada para todos los tipos de eventos.

d. En el bloque **Reglas de exclusión**, haga clic en el botón **Añadir**.

Se abre la ventana **Añadir regla de exclusión**.

e. Realice las acciones descritas en los pasos 7 a 13 para cada regla que añada.

15. Para algunos tipos de eventos también puede añadir reglas de inclusión para expandir la telemetría recopilada:

a. En el bloque **Reglas de inclusión**, haga clic en el botón **Añadir**.

Se abre la ventana **Añadir reglas de inclusión**.

b. Introduzca un nombre para la regla.

c. En **Condición**, introduzca valores para los campos que aparecen. El tipo de campos disponibles depende del evento seleccionado.

Las reglas de exclusión tienen prioridad sobre las reglas de inclusión.

16. Para aplicar la directiva a los equipos, asegúrese de que los candados estén cerrados (🔒) y guarde los cambios.

Cómo exportar o importar filtros de eventos de EDR Expert (cloud)

Puede exportar la lista de exclusiones a un archivo JSON. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad ID de eventos. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de filtros de eventos o para migrar la lista a un servidor diferente.

Usar demasiadas reglas puede aumentar la carga sobre el servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos añadir solo las reglas necesarias.

Para exportar o importar filtros de eventos en la consola web:

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de Telemetría**.

5. Seleccione la pestaña **Telemetría de EDR Expert (cloud)**.

6. Para exportar los filtros de eventos:

    a. Haga clic en **Exportar**.

    b. En la ventana que se abre, especifique el nombre del archivo JSON al que desee exportar los filtros de eventos y seleccione la carpeta en la que desee guardar este archivo.

    c. Guarde el archivo.

    Kaspersky Endpoint Security exporta los filtros de eventos al archivo JSON.

7. Para importar los filtros de eventos:

    a. Haga clic en **Importar**.

    b. En la ventana que se abre, seleccione el archivo JSON del que importar los filtros de eventos.

    c. Seleccione cómo desea que se importen las reglas de filtrado de eventos: añadiéndolas a reglas existentes o descartando las reglas existentes y reemplazándolas por otras nuevas.

    d. Abra el archivo.

8. Para aplicar la directiva a los equipos, asegúrese de que los candados estén cerrados (🔒) y guarde los cambios.

    1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.

    2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

    Se abre la ventana de propiedades de la directiva.

    3. Seleccione la pestaña **Configuración de la aplicación**.

    4. Vaya a **Configuración general → Configuración de Telemetría**.

    5. Seleccione la pestaña **Telemetría de EDR Expert (cloud)**.

    6. Para exportar los filtros de eventos:

        a. Haga clic en **Exportar**.

        b. En la ventana que se abre, especifique el nombre del archivo JSON al que desee exportar los filtros de eventos y seleccione la carpeta en la que desee guardar este archivo.

        c. Guarde el archivo.

        Kaspersky Endpoint Security exporta los filtros de eventos al archivo JSON.

    7. Para importar los filtros de eventos:

        a. Haga clic en **Importar**.

        b. En la ventana que se abre, seleccione el archivo JSON del que importar los filtros de eventos.

c. Seleccione cómo desea que se importen las reglas de filtrado de eventos: añadiéndolas a reglas existentes o descartando las reglas existentes y reemplazándolas por otras nuevas.

d. Abra el archivo.

8. Para aplicar la directiva a los equipos, asegúrese de que los candados estén cerrados (🔒) y guarde los cambios.

Administración de Cuarentena

Cuarentena es un almacenamiento local especial en el equipo. El usuario puede poner en cuarentena archivos que considere peligrosos para el equipo. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la Cuarentena solo cuando se integra con soluciones de Kaspersky Detection and Response. En otros casos, Kaspersky Endpoint Security coloca el archivo relevante en Copia de seguridad. Para obtener información sobre cómo administrar la cuarentena como parte de las soluciones, consulte la Ayuda de Kaspersky Sandbox, la Ayuda de Kaspersky Endpoint Detection and Response Optimum, la Ayuda de Kaspersky Endpoint Detection and Response Expert, la Ayuda de Kaspersky Anti Targeted Attack Platform y la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security utiliza la cuenta del sistema (SYSTEM) para poner archivos en cuarentena.

Puede configurar los parámetros de la Cuarentena solo en la Consola de Kaspersky Security Center. También puede usar la Consola de Kaspersky Security Center para administrar objetos en cuarentena (restaurar, eliminar, añadir, etc.). Localmente, en el equipo solo puede restaurar el objeto a través de la línea de comando.

Configuración del tamaño máximo de Cuarentena

De forma predeterminada, el tamaño de la Cuarentena está limitado a 1024 MB. Cuando la Cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security deja de enviar los archivos y genera el evento *No hay espacio suficiente en el almacenamiento de Cuarentena*. Para evitar que la cuarentena se quede sin espacio en disco, puede establecer un umbral en el que Kaspersky Endpoint Security genere un evento *El almacenamiento de Cuarentena ya casi no tiene espacio libre*. No puede configurar un período de retención para que los archivos en cuarentena se eliminen automáticamente.

Si la solución Kaspersky Anti Targeted Attack Platform (EDR) está desplegada en su organización, le recomendamos aumentar el tamaño de la Cuarentena. Cuando se realiza un análisis de YARA, es posible que la aplicación se encuentre con un volcado de la memoria de gran tamaño. Si el tamaño del volcado de la memoria excede el tamaño de la Cuarentena, el análisis de YARA finaliza con un error, y el volcado de la memoria no se pone en cuarentena. Recomendamos configurar el tamaño de Cuarentena igual al tamaño total de RAM en el equipo (por ejemplo, 8 GB) o desactivar el límite de tamaño de Cuarentena.

Cómo configurar el tamaño máximo de Cuarentena en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y Almacenamiento**.

4. En el bloque **Cuarentena**, configure el tamaño de Cuarentena:

   - **Limitar el tamaño de Cuarentena a N MB**. Si la casilla de verificación está seleccionada, el espacio de Cuarentena se limitará al tamaño definido como máximo. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Cuando la cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security envía el evento *No hay espacio suficiente en el almacenamiento de Cuarentena* a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación deja de colocar nuevos objetos en cuarentena. Debe vaciar manualmente la Cuarentena.

     Si la casilla de verificación está desactivada, el tamaño de Cuarentena está limitado por el espacio libre en disco disponible.

   - **Notificar cuando se alcanza el almacenamiento de Cuarentena N porcentaje**. Valor umbral de la cuarentena. Por ejemplo, puede establecer el umbral de la cuarentena en 50 %. Cuando la cuarentena alcanza el umbral, Kaspersky Endpoint Security envía el evento correspondiente a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación continúa poniendo en cuarentena nuevos objetos.

     Si esta casilla de verificación está desmarcada, la aplicación no genera eventos cuando se alcanza el umbral de cuarentena.

5. Guarde los cambios.

Cómo configurar el tamaño máximo de la Cuarentena en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Informes y Almacenamiento**.

5. En el bloque **Cuarentena**, configure el tamaño de Cuarentena:

   - **Limitar el tamaño de Cuarentena**. Si la casilla de verificación está seleccionada, el espacio de Cuarentena se limitará al valor especificado. Si la casilla de verificación está desactivada, el tamaño de Cuarentena está limitado por el espacio libre en disco disponible. Esto puede ser necesario para el análisis de YARA, porque la aplicación puede guardar un archivo de volcado de memoria grande.

   - **Tamaño máximo de Cuarentena (MB)**. Si la casilla de verificación está seleccionada, el espacio de Cuarentena se limitará al tamaño definido como máximo. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Cuando la cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security envía el evento *No hay espacio suficiente en el almacenamiento de Cuarentena* a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación deja de colocar nuevos objetos en cuarentena. Debe vaciar manualmente la Cuarentena.

     Si la casilla de verificación está desactivada, el tamaño de Cuarentena está limitado por el espacio libre en disco disponible.

   - **Notificar cuando se alcanza el almacenamiento de Cuarentena (%)**. Valor umbral de la cuarentena. Por ejemplo, puede establecer el umbral de la cuarentena en 50 %. Cuando la cuarentena alcanza el umbral, Kaspersky Endpoint Security envía el evento correspondiente a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación continúa poniendo en cuarentena nuevos objetos.

6. Guarde los cambios.

Envío de datos sobre archivos en Cuarentena a Kaspersky Security Center

Para realizar acciones con objetos en cuarentena en Web Console, debe activar el envío de datos de archivos en Cuarentena al Servidor de administración. Por ejemplo, puede descargar un archivo desde la cuarentena para analizarlo en Web Console. El envío de datos de archivos en Cuarentena debe estar activado para todas las funciones de Kaspersky Sandbox y Kaspersky Endpoint Detection and Response para que funcione.

Cómo activar la transferencia de datos de archivos en Cuarentena en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y Almacenamiento**.
4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, active la casilla **Archivos en cuarentena**.
6. Guarde los cambios.

Cómo activar la transferencia de datos de archivos en Cuarentena en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Integración con KSC**.
5. En el bloque **Transferencia de datos al Servidor de administración**, seleccione la casilla de verificación **Acerca de los archivos en Cuarentena**.
6. Guarde los cambios.

Como resultado, puede ver una lista de archivos, en Cuarentena dentro de su equipo, en la Consola de Kaspersky Security Center. Puede usar la Consola de Kaspersky Security Center para administrar objetos en Cuarentena (restaurar, eliminar, añadir, etc.). Para obtener más información sobre cómo trabajar en la Cuarentena, consulte la Ayuda de Kaspersky Security Center.

Restauración de archivos de la cuarentena

De forma predeterminada, Kaspersky Endpoint Security restaura los archivos a su carpeta original. Si la carpeta de destino se ha eliminado o el usuario no tiene derechos de acceso a esa carpeta, la aplicación sitúa el archivo en la carpeta `%DataRoot%\QB\Restored`. Luego, debe mover el archivo manualmente a la carpeta de destino.

Para restaurar archivos de la cuarentena:

1. En la ventana principal de Web Console, seleccione **Operaciones → Repositorios → Cuarentena**.
2. Esto abre la lista de archivos en cuarentena; en esa lista, elija los archivos que desea restaurar y haga clic en **Restaurar**.

Kaspersky Endpoint Security restaura el archivo. Si la carpeta de destino ya tiene un archivo con el mismo nombre, la aplicación cancela la restauración del archivo. La aplicación guarda una copia del archivo en Cuarentena después de restaurarlo. Para eliminar el archivo, debe vaciar manualmente la Cuarentena.

Supervisión de acciones de EDR

Kaspersky Endpoint Security para Windows 12.9 presenta el centro de supervisión de acciones de EDR. El *centro de supervisión de acciones de EDR* es una consola en la que puede ver el historial de Respuesta ante amenazas de todas las soluciones de Kaspersky Detection and Response. Si su organización tiene implementadas varias instancias de Detection and Response (por ejemplo, EDR Optimum y MDR), Kaspersky Endpoint Security muestra el historial de Respuesta ante amenazas para todas las soluciones. Esto le permite analizar el rendimiento de las soluciones de Detection and Response en un equipo independiente y optimizar la configuración de estas soluciones.

El centro de supervisión proporciona la siguiente información:

- Información sobre las tareas de Respuesta ante amenazas (por ejemplo, la tarea *Terminar proceso*)
- Cambios en las reglas del aislamiento de red y de prevención de ejecución

Si la respuesta a la amenaza encuentra un error relacionado con el acceso a un recurso compartido de red, dicho error se omite en el historial de Respuesta ante amenazas que se muestra.

Para navegar al centro de supervisión de acciones de EDR:

1. En la ventana principal de Web Console, seleccione **Administración de activos → Activos (dispositivos)**.
2. Seleccione un equipo para el cual quiera configurar la configuración local de la aplicación.

   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows 14.2**.

   Se abre la configuración local de la aplicación.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Vaya a **Detection and Response → Historial de respuestas**.

Esto abre la consola del centro de supervisión de acciones de EDR. Puede usar la consola para ver los estados de la tarea Respuesta ante amenazas, la duración de la tarea, los cambios en las reglas y los detalles del iniciador.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security para Windows es compatible con la solución Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* es una solución de gestión de información y eventos (SIEM) para la infraestructura de TI de las organizaciones. KUMA permite detectar, analizar y mitigar las amenazas a la seguridad antes de que puedan causar daños.

Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y supervisa continuamente los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos en el equipo (telemetría) se envía al servidor de Kaspersky Unified Monitoring and Analysis Platform (KUMA). En su consola, KUMA muestra los eventos como una lista sin marca, similar al registro de eventos de Windows.

Kaspersky Endpoint Security no proporciona todas las funciones de un agente para KUMA. La aplicación solo envía eventos a KUMA sin marcado. Para acceder a todas las funciones de KUMA, debe comprar una licencia e implementar la solución de acuerdo con la Guía del administrador de KUMA.

Integración de Kaspersky Endpoint Security con KUMA

La configuración de la integración de KES con KUMA implica los siguientes pasos:

1. En la consola de KUMA, añada un recopilador.
2. En la consola de KUMA, configure un conector para que el recopilador reciba eventos de KES.
3. En la consola de KUMA, active la autenticación bidireccional (opcional).
4. En la directiva de Kaspersky Endpoint Security para Windows, configure las opciones para conectar KES a KUMA.
5. En la consola de KUMA, asegúrese de que los eventos de KES lleguen al inquilino correcto y se procesen mediante las reglas de correlación correctas.

Preparación para la integración de KES con KUMA

Para utilizar KUMA, se deben cumplir las siguientes condiciones:

- Kaspersky Security Center versión 14.2 o superior. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de integración de KUMA.
- La aplicación está activada y la funcionalidad se incluye en la licencia.
- El componente de integración de KUMA está activado.

La preparación para la integración de KES con KUMA consta de los siguientes pasos:

1. **Instalación del componente de integración de KUMA**

   Puede seleccionar el componente de integración de KUMA durante la instalación o la actualización, además de utilizar la tarea *Cambiar componentes de la aplicación*.

   Debe reiniciar el equipo para terminar de actualizar la aplicación con el nuevo componente.

2. **Activación KUMA**

   Además de una licencia de la aplicación de Kaspersky Endpoint Security (por ejemplo, Kaspersky Endpoint Security for Business Standard), necesita una licencia independiente para la integración de Kaspersky Endpoint Security con KUMA (complemento de integración de KUMA con Kaspersky Endpoint Security para Windows).

   Si está instalando la aplicación en modo EDR Agent, necesita una licencia para integrar Kaspersky Endpoint Security con KUMA y una licencia de Kaspersky Anti Targeted Attack Platform (KATA) o una licencia de Kaspersky Managed Detection and Response (MDR). No puede implementar EDR Agent solo para KUMA.

   La funcionalidad está disponible después de agregar la clave KUMA independiente. Como resultado, habrá otra clave activa en el equipo para la integración de Kaspersky Endpoint Security con KUMA.

   La licencia para la funcionalidad independiente de KUMA es la misma licencia que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad KUMA esté incluida en la licencia y en ejecución en la interfaz local de la aplicación.

Conexión de KES a KUMA

Para conectar el equipo con la aplicación Kaspersky Endpoint Security a la solución KUMA:

1. En la consola de KUMA, añada un recopilador con conectores de tipo **tcp**, **udp** o **http**, y especifique la configuración de red básica de la conexión. Para obtener más información sobre la administración de conectores, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform.

2. En la directiva de Kaspersky Endpoint Security, añada las direcciones de los recopiladores de KUMA y especifique la configuración de red de la conexión.

Cómo conectar un equipo con Kaspersky Endpoint Security a KUMA mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione **Directivas**.

3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Integración con KUMA**

5. Seleccione la casilla **Integración con KUMA**.

6. En el bloque **Configuración de la integración**, seleccione la casilla de verificación **$IsKUMATelemetry ? "Activa la transmisión de eventos de Windows a un servidor de KUMA": "Activa la transmisión de eventos de Windows a un servidor de SIEM**.

7. Añada servidores de KUMA:

   a. Haga clic en **Añadir**.

   Esto abre el formulario en el que puede añadir servidores de KUMA.

   b. Seleccione el protocolo para conectarse al servidor de KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   El protocolo para conectarse al recopilador en Kaspersky Endpoint Security debe coincidir con el tipo de conector en KUMA: **http**, **tcp** o **udp**.

   > Al utilizar el protocolo UDP, es posible que se pierdan datos debido a la pérdida de tráfico inherente al protocolo.

   c. Introduzca la dirección del servidor (IPv4, IPv6, FQDN) y el puerto para conectarse al servidor (de forma predeterminada, se especifica el puerto 443).

   Al introducir la dirección del servidor, tenga en cuenta lo siguiente:

   - **TCP**:
     - **Sin TLS**. Puede especificar la dirección IP o el FQDN del servidor.
     - **Con TLS**. Debe especificar únicamente el FQDN del servidor.
   - **HTTP / HTTPS**:
     - **Sin TLS**. Debe especificar explícitamente el protocolo HTTP en la dirección del servidor (por ejemplo, `http://server.com` o `http://10.10.10.100`).
     - **Con TLS**. No es necesario especificar el protocolo (por ejemplo, `https://server.com` o `server.com`).
   - **UDP**. El protocolo UDP no admite el cifrado TLS. Puede especificar la dirección IP o el FQDN del servidor.

   Puede consultar la dirección del servidor en las propiedades del conector en la consola de KUMA. Para obtener más información sobre los conectores de KUMA, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform.

   d. Haga clic en **Aceptar**.

   Kaspersky Endpoint Security se conecta al primer servidor de KUMA de la lista. Si la conexión falla, Kaspersky Endpoint Security se conecta al segundo servidor de KUMA de la lista, y así sucesivamente.

8. Si es necesario, configure el ajuste **Retraso máximo de transmisión de eventos (seg)** en el bloque **Configuración de transmisión de datos**. Cuando se agota el tiempo especificado, Kaspersky Endpoint Security intenta conectarse al mismo recopilador o se conecta al siguiente recopilador de la lista si hay varios recopiladores. El valor predeterminado es 30 segundos.

9. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo conectar un equipo con Kaspersky Endpoint Security a KUMA mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados → Integración con KUMA**.
5. Active la opción **Integración con KUMA ACTIVADA**.
6. Añada servidores de KUMA:

   a. Haga clic en **Añadir**.

   Esto abre el formulario en el que puede añadir servidores de KUMA.

   b. Seleccione el protocolo para conectarse al servidor de KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

   El protocolo para conectarse al recopilador en Kaspersky Endpoint Security debe coincidir con el tipo de conector en KUMA: **http**, **tcp** o **udp**.

   > Al utilizar el protocolo UDP, es posible que se pierdan datos debido a la pérdida de tráfico inherente al protocolo.

   c. Introduzca la dirección del servidor (IPv4, IPv6, FQDN) y el puerto para conectarse al servidor (de forma predeterminada, se especifica el puerto 443).

   Al introducir la dirección del servidor, tenga en cuenta lo siguiente:

   - **TCP**:
     - **Sin TLS**. Puede especificar la dirección IP o el FQDN del servidor.
     - **Con TLS**. Debe especificar únicamente el FQDN del servidor.
   - **HTTP/HTTPS**:
     - **Sin TLS**. Debe especificar explícitamente el protocolo HTTP en la dirección del servidor (por ejemplo, `http://server.com` o `http://10.10.10.100`).
     - **Con TLS**. No es necesario especificar el protocolo (por ejemplo, `https://server.com` o `server.com`).
   - **UDP**. El protocolo UDP no admite el cifrado TLS. Puede especificar la dirección IP o el FQDN del servidor.

   Puede consultar la dirección del servidor en las propiedades del conector en la consola de KUMA. Para obtener más información sobre los conectores de KUMA, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform.

   d. Haga clic en **Aceptar**.

Kaspersky Endpoint Security se conecta al primer servidor de KUMA de la lista. Si la conexión falla, Kaspersky Endpoint Security se conecta al segundo servidor de KUMA de la lista, y así sucesivamente.

7. Si es necesario, configure el ajuste **Retraso máximo al enviar eventos (seg)** en el bloque **Configuración de conexión a servidor**. Cuando se agota el tiempo especificado, Kaspersky Endpoint Security intenta conectarse al mismo recopilador o se conecta al siguiente recopilador de la lista si hay varios recopiladores. El valor predeterminado es 30 segundos.

8. Guarde los cambios.

Puede verificar que la integración de KUMA esté configurada correctamente en la consola de KUMA (para obtener más información, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). Consulte *Informe sobre el estado de los componentes de la aplicación* para verificar el estado operativo del componente en la consola de Kaspersky Security Center. También puede ver el estado operativo de un componente en los informes de la interfaz local de Kaspersky Endpoint Security. El componente **Integración con KUMA** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Establecimiento de una conexión de confianza entre KES y KUMA

Puede establecer una conexión de confianza entre Kaspersky Endpoint Security y un recopilador de KUMA con un conector de tipo tcp o http. No se puede establecer una conexión de confianza con un conector del tipo udp.

Para establecer una conexión de confianza, debe configurar un modo TLS en la configuración del conector. Están disponibles los siguientes modos TLS:

- **Disabled**: No utilizar el cifrado TLS. Esta opción está seleccionada de forma predeterminada.
- **Enabled**: Utilizar el cifrado TLS, pero sin verificar el certificado.
- **Custom PFX with client authentication**: Utilizar el cifrado TLS con un secreto PFX. En este modo, el cliente se autentica mediante un certificado.

Kaspersky Endpoint Security no admite el modo TLS **Custom PFX**. Al integrar KES con KUMA mediante PFX, es necesario autenticar al usuario con una contraseña.

Para configurar una conexión de confianza, necesita un certificado TLS: el *certificado de la autoridad de certificación para el microservicio*. Puede obtener un certificado TLS en la consola de KUMA. Para obtener más información sobre la descarga de certificados TLS, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform. A continuación, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).

Para que la conexión sea más segura, puede habilitar la autenticación adicional del equipo en KUMA (autenticación bidireccional). Para habilitar este tipo de autenticación, debe crear un contenedor criptográfico en una autoridad de certificación externa. Un *contenedor criptográfico* es un archivo PFX que contiene un certificado y una clave privada en formato PKCS#12. A continuación, debe habilitar la autenticación bidireccional en la configuración de KUMA (modo TLS **Custom PFX with client authentication**), habilitar la autenticación bidireccional en Kaspersky Endpoint Security y añadir un archivo PFX a la consola de KUMA y a Kaspersky Endpoint Security.

Cómo configurar una conexión de confianza entre KES y KUMA en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la consola, seleccione **Directivas**.

3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Integración con KUMA**
5. Seleccione la casilla **Integración con KUMA**.
6. En el bloque **Ajustes de conexión a servidores KUMA**, seleccione la casilla de verificación **Usar cifrado TLS**.
7. Configurar la conexión de confianza:
   a. Haga clic en **Ajustes de conexión a servidores KUMA**.
   b. Configure la conexión del servidor:
      - **Tiempo de espera (seg)**. Tiempo máximo de espera de una respuesta del servidor de KUMA (de forma predeterminada, el valor es de 5 segundos). Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de KUMA diferente.
      - **Certificado TLS del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de KUMA. Puede obtener un certificado TLS en la consola de Kaspersky Unified Monitoring and Analysis Platform (consulte las instrucciones en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform).

        Para establecer una conexión de confianza, debe seleccionar el modo TLS **Enabled** en la consola de KUMA.
      - **Utilizar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre KES y KUMA. Para usar la autenticación bidireccional, debe seleccionar el modo TLS **Custom PFX with client authentication** en la configuración del conector de la consola de KUMA (consulte la configuración del conector en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). A continuación, debe descargar un certificado de servidor y establecer una contraseña para proteger el contenedor criptográfico.

        > El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar una conexión de confianza entre KES y KUMA en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados → Integración con KUMA**.
5. Active la opción **Integración con KUMA ACTIVADA**.
6. En **Configuración de conexión a servidor**, active el interruptor **Usar cifrado TLS**.

7. Configurar la conexión de confianza:

   a. Haga clic en **Configuración de conexión**.

   b. Configure la conexión del servidor:

   - **Tiempo de espera (seg)**. Tiempo máximo de espera de una respuesta del servidor de KUMA (de forma predeterminada, el valor es de 5 segundos). Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de KUMA diferente.

   - **Certificado TLS del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de KUMA. Puede obtener un certificado TLS en la consola de Kaspersky Unified Monitoring and Analysis Platform (consulte las instrucciones en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform).

     Para establecer una conexión de confianza, debe seleccionar el modo TLS **Enabled** en la consola de KUMA.

   - **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre KES y KUMA. Para usar la autenticación bidireccional, debe seleccionar el modo TLS **Custom PFX with client authentication** en la configuración del conector de la consola de KUMA (consulte la configuración del conector en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). A continuación, debe descargar un certificado de servidor y establecer una contraseña para proteger el contenedor criptográfico.

     > El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Activar el envío de telemetría al servidor KUMA

De forma predeterminada, el envío de eventos al servidor KUMA está desactivado. Para asegurarse de que KUMA funcione correctamente, debe habilitar el envío de telemetría. Puede seleccionar el origen de un evento desde los registros estándar: *Application*, *Security* o *System*.

Cómo habilitar el envío de telemetría a KUMA en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general → Exclusiones y tipos de objeto**.
5. En el bloque **Configuración de telemetría → Telemetría de KUMA**, haga clic en el botón **Configuración**.

6. Seleccione los registros de eventos que desea usar como fuentes de eventos: *Application*, *Security* o *System*.
   Además de los registros estándar, puede especificar un registro de una aplicación de terceros.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo habilitar el envío de telemetría a KUMA en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de KUMA**.
6. Seleccione los registros de eventos que desea usar como fuentes de eventos: *Application*, *Security* o *System*.
   Además de los registros estándar, puede especificar un registro de una aplicación de terceros.
7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Filtrado de eventos que se enviarán a KUMA

De forma predeterminada, el envío de eventos al servidor KUMA está desactivado. Para asegurarse de que KUMA funcione correctamente, debe habilitar el envío de telemetría. Puede seleccionar el origen de un evento desde los registros estándar: *Application*, *Security* o *System*. Para mejorar el rendimiento y optimizar la transmisión de datos al servidor KUMA, puede agregar o excluir manualmente eventos individuales de la telemetría. Por ejemplo, puede excluir eventos de Sysmon.

Cómo crear una lista de eventos para enviar a KUMA en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones y tipos de objeto**.
5. En el bloque **Configuración de telemetría** → **Telemetría de KUMA**, haga clic en el botón **Configuración**.
6. En la ventana que aparece, configure los filtros de eventos que se enviarán a KUMA.

Puede configurar el filtrado de eventos para los registros *Application*, *Security*, *System* estándar o añadir manualmente otro registro:

a. Abra las propiedades del registro o haga clic en el botón **Añadir** e introduzca el nombre del registro.

b. Seleccione un modo de envío de eventos:

- **Enviar todos los eventos**. En este modo, la aplicación envía todos los eventos del registro de Windows, excepto los eventos añadidos a las reglas de exclusión.
- **Enviar solo eventos seleccionados**. En este modo, la aplicación envía solo los eventos añadidos en las reglas de inclusión.

c. Cree listas de reglas de exclusión o reglas de inclusión para el modo de envío de eventos relevante.

Para agregar reglas, debe especificar el ID del evento en el registro de eventos de Windows. Puede enumerar varios ID de eventos en una regla. Para especificar varios ID de eventos, utilice el carácter de coma ("`,`").

d. Si es necesario, active el registro de eventos usando la casilla de verificación situada junto al nombre del registro.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo crear una lista de eventos para enviar a KUMA en Web Console

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de KUMA**.
6. En la ventana que aparece, configure los filtros de eventos que se enviarán a KUMA.

Puede configurar el filtrado de eventos para los registros *Application*, *Security*, *System* estándar o añadir manualmente otro registro:

a. Abra las propiedades del registro o haga clic en el botón **Añadir** e introduzca el nombre del registro.

b. Seleccione un modo de envío de eventos:

- **Enviar todos los eventos**. En este modo, la aplicación envía todos los eventos del registro de Windows, excepto los eventos añadidos a las reglas de exclusión.
- **Enviar solo eventos seleccionados**. En este modo, la aplicación envía solo los eventos añadidos en las reglas de inclusión.

c. Cree listas de reglas de exclusión o reglas de inclusión para el modo de envío de eventos relevante.

Para agregar reglas, debe especificar el ID del evento en el registro de eventos de Windows. Puede enumerar varios ID de eventos en una regla. Para especificar varios ID de eventos, utilice el carácter de coma (",").

d. Si es necesario, active el registro de eventos usando el interruptor situado junto al nombre del registro.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Exportación e importación de filtros de eventos de KUMA

Puede exportar la lista de exclusiones a un archivo JSON. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad ID de eventos. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de filtros de eventos o para migrar la lista a un servidor diferente.

Usar demasiadas reglas puede aumentar la carga sobre el servidor KUMA y reducir el rendimiento del equipo. Recomendamos añadir solo las reglas necesarias.

Cómo exportar e importar filtros de eventos en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones y tipos de objeto**.
5. En el bloque **Configuración de telemetría** → **Telemetría de KUMA**, haga clic en el botón **Configuración**.
6. Para exportar los filtros de eventos:
   a. Seleccione los registros de eventos con filtros que desee exportar.
   b. Haga clic en el botón → **Exportar**.
   c. En la ventana que se abre, especifique el nombre del archivo JSON al que desee exportar los filtros de eventos y seleccione la carpeta en la que desee guardar este archivo.
   d. Guarde el archivo.

   Kaspersky Endpoint Security exporta los filtros de eventos al archivo JSON.
7. Para importar los filtros de eventos:
   a. Haga clic en el botón → **Importar**.
   b. En la ventana que se abre, seleccione el archivo JSON del que importar los filtros de eventos.

c. Abra el archivo.

Si ya existen reglas de filtrado de eventos en el equipo, Kaspersky Endpoint Security las reemplaza al importar.

8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo exportar e importar filtros de eventos en la consola web

1. En la ventana principal de Web Console, seleccione la pestaña **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de Telemetría**.
5. Seleccione la pestaña **Telemetría de KUMA**.
6. Para exportar los filtros de eventos:

   a. Seleccione los registros de eventos con filtros que desee exportar.

   b. Haga clic en el botón → **Exportar**.

   c. En la ventana que se abre, especifique el nombre del archivo JSON al que desee exportar los filtros de eventos y seleccione la carpeta en la que desee guardar este archivo.

   d. Guarde el archivo.

   Kaspersky Endpoint Security exporta los filtros de eventos al archivo JSON.
7. Para importar los filtros de eventos:

   a. Haga clic en el botón → **Importar**.

   b. En la ventana que se abre, seleccione el archivo JSON del que importar los filtros de eventos.

   c. Abra el archivo.

   Si ya existen reglas de filtrado de eventos en el equipo, Kaspersky Endpoint Security las reemplaza al importar.
8. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

También puede exportar o importar filtros de eventos en la línea de comandos.

Guía de migración de KSWS a KES

A partir de la versión 11.8.0, Kaspersky Endpoint Security para Windows admite la funcionalidad básica de la solución Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* protege los servidores que ejecutan los sistemas operativos Microsoft Windows y los almacenamientos conectados a la red contra virus y otras amenazas de seguridad informática a las que están expuestos los servidores y los almacenamientos conectados a la red al intercambiar archivos. Para obtener información detallada sobre cómo funciona la solución, consulte la Ayuda de Kaspersky Security for Windows Server. A partir de Kaspersky Endpoint Security 11.8.0, puede migrar de Kaspersky Security for Windows Server a Kaspersky Endpoint Security para Windows y usar la misma solución para proteger estaciones de trabajo y servidores.

Requisitos de software

Antes de comenzar la migración de KSWS a KES, asegúrese de que su servidor cumpla con los requisitos de hardware y software de Kaspersky Endpoint Security para Windows. Las listas de versiones de sistemas operativos compatibles son diferentes para KES y KSWS. Por ejemplo, KES no es compatible con servidores que ejecutan Windows Server 2003.

Requisitos mínimos de software para migrar de KSWS a KES:

- Kaspersky Endpoint Security para Windows 12.0.
- Kaspersky Security 11.0.1 para Windows Server.

  Si tiene instalada una versión anterior de Kaspersky Security for Windows Server, le recomendamos que actualice la aplicación a la última versión. El asistente de conversión de directivas y tareas no es compatible con versiones anteriores de Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Si tiene instalada una versión anterior de Kaspersky Security Center, actualícela a la 14.2 o posterior. En esta versión de Kaspersky Security Center, el asistente de conversión por lotes de directivas y tareas le permite migrar directivas a un perfil en lugar de a una directiva. En esta versión de Kaspersky Security Center, el asistente de conversión por lotes de directivas y tareas también le permite migrar una gama más amplia de configuraciones de directivas.
- Kaspersky Endpoint Agent 3.10.

  Si tiene instalada una versión anterior de Kaspersky Endpoint Agent, le recomendamos que actualice la aplicación a la última versión. Kaspersky Endpoint Security soporta la migración de una configuración [KSWS+KEA] a [KES+agente incorporado] a partir de Kaspersky Endpoint Agent 3.10.

Recomendaciones de migración

Al migrar de KSWS a KES, tenga en cuenta las siguientes recomendaciones:

- Planifique el tiempo de migración de KSWS a KES con antelación. Elija un momento en el que los servidores estén funcionando con la carga más ligera; por ejemplo, durante el fin de semana.
- Después de la migración, active los componentes de la aplicación de forma gradual. Es decir: comience, por ejemplo, activando solo el componente frente a amenazas en archivos; a continuación, active otros componentes de protección; luego active los componentes de control, y así sucesivamente. En cada paso, debe asegurarse de que la aplicación funcione correctamente y monitorear el rendimiento del servidor. La arquitectura de KES es distinta de la de KSWS, por lo que el sistema operativo también puede comportarse de manera diferente.
- Realice la migración de forma gradual. Migre primero un solo servidor; luego, varios servidores; a continuación, realice la migración en todos los servidores de la organización.
- Migre los distintos tipos de servidores por separado. Es decir: migre primero, por ejemplo, los servidores de bases de datos, luego los servidores de correo, etc.
- La migración en servidores de carga alta conlleva algunas consideraciones especiales.

Pasos de migración

La migración de KSWS a KES se realiza de forma semiautomática. Esto es necesario debido a las diferentes arquitecturas de las aplicaciones. Para migrar la configuración de directivas, debe ejecutar el asistente de conversión por lotes de directivas y tareas (el asistente de migración). Después de migrar la configuración de la directiva, debe configurar manualmente los ajustes que el asistente de migración no puede migrar automáticamente (por ejemplo, la configuración de la protección con contraseña). Después de la migración, también se recomienda verificar si el asistente de migración ha migrado correctamente todas las configuraciones.

Realice la migración de KSWS a KES en el siguiente orden:

1. **Migración de tareas y directivas de KSWS**

   Después de migrar las directivas y tareas, debe realizar pasos de configuración adicionales. También recomendamos asegurarse de que Kaspersky Endpoint Security proporcione el nivel de seguridad necesario después de la migración desde KSWS.

   > El asistente de conversión por lotes de directivas y tareas para Kaspersky Security for Windows Server solo está disponible en la Consola de administración (MMC). La configuración de directivas y tareas no se puede migrar en Web Console y Kaspersky Security Center Cloud Console.

2. **Instale Kaspersky Endpoint Security**.

Puede instalar Kaspersky Endpoint Security de las siguientes maneras:

- Instalando KES después de eliminar KSWS (recomendado).

  La utilidad kavremover no soporta la administración de KSWS.

- Instalando KES encima de KSWS

3. Activación de KES con una clave de KSWS

4. **Confirme que la aplicación funciona correctamente después de la migración**

   Después de migrar de KSWS a KES, asegúrese de que la aplicación funciona correctamente. Verifique el estado del servidor en la consola (debe ser *Sin inconvenientes*). Asegúrese de que no se notifiquen errores de la aplicación; verifique también la hora de la última conexión al Servidor de administración, la hora de la última actualización de la base de datos y el estado de protección del servidor.

   Preste especial atención a la migración de listas de exclusión, aplicaciones de confianza, direcciones web de confianza y reglas de control de aplicaciones.

Correspondencia de los componentes de KSWS y KES

Al migrar de KSWS a KES, el conjunto de componentes se migra solo cuando la aplicación se instala localmente.

Correspondencia de los componentes de Kaspersky Security for Windows Server y Kaspersky Endpoint Security para Windows

Componente de Kaspersky Security for Windows Server	Componente de Kaspersky Endpoint Security para Windows
Basic functionality	Núcleo de la aplicación
Log Inspection	Inspección de registros
Device Control	Control de dispositivos
Firewall Management	*(no compatible)* Las funciones de firewall de KSWS están a cargo del firewall en el nivel del sistema. En KES, un componente separado es responsable de la funcionalidad del Firewall. Después de la migración, puede configurar el firewall de Kaspersky Endpoint Security.
File Integrity Monitor	Control de integridad del sistema
Exploit Prevention	Prevención de exploits
System Tray Icon	*(no compatible)* Puede configurar la interacción del usuario en la configuración de la interfaz de la aplicación.
Integration with Kaspersky Security Center	Conector de Agente de red
Endpoint Agent	*(no compatible)* En Kaspersky Endpoint Security 11.9.0, el paquete de distribución de Kaspersky Endpoint Agent ya no forma parte del kit de distribución de Kaspersky Endpoint Security. Debe descargar el paquete de distribución de Kaspersky Endpoint Agent por separado.
Network Threat Protection	Protección frente a amenazas en la red
Anti-Cryptor	Detección de comportamiento
Anti-Cryptor for NetApp	*(no compatible)*

Componente de Kaspersky Security for Windows Server	Componente de Kaspersky Endpoint Security para Windows
Traffic Security	Protección frente a amenazas web Protección frente a amenazas en el correo Control Web
On-Demand Scan	Núcleo de la aplicación
ICAP Network Storage Protection	*(no compatible)* Kaspersky Endpoint Security no admite componentes de protección de almacenamiento conectados a la red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(no compatible)* Kaspersky Endpoint Security no admite componentes de protección de almacenamiento conectados a la red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.
Real-Time File Protection	Protección frente a amenazas en archivos
Script Monitoring	*(no compatible)* Supervisión de scripts es controlado por otros componentes, por ejemplo, Protección AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Control de aplicaciones
Performance counters	*(no compatible)*

Correspondencia de la configuración de KSWS y KES

Al migrar directivas y tareas, KES se configura de acuerdo con la configuración de KSWS. La configuración de los componentes de la aplicación que KSWS no tiene se establece con los valores predeterminados.

Application settings

Scalability, interface and scanning settings

La configuración de la aplicación no admite Kaspersky Endpoint Security para Windows.

Configuración de la aplicación

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Scalability settings	*(no migra)* Kaspersky Endpoint Security gestiona todos los procesos de trabajo.
Show System Tray Icon	*(no migra)* En un equipo cliente, se podrá acceder de forma predeterminada tanto a la ventana principal de Kaspersky Endpoint Security como al icono ubicado en el área de notificaciones de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono. Puede configurar la interacción del usuario en la configuración de la interfaz de la aplicación.
Restore file attributes after scanning	*(no migra)* Kaspersky Endpoint Security restaura automáticamente los atributos del archivo después de analizarlo.
Limit CPU usage for scanning threads	*(no migra)* Kaspersky Endpoint Security no limita el uso de la CPU durante el análisis. Puede configurar la tarea para que se ejecute cuando el equipo esté funcionando con una carga mínima.

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Folder for temporary files created during scanning	*(no migra)* Kaspersky Endpoint Security coloca los archivos temporales en la carpeta `C:\Windows\Temp`.
HSM system settings	*(no migra)* Kaspersky Endpoint Security no admite los sistemas HSM.

Security and reliability

La configuración de seguridad de KSWS se migra a la sección **Configuración general**, subsecciones Configuración de la aplicación e Interfaz.

Configuración de seguridad de aplicaciones

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Protect application processes from external threats	**Activar la autoprotección** (subsección **Configuración de la aplicación**)
Apply password protection	*(no migra)* Kaspersky Endpoint Security tiene una función integrada de protección con contraseña (consulte la subsección **Interfaz**).
Perform task recovery	*(no migra)* Kaspersky Endpoint Security solo restaura automáticamente tareas de *Análisis antimalware*. Kaspersky Endpoint Security ejecuta otras tareas según una programación.
Do not start scheduled scan tasks	**Posponer tareas planificadas al funcionar con batería** (subsección **Configuración de la aplicación**)
Stop current scan tasks	*(no migra)* Cuando el equipo recibe alimentación de un UPS, Kaspersky Endpoint Security no detiene las tareas de análisis que ya se están ejecutando.

Connection settings

La configuración de interacción del Servidor de administración se migra a la sección **Configuración general**, subsecciones Configuración de red y Configuración de la aplicación.

Configuración de interacción del Servidor de administración

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Proxy server settings	**Configuración del servidor proxy** (subsección **Configuración de red**)
Do not use proxy server for local addresses	**No usar servidor proxy para direcciones locales** (subsección **Configuración de red**)
Proxy server authentication settings	**Usar autenticación de servidor proxy** (subsección **Configuración de red**) La contraseña de autenticación del servidor proxy no se migra. Después de migrar una directiva, la contraseña debe introducirse manualmente.
Use Kaspersky Security Center as a proxy server when activating the application	**Usar Kaspersky Security Center como servidor proxy para la activación** (subsección **Configuración de la aplicación**)

Run local system tasks

Kaspersky Endpoint Security ignora la configuración para ejecutar tareas del sistema local de Kaspersky Security for Windows Server. Puede configurar el uso de tareas de KES locales en **Tareas locales**, Gestión de tareas. También puede configurar una programación para ejecutar las tareas *Análisis antimalware* y *Actualización de las bases de datos y módulos de la aplicación* en las propiedades de estas tareas.

Supplementary

Trusted zone

La configuración de la zona de confianza de KSWS se migra a la sección **Configuración general**, subsección **Exclusiones**.

Configuración de la zona de confianza

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Object to scan (Exclusions)	**Exclusiones del análisis** (Exclusiones del análisis) Los métodos utilizados por KSWS y KES para seleccionar objetos son diferentes. Al migrar, KES admite exclusiones definidas como archivos individuales o rutas a archivos/carpetas. Si KSWS tiene exclusiones configuradas como un área predefinida o una URL de script, dichas exclusiones no se migran. Después de la migración, debe añadir dichas exclusiones manualmente. Las exclusiones como áreas predefinidas se deben configurar en la configuración de la tarea *Análisis antimalware*. Las exclusiones como direcciones web de scripts se deben añadir a las direcciones web de confianza de Protección frente a amenazas web.
Apply also to subfolders (Exclusions)	**Incluir subcarpetas** (Exclusiones del análisis)
Objects to detect (Exclusions)	**Tipos de objetos detectados** (Exclusiones del análisis)
Exclusion usage scope (Exclusions)	**Componentes de protección** (Exclusiones del análisis) Si se selecciona al menos un componente en KSWS, KES aplica las exclusiones a todos los componentes de la aplicación.
Comment (Exclusions)	**Comentario** (Exclusiones del análisis)
Trusted process (Trusted process)	**Aplicaciones de confianza** Los métodos de selección de procesos/aplicaciones de confianza de KSWS y KES son distintos. Al migrar, KES admite aplicaciones de confianza configuradas como una ruta al archivo ejecutable o máscara. Si KSWS tiene procesos de confianza configurados como un hash de archivo, estos procesos de confianza no se migran. Después de la migración, debe añadir los procesos de confianza manualmente.
Do not check file backup operations (Trusted process)	**No supervisar la actividad de la aplicación** (Aplicaciones de confianza)

Removable drives scan

La configuración del análisis de unidades extraíbles se migra a la sección **Tareas locales**, subsección **Análisis de unidades extraíbles**.

Configuración de Análisis de unidades extraíbles

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Scan removable drives on connection via USB	**Acción al conectar una unidad extraíble**
Scan removable drives if its stored data volume does not exceed (MB)	**Tamaño máximo de la unidad extraíble**

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Acción al conectar una unidad extraíble**: • **Protección máxima**. • **Recomendado**. Los niveles de seguridad de KSWS corresponden a los modos de análisis de KES de la siguiente manera: • Maximum protection – Protección máxima • Recommended – Recomendado • Maximum performance – Recomendado

User permissions for application management

Kaspersky Endpoint Security no admite la asignación de permisos de acceso de usuario para la administración de aplicaciones y la administración de servicios de aplicaciones. Puede configurar los ajustes de acceso para usuarios y grupos de usuarios para administrar la aplicación en Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security no admite la asignación de permisos de acceso de usuario para la administración de aplicaciones y la administración de servicios de aplicaciones. Puede configurar los ajustes de acceso para usuarios y grupos de usuarios para administrar la aplicación en Kaspersky Security Center.

Storages

La configuración del almacenamiento de KSWS se migra a la sección **Configuración general**, subsección Informes y Almacenamiento, y a la sección **Protección frente a amenazas básicas**, subsección Protección frente a amenazas en la red.

Configuración de almacenes

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Backup folder	*(no migra)* Kaspersky Endpoint Security guarda copias de seguridad de los archivos en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Backup size (MB)	**Limitar el tamaño de la copia de seguridad a N MB** (sección **Configuración general** → **Informes y Almacenamiento**)
Threshold value for space available (MB)	*(no migra)* Kaspersky Endpoint Security registra el evento *El almacenamiento de Cuarentena ya casi no tiene espacio libre* cuando se alcanza el umbral del 50 %.
Target folder for restoring objects	*(no migra)* Kaspersky Endpoint Security restaura los archivos a su carpeta original.
Quarantine folder	*(no migra)* Kaspersky Endpoint Security guarda copias de seguridad de los archivos en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Quarantine size (MB)	*(no migra)* Kaspersky Endpoint Security utiliza Copia de seguridad para almacenar objetos probablemente infectados. Durante la migración, Kaspersky Endpoint Security ignora la configuración de Cuarentena.
Threshold value for space available (MB)	*(no migra)* Kaspersky Endpoint Security utiliza Copia de seguridad para almacenar objetos probablemente infectados. Durante la migración, Kaspersky Endpoint Security ignora la configuración de Cuarentena.
Target folder for restoring objects	*(no migra)* Kaspersky Endpoint Security restaura los archivos a su carpeta original.
Unblock automatically in N	**Bloquear dispositivos atacantes durante N min** (sección **Protección frente a amenazas básicas** → **Protección frente a amenazas en la red**)

Real-time server protection

Real-Time File Protection

La configuración de protección de archivos en tiempo real de KSWS se migra a la sección **Protección frente a amenazas básicas**, subsección **Protección frente a amenazas en archivos**.

Configuración de protección de archivos en tiempo real

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Modo de análisis**: • **Modo inteligente**. • **Al ejecutar**. • **Al acceder**. • **Al acceder y modificar**.
Deeper analysis of launching processes	*(no migra)* Kaspersky Endpoint Security solo admite un modo de análisis, el modo Optimal.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Análisis heurístico**: • **Análisis superficial**. • **Análisis medio**. • **Análisis profundo**.
Apply Trusted Zone	*(no migra)* Kaspersky Endpoint Security aplica la zona de confianza a todos los componentes. Puede configurar exclusiones en la configuración de la zona de confianza.
Use KSN for protection	*(no migra)* Kaspersky Endpoint Security usa KSN para todos los componentes de la aplicación.
Block access to network shared resources for the hosts that show malicious activity	*(no migra)* De forma predeterminada, Kaspersky Endpoint Security bloquea el acceso a los recursos compartidos de la red para los hosts que muestran actividad maliciosa.
Launch critical areas scan when active infection is detected	*(no migra)* Kaspersky Endpoint Security no inicia la tarea de análisis de áreas críticas cuando se detecta una infección activa.
Use Kaspersky Sandbox for protection	*(no migra)* De forma predeterminada, Kaspersky Endpoint Security envía objetos para su análisis a Kaspersky Sandbox.
Protection scope	**Cobertura de protección**
Schedule settings	*(no migra)* Kaspersky Endpoint Security utiliza su propia programación para pausar la Protección frente a amenazas en archivos.

KSN Usage

La configuración de KSWS para Kaspersky Security Network se migra a la sección **Protección frente a amenazas avanzadas**, subsección **Kaspersky Security Network**.

Parámetros de Kaspersky Security Network

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Declaración de Kaspersky Security Network** Kaspersky Endpoint Security solicita consentimiento a la Declaración de Kaspersky Security Network cuando se instala la aplicación, se crea una nueva directiva o se activa el uso de Kaspersky Security Network.
Send data about scanned files	*(no migra)* Kaspersky Endpoint Security envía datos sobre los archivos analizados automáticamente si KSN está activado.
Send data about requested URLs	*(no migra)* Kaspersky Endpoint Security envía datos sobre las URL solicitadas automáticamente si KSN está activado.
Send Kaspersky Security Network statistics	**Activar el modo ampliado de KSN**
Accept the terms of the Kaspersky Managed Protection Statement	*(no migra)* Kaspersky Endpoint Security no incluye el servicio KMP.
Action to perform on KSN untrusted objects	*(no migra)* Puede configurar la Acción al detectar una amenaza en la configuración del componente de protección y la configuración de la tarea de análisis.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(no migra)* Puede configurar restricciones de análisis de archivos grandes en la configuración del componente de protección y la configuración de la tarea de análisis.
Use Kaspersky Security Center as KSN Proxy	**Utilizar Servidor de administración como servidor proxy de KSN**
Schedule settings	*(no migra)* No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

Traffic Security

La configuración de seguridad de tráfico de KSWS se migra a la sección **Protección frente a amenazas básicas**, subsecciones **Protección frente a amenazas web** y **Protección frente a amenazas en el correo**, sección **Controles de seguridad**, subsección **Control Web**, sección **Configuración general**, subsección **Configuración de red**.

Configuración de seguridad del tráfico

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Apply URL-based rules	**Control Web** (subsección **Control Web**) Las reglas basadas en URL se migran a reglas independientes en Kaspersky Endpoint Security.
Apply certificate-based rules	*(no migra)* Kaspersky Endpoint Security no admite las reglas basadas en certificados.
Apply rules for web traffic category control	**Control Web** (subsección **Control Web**) Las reglas de bloqueo para el control de categorías de tráfico web se migran a una sola regla de bloqueo en Kaspersky Endpoint Security. Kaspersky Endpoint Security ignora las reglas de autorización para el control de categorías. La correspondencia de las categorías de KSWS y KES se enumera a continuación.
Allow access if the web page can not be categorized	*(no migra)* Kaspersky Endpoint Security permite el acceso si la página web no se puede categorizar.
Allow access to legitimate web resources that can be used to damage a protected device	*(no migra)* Kaspersky Endpoint Security permite el acceso a recursos web legítimos que se pueden usar para dañar el dispositivo protegido.
Allow access to legitimate advertisement	*(no migra)* Puede administrar el acceso a publicidad legítima a través de la categoría de recursos web *Banners* en la configuración de Control Web.

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(no migra)* Kaspersky Endpoint Security solo admite el modo Driver Interceptor.
ICAP-service connection settings	*(no migra)* Kaspersky Endpoint Security no admite ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Modo **Analizar conexiones cifradas** / **Analizar conexiones cifradas siempre** (subsección **Configuración de red**)
Use TLS protocol version	*(no migra)* Kaspersky Endpoint Security analiza el tráfico de red cifrado que se transmite a través de los siguientes protocolos: • SSL 3.0 • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Además, puede bloquear las conexiones SSL 2.0 en la configuración de análisis de conexiones cifradas.
Do not trust web-servers with invalid certificate	**Dirección** (subsección **Configuración de red**)
Intercept ports (Interception area)	**Puertos vigilados** (subsección **Configuración de red**) Durante la migración, KES desactiva las casillas de verificación **Vigilar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky** y **Vigilar todos los puertos de las aplicaciones especificadas**.
Exclude ports (Interception area)	*(no migra)*
Exclude IP addresses (Interception area)	**Configurar direcciones de confianza** (subsección **Configuración de red**)
Exclude processes (Interception area)	**Configurar aplicaciones de confianza** (subsección **Configuración de red**) Durante la migración, KES configura los siguientes parámetros para la aplicación de confianza: • La casilla de verificación **No analizar el tráfico de red** está seleccionada. KES no analiza el tráfico de red para ninguna dirección IP remota ni ningún puerto. • Las otras casillas de verificación en la configuración de la aplicación de confianza no están marcadas.
Security port	*(no migra)*
Use malicious URL database to scan web links	**Contrastar la dirección web en la base de datos de direcciones web maliciosas** (subsección **Protección frente a amenazas web**)
Use anti-phishing database to scan web pages	**Contrastar la dirección web en la base de datos de direcciones web de phishing** (subsección **Protección frente a amenazas web**)
Use KSN for protection	*(no migra)* Kaspersky Endpoint Security usa KSN para todos los componentes de la aplicación.
Use Trusted Zone	*(no migra)* Kaspersky Endpoint Security aplica la zona de confianza a todos los componentes. Puede configurar exclusiones en la configuración de la zona de confianza.
Use heuristic analyzer	**Usar análisis heurístico** (subsecciones **Protección frente a amenazas web** y **Protección frente a amenazas en el correo**)
Security level	*(no migra)* Kaspersky Endpoint Security tiene sus propios niveles de seguridad para los componentes Protección frente a amenazas web y Protección frente a amenazas en el correo. De forma predeterminada, Kaspersky Endpoint Security establece el nivel de seguridad recomendado.
Enable mail threat protection	**Protección frente a amenazas en el correo** (subsección **Protección frente a amenazas en el correo**) **Conectar el complemento de Microsoft Outlook** **Solo mensajes entrantes** (Cobertura de protección) **Analizar al recibir** (Protección del correo)
Schedule settings	*(no migra)* No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

Exploit Prevention

La configuración de prevención de exploits de KSWS se migra a la sección **Protección frente a amenazas avanzadas**, subsección **Prevención de exploits**.

Configuración de prevención de exploits

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Al detectar vulnerabilidades**: • **Bloquear**. • **Informar**.
Notify about abused processes via Terminal Service	*(no migra)* Kaspersky Endpoint Security no admite los servicios de terminales.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(no migra)* Kaspersky Endpoint Security evita constantemente la explotación de procesos vulnerables.
Protected processes	**Activar protección de la memoria de los procesos del sistema** Kaspersky Endpoint Security no admite la selección de procesos protegidos. Solo puede activar la protección de la memoria de los procesos del sistema.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(no migra)* Kaspersky Endpoint Security aplica todas las técnicas de prevención de exploits disponibles.

Network Threat Protection

Los parámetros de Protección frente a amenazas en la red de KSWS se migran a la sección **Protección frente a amenazas básicas**, subsección **Protección frente a amenazas en la red**.

Parámetros de Protección frente a amenazas en la red

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Protección frente a amenazas en la red** Si se elige el modo **Pass-through**, la Protección frente a amenazas en la red está desactivada. Si se elige el modo **Only inform about network attacks** o el modo **Block connections when attack is detected**, la Protección frente a amenazas en la red está activada. Kaspersky Endpoint Security siempre funciona en el modo **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	*(no migra)* Kaspersky Endpoint Security analiza el tráfico continuamente si el componente está activado.
Do not control excluded IP addresses	**Exclusiones**
Schedule settings	*(no migra)* No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

Script Monitoring

Kaspersky Endpoint Security no admite el componente Supervisión de scripts. Supervisión de scripts es controlado por otros componentes, por ejemplo, Protección AMSI.

Website categories

Kaspersky Endpoint Security no admite todas las categorías de Kaspersky Security for Windows Server. Las categorías que no existen en Kaspersky Endpoint Security no se migran. Por lo tanto, las reglas de clasificación de recursos web con categorías no admitidas no se migran.

Categorías de Kaspersky Security for Windows Server	Categorías de Kaspersky Endpoint Security para Windows
Wargaming	Videojuegos
Abortion	*(no migra)*
Lotteries (extended)	Apuestas, loterías, sorteos
Alcohol	Alcohol, tabaco, narcóticos
Anonymous proxy servers	Anonimizadores
Anorexia	*(no migra)*
Rentals for real estate	*(no migra)*
Audio, video and software	Software, audio, vídeo
Banks	Bancos
Blogs	Blogs
Military	Armas, explosivos, asuntos militares
For children	*(no migra)*
Discrimination	Violencia, intolerancia
Home and family	*(no migra)*
Hosting and domain services	Comunicación por Internet
Pets and animals	*(no migra)*
Law and politics	Prohibido por leyes regionales
Restricted by Roskomnadzor (RF)	Prohibido por la ley de la Federación de Rusia
Restricted by Federal Law 436 (RF)	Prohibido por la ley de la Federación de Rusia
Restricted by RF legislation	Prohibido por la ley de la Federación de Rusia
Restricted by global legislation	Prohibido por leyes regionales
Adult dating	Contenido para adultos
Internet services	*(no migra)*
Sex shops	Contenido para adultos
Information technologies	*(no migra)*
Casinos, card games	Apuestas, loterías, sorteos
Books and writing	*(no migra)*
Computer games	Videojuegos
Health and beauty	*(no migra)*
Culture and society	*(no migra)*
LGBT	Contenido para adultos
Lotteries	Apuestas, loterías, sorteos
Medicine	*(no migra)*
Fashion	*(no migra)*
Music	*(no migra)*
Drugs	Alcohol, tabaco, narcóticos
Violence	Violencia, intolerancia
Discontent	*(no migra)*
Illegal drugs	Alcohol, tabaco, narcóticos
Hate and discrimination	Violencia, intolerancia

Categorías de Kaspersky Security for Windows Server	Categorías de Kaspersky Endpoint Security para Windows
Obscene vocabulary	Blasfemias, obscenidades
Lingerie	Contenido para adultos
News	Medios de comunicación
Nudism	Contenido para adultos
Education	*(no migra)*
Online shopping	Tiendas en línea
All communication media	Comunicación por Internet
Payment by credit cards	Sistemas de pago
Online shopping (own payment system)	Tiendas en línea
Online encyclopedias	*(no migra)*
Online banking	Bancos
Weapons	Armas, explosivos, asuntos militares
Fishing and hunting	*(no migra)*
Payment systems	Sistemas de pago
Job search	Búsqueda de trabajo
Search engines	*(no migra)*
Police decision (JP)	Prohibido por la policía de Japón
Trusted by KPSN	*(no migra)*
Untrusted by KPSN	*(no migra)*
Porn	Contenido para adultos
Media hosting and streaming	Medios de comunicación
Web Mail	Correo electrónico basado en Web
Traveling	*(no migra)*
TV and radio	Medios de comunicación
Teasers and ads services	Banners
Religion	Religiones, asociaciones religiosas
Restaurants, cafe and food	*(no migra)*
Dating sites	Sitios de contactos
Sex education	Contenido para adultos
Social networks	Redes sociales
Sport	*(no migra)*
Betting	Apuestas, loterías, sorteos
Suicide	Violencia, intolerancia
Tobacco	Alcohol, tabaco, narcóticos
Torrents	Archivos torrent
Mentioned in Federal list of extremists (RF)	Prohibido por la ley de la Federación de Rusia
File sharing	Uso compartido de archivos
Pharmacy	*(no migra)*
Hobby and entertainment	*(no migra)*
Chats and forums	Chats, foros, mensajería instantánea
Schools and universities pages	*(no migra)*

Categorías de Kaspersky Security for Windows Server	Categorías de Kaspersky Endpoint Security para Windows
Astrology and esoterica	*(no migra)*
Extremism and racism	Violencia, intolerancia
E-commerce	Tiendas en línea
Erotic	Contenido para adultos
Humor	*(no migra)*

Local activity control

Applications Launch Control

La configuración de Control de aplicaciones de KSWS se migra a la sección **Controles de seguridad**, subsección **Control de aplicaciones**.

Configuración de Control de inicio de aplicaciones

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Operation mode: • **Statistics only** • **Active**	**Action** (Control de aplicaciones): • **Probar reglas**. • **Aplicar reglas**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(no migra)* Kaspersky Endpoint Security analiza la aplicación cada vez que intenta ejecutarse.
Deny the command interpreters launch with no command to execute	*(no migra)* Kaspersky Endpoint Security permite ejecutar intérpretes de comandos si no están prohibidos por Control de aplicaciones.
Rules	**Reglas de Control de aplicaciones** *(compatible con limitaciones)* Kaspersky Endpoint Security 11.11.0 incorpora soporte para la migración de las reglas de Control de ejecución de aplicaciones. La funcionalidad de migración de la regla de Control de ejecución de aplicaciones tiene algunas limitaciones. De manera predeterminada, el Control de ejecución de aplicaciones de KSWS incluye dos reglas: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Si al menos una regla de origen de KSWS es del tipo **Allow**, KES crea una nueva regla de autorización durante la migración, **Aplicaciones con certificados raíz de confianza**. Esto quiere decir que el Control de aplicaciones de KES utiliza una regla única para autorizar los scripts de confianza en ejecución, los paquete de MSI y los archivos ejecutables. Si ambas reglas de origen de KSWS son del tipo **Deny**, KES no añade las reglas para la administración de aplicaciones con certificados raíz de confianza.
Apply rules to executable files	*(no migra)* El alcance de la aplicación de la regla no se puede configurar en la configuración de Control de aplicaciones de KES. El Control de aplicaciones de KES aplica reglas a todos los tipos de archivos: archivos ejecutables, scripts y paquetes de MSI. Si todos los tipos de archivos se incluyen en el alcance de la aplicación de la regla en KSWS, KES traslada las reglas de KSWS durante la migración. Si se excluye algún tipo de archivo del alcance de la aplicación de la regla en KSWS, KES también traslada las reglas de KSWS durante la migración, pero se selecciona **Probar reglas** como la acción de Control de aplicaciones.
Monitor loading of DLL modules	**Supervisar la carga de los módulos DLL (incrementa significativamente la carga del sistema)**
Apply rules to scripts and MSI packages	*(no migra)* El alcance de la aplicación de la regla no se puede configurar en la configuración de Control de aplicaciones de KES. El Control de aplicaciones de KES aplica reglas a todos los tipos de archivos: archivos ejecutables, scripts y paquetes de MSI. Si todos los tipos de archivos se incluyen en el alcance de la aplicación de la regla en KSWS, KES traslada las reglas de KSWS durante la migración. Si se excluye algún tipo de archivo del alcance de la aplicación de la regla en KSWS, KES traslada las reglas de KSWS durante la migración, pero se selecciona **Probar reglas** como la acción de Control de aplicaciones.

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Deny applications untrusted by KSN	*(no migra)* Kaspersky Endpoint Security no tiene en cuenta la reputación de las aplicaciones y permite o deniega la ejecución de aplicaciones de acuerdo con las reglas.
Allow applications trusted by KSN	Durante la migración, KES añade una regla de permiso nueva. La categoría KL **Otro software\Aplicaciones de confianza de acuerdo con la reputación en KSN** se especifica como condición de activación de reglas.
Users and / or user groups allowed to run applications trusted by KSN	**Usuarios y sus derechos** en una regla de permiso de Control de aplicaciones que incluye la categoría KL **Otro software\Aplicaciones de confianza de acuerdo con la reputación en KSN**.
Automatically allow software distribution via applications and packages listed	El Control de distribución de software en KSWS y KES funciona diferente. Durante la migración, KES añade reglas nuevas para las aplicaciones que tienen activada la distribución automática de software. El hash del archivo está especificado como la condición de activación de la regla.
Always allow software distribution via Windows Installer	El Control de distribución de software en KSWS y KES funciona diferente. Durante la migración, KES añade reglas nuevas para las aplicaciones que tienen activada la distribución automática de software (**Software distribution applications and packages allowed**). El hash del archivo está especificado como la condición de activación de la regla. La casilla **Actualizadores de confianza** está activada en las propiedades de la cuenta.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(no migra)*
Software distribution applications and packages allowed	El Control de distribución de software en KSWS y KES funciona diferente. Durante la migración, KES añade reglas nuevas para las aplicaciones que tienen activada la distribución automática de software. El hash del archivo está especificado como la condición de activación de la regla. La casilla **Actualizadores de confianza** está activada en las propiedades de la cuenta.
Schedule settings	*(no migra)* Si se configura una programación para el componente en la configuración de KSWS, el componente de Control de aplicaciones se activa durante la migración. Si no se configura una programación para el componente en la configuración de KSWS, el Control de aplicaciones estará desactivado durante la migración. No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

Device Control

La configuración de Control de dispositivos de KSWS se migra a la sección **Controles de seguridad**, subsección **Control de dispositivos**.

Configuración de Control de dispositivos

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Operation mode: • **Active** • **Statistics only**	*(no migra)* Control de aplicaciones funciona en modo *Active*. Auditoría proporciona continuamente estadísticas de conexión de dispositivos.
Allow using all external devices when the Device Control task is not running	*(no migra)* Control de dispositivos siempre está activado mientras Kaspersky Endpoint Security se está ejecutando.
Device Control rules	**Dispositivos de confianza** Durante la migración, Kaspersky Endpoint Security ignora las reglas de KSWS desactivadas.
Schedule settings	*(no migra)* Kaspersky Endpoint Security utiliza su propio horario para acceder a ciertos tipos de dispositivos.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security no admite componentes de protección de almacenamiento conectados a la red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.

ICAP Network Storage Protection

Kaspersky Endpoint Security no admite componentes de protección de almacenamiento conectados a la red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security no admite Anti-Cryptor para NetApp. La funcionalidad de Anti-Cryptor la proporcionan otros componentes de la aplicación, como Detección de comportamiento.

Network activity control

Firewall Management

Kaspersky Endpoint Security no admite la administración de firewall de KSWS. Las funciones de firewall de KSWS están a cargo del firewall en el nivel del sistema. Después de la migración, puede configurar el firewall de Kaspersky Endpoint Security.

Anti-Cryptor

La configuración de red de Anti-Cryptor se migra a la sección **Protección frente a amenazas avanzadas**, subsección **Detección de comportamiento**.

Configuración de Anti-Cryptor

Configuración de KSWS	Configuración de KES
Operation mode: • **Statistics only** • **Active**	**Al detectar cifrado externo de carpetas compartidas**: • **Informar**. • **Bloquear**.
Heuristic analyzer	*(no migra)* Kaspersky Endpoint Security no utiliza el análisis heurístico para Detección de comportamiento.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(no migra)* Kaspersky Endpoint Security evita el cifrado de todas las carpetas de red compartidas del equipo protegido.
Exclusions	*(no migra)* Kaspersky Endpoint Security tiene sus propias exclusiones para el componente Detección de comportamiento. Puede añadir manualmente exclusiones después de la migración.
Schedule settings	*(no migra)* No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

System Inspection

File Integrity Monitor

La configuración de File Integrity Monitor de KSWS se migran a la sección **Controles de seguridad**, subsección **Control de integridad del sistema**.

Configuración del monitor de integridad de archivos

Configuración de KSWS	Configuración de KES
Log information about file operations that appear during the monitor interruption period	*(no migra)* Kaspersky Endpoint Security no registra eventos para las operaciones de archivos realizadas durante la interrupción del monitor.
Block attempts to compromise the USN log	*(no migra)* Kaspersky Endpoint Security no bloquea los intentos de vulnerar el registro de USN.
Monitoring scope	**Cobertura de supervisión → Archivo** *(compatible con limitaciones)* Los registros de la cobertura de supervisión desactivados no migran hacia KES. Kaspersky Endpoint Security añade únicamente los registros activados a la cobertura de supervisión.
Trusted users	**Usuarios o grupos de usuarios de confianza**
File operation markers	**Marcadores de operaciones con archivos**
Calculate checksum for the file if possible	**Hash**
Exclusions	**Exclusiones → Archivo**

Log Inspection

La configuración de Inspección de registros de KSWS se migra a la sección **Controles de seguridad**, subsección **Inspección de registros**.

Configuración de inspección de registros

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Apply custom rules for log inspection	*(no migra)* Kaspersky Endpoint Security aplica todas las reglas personalizadas activadas.
Custom rules	**Reglas personalizadas** La regla predefinida **A service was installed in the system (for Server 2003 OS)** no migra hacia KES.
Apply predefined rules for log inspection	*(no migra)* Kaspersky Endpoint Security aplica todas las reglas predefinidas activadas.
Predefined rules	**Reglas predefinidas**
Password brute-force detection	**Detección de ataque de fuerza bruta**
Network logon detection	**Detección de inicio de sesión de red**
Exclusions (IP addresses)	**Exclusiones** (Dirección IP)
Exclusions (users)	**Exclusiones** (Usuarios)
Schedule settings	*(no migra)* No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

Logs and notifications

Task logs

La configuración de registros de KSWS se migra a la sección **Configuración general**, subsecciones **Interfaz** e **Informes y almacenamiento**.

Configuración de registros

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Event logging	**Notificaciones** (subsección **Interfaz**)
Logs folder	*(no migra)* Kaspersky Endpoint Security guarda los informes en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Remove task logs older than N day(s)	*(no migra)* Puede configurar el período de almacenamiento para informes de KES en **Configuración general**, **Informes y almacenamiento**.
Remove from the audit log events N day(s)	*(no migra)* Kaspersky Endpoint Security aplica limitaciones de almacenamiento de informes a todos los informes, incluidos los informes de auditoría del sistema.
SIEM Integration	*(no migra)* Puede configurar la integración con SIEM en Kaspersky Security Center.

Event notifications

La configuración de las notificaciones de KSWS se migra a la sección **Configuración general**, subsección **Interfaz**.

Configuración de notificaciones

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Notifications	**Notificaciones**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(no migra)* Kaspersky Endpoint Security no admite la modificación del texto de notificación. Kaspersky Endpoint Security muestra notificaciones estándar.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Solo los parámetros de notificaciones por correo se migran a Kaspersky Endpoint Security – **Configuración de notificaciones por correo** (bloque **Notificaciones**). No se admiten otros métodos para notificar a los administradores.
Application database is out of date	**Enviar la notificación "Bases de datos desactualizadas" si las bases de datos no se han actualizado**
Application database is extremely out of date	**Enviar la notificación "Bases de datos muy desactualizadas" si las bases de datos no se han actualizado**
Critical areas scan has not been performed for a long time	*(no migra)* Kaspersky Endpoint Security genera un evento de Análisis de áreas críticas perdido después de tres días.

Interaction with Administration Server

La configuración de interacción del Servidor de administración de KSWS se migra a la sección **Configuración general**, subsección **Informes y almacenamiento**.

Configuración de interacción del Servidor de administración

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Quarantined files	**Archivos en cuarentena**
Backed up files	**Archivos de la copia de seguridad**
Blocked hosts	*(no migra)* Kaspersky Endpoint Security envía automáticamente datos sobre hosts bloqueados.

Tasks

Activating the application

Kaspersky Endpoint Security no admite la tarea *Application activation* (KSWS). Puede crear una tarea *Añadir clave* (KES), añadir una clave de licencia al Paquete de instalación o activar la distribución automática de claves de licencia.

Copying Updates

La configuración de la tarea *Copying Updates* (KSWS) se migra a la tarea *Actualización de las bases de datos y módulos de la aplicación* (KES).

Configuración de la tarea Copia de actualizaciones

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Origen de actualizaciones**: • **Kaspersky Security Center**. • **Servidores de actualizaciones de Kaspersky**. • **Especificado por el usuario**.
Use Kaspersky update servers if specified servers are not available	*(no migra)* Kaspersky Endpoint Security permite seleccionar múltiples orígenes de actualizaciones, incluidos los servidores de actualización de Kaspersky. Si el primer origen de actualización no está disponible, Kaspersky Endpoint Security le permite obtener actualizaciones de otro origen en la lista.
Use proxy server settings to connect to Kaspersky update servers	*(no migra)* Kaspersky Endpoint Security utiliza el servidor proxy para todos los componentes. Puede configurar la conexión del servidor proxy en las opciones de red de la aplicación.
Use proxy server settings to connect to other servers	*(no migra)* Kaspersky Endpoint Security utiliza el servidor proxy para todos los componentes. Puede configurar la conexión del servidor proxy en las opciones de red de la aplicación.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(no migra)* Kaspersky Endpoint Security copia las actualizaciones de las bases de datos y las actualizaciones críticas de los módulos de la aplicación en un solo paquete.
Folder for local storage of copied updates	**Copiar las actualizaciones a la carpeta**

Baseline File Integrity Monitor

La configuración de la tarea *Baseline File Integrity Monitor* (KSWS) se migra a la tarea *Comprobación de la integridad del sistema* y a la sección de directivas **Controles de seguridad**, subsección **Control de integridad del sistema**.

Configuración de la tarea del Monitor de integridad de archivos de línea de base

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Hash calculation algorithm: • **MD5** • **SHA256**.	*(no migra)* Kaspersky Endpoint Security utiliza el algoritmo SHA256 para el cálculo de la suma de verificación.
Scan scope	**Cobertura de supervisión** (subsección **Control de integridad del sistema**)

Database Update

La configuración de la tarea *Database Update* (KSWS) se migra a la tarea *Actualización de las bases de datos y módulos de la aplicación* (KES).

Configuración de la tarea Actualización de las bases de datos

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Origen de actualizaciones**: • **Kaspersky Security Center**. • **Servidores de actualizaciones de Kaspersky**. • **Especificado por el usuario**.
Use Kaspersky update servers if specified servers are not available	*(no migra)* Kaspersky Endpoint Security permite seleccionar múltiples orígenes de actualizaciones, incluidos los servidores de actualización de Kaspersky. Si el primer origen de actualización no está disponible, Kaspersky Endpoint Security le permite obtener actualizaciones de otro origen en la lista.
Use proxy server settings to connect to Kaspersky update servers	*(no migra)* Kaspersky Endpoint Security utiliza el servidor proxy para todos los componentes. Puede configurar la conexión del servidor proxy en las opciones de red de la aplicación.
Use proxy server settings to connect to other servers	*(no migra)* Kaspersky Endpoint Security utiliza el servidor proxy para todos los componentes. Puede configurar la conexión del servidor proxy en las opciones de red de la aplicación.
Lower the load on the disk I/O	*(no migra)*

Software modules updates

La configuración de la tarea *Software Modules Update* (KSWS) se migra a la tarea *Actualización de las bases de datos y módulos de la aplicación* (KES).

Configuración de la tarea Actualización de módulos de software

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Origen de actualizaciones**: • **Kaspersky Security Center**. • **Servidores de actualizaciones de Kaspersky**. • **Especificado por el usuario**.
Use Kaspersky update servers if specified servers are not available	*(no migra)* Kaspersky Endpoint Security permite seleccionar múltiples orígenes de actualizaciones, incluidos los servidores de actualización de Kaspersky. Si el primer origen de actualización no está disponible, Kaspersky Endpoint Security le permite obtener actualizaciones de otro origen en la lista.
Use proxy server settings to connect to Kaspersky update servers	*(no migra)* Kaspersky Endpoint Security utiliza el servidor proxy para todos los componentes. Puede configurar la conexión del servidor proxy en las opciones de red de la aplicación.
Use proxy server settings to connect to other servers	*(no migra)* Kaspersky Endpoint Security utiliza el servidor proxy para todos los componentes. Puede configurar la conexión del servidor proxy en las opciones de red de la aplicación.

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Copy and install critical software modules updates	**Instalar actualizaciones críticas y aprobadas**
Only check for critical software updates available	*(no migra)* Kaspersky Endpoint Security comprueba continuamente la disponibilidad de actualizaciones críticas para módulos de la aplicación.
Allow operating system restart	*(no migra)* Kaspersky Endpoint Security solicita al usuario permiso para reiniciar el equipo.
Receive information about available scheduled software modules updates	*(no migra)* Kaspersky Endpoint Security muestra notificaciones sobre actualizaciones de módulos de software.

Rollback of Application Database Update

La configuración de la tarea *Rollback of Application Database Update* (KSWS) se migra a la tarea *Revertir actualización* (KES). La nueva tarea (KES) *Revertir actualización* tiene una programación de inicio de tarea: *Manualmente*.

On-Demand Scan

La configuración de la tarea *On-Demand Scan* (KSWS) se migra a la tarea *Análisis antimalware* (KES).

Configuración de la tarea Análisis antivirus

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Scan scope	**Cobertura del análisis**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Nivel de seguridad**: • **Máximo**. • **Recomendado**. • **Mínimo**. La configuración del nivel de seguridad es diferente en KSWS y KES.
Objects to scan: • **All objects** • **Objects scanned by format** • **Objects scanned according to list of extensions specified in anti-virus database** • **Objects scanned by specified list of extensions**	**Tipos de archivos**: • **Todos los archivos**. • **Analizar archivos por formato**. • **Analizar archivos por extensión**. Kaspersky Endpoint Security no permite la creación de listas de extensiones personalizadas. Kaspersky Endpoint Security reemplaza el valor **Objects scanned by specified list of extensions** con el valor **Analizar archivos por extensión**.
Subfolders	**Incluir subcarpetas**
Subfiles	*(no migra)*
Scan disk boot sectors and MBR	*(no migra)*
Scan alternate NTFS streams	*(no migra)*
Scan only new and modified files	**Analizar solamente archivos nuevos y modificados**
Scan of compound objects: • **All archives** • **All SFX archives** • **All email databases** • **All packed objects** • **All plain email** • **All embedded OLE objects**	**Análisis de archivos compuestos**: • **Analizar archivos**. • **Analizar archivos comprimidos protegidos por contraseña**. • **Analizar paquetes de distribución**. • **Analizar archivos de formatos de correo electrónico**. • **Analizar archivos en formatos de Microsoft Office**.
Action to perform on infected and other objects: • **Disinfect** • **Disinfect. Remove if disinfection fails** • **Remove** • **Perform recommended action** • **Notify only**	**Acción al detectar una amenaza**: • **Desinfectar; eliminar si la desinfección falla**. • **Desinfectar; informar si falla la desinfección**. • **Informar**.

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Action to perform on probably infected objects: • **Quarantine** • **Remove** • **Perform recommended action** • **Notify only**	*(no migra)* Kaspersky Endpoint Security aplica la acción si se detecta alguna amenaza.
Perform actions depending on the type of object detected	*(no migra)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(no migra)*
Exclude files	*(no migra)* Kaspersky Endpoint Security aplica la zona de confianza a todos los componentes. Puede configurar exclusiones en la configuración de la zona de confianza.
Do not detect	*(no migra)*
Stop scanning if it takes longer than N sec	**Omitir archivos analizados durante más de N s**
Do not scan compound objects larger than N MB	**No descomprimir archivos compuestos de gran tamaño**
Use iSwift technology	**Tecnología iSwift**
Use iChecker technology	**Tecnología iChecker**
Action on the offline files: • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(no migra)* Kaspersky Endpoint Security analiza archivos fuera de línea en su totalidad.

Application Integrity Check

La configuración de la tarea *Application Integrity Control* (KSWS) se migra a la tarea *Comprobación de integridad de la aplicación* (KES).

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security no admite la tarea *Applications Launch Control Generator*. Puede generar reglas en Configuración de Control de aplicaciones.

Rule Generator for Device Control

Kaspersky Endpoint Security no admite la tarea *Rule Generator for Device Control*. Puede generar reglas de acceso en Configuración de Control de dispositivos.

Migración de componentes de KSWS

Antes de la instalación local, Kaspersky Endpoint Security comprueba el equipo para buscar aplicaciones de Kaspersky. Si Kaspersky Security for Windows Server está instalado en el equipo, KES detecta el conjunto de componentes de KSWS que están instalados y selecciona los mismos componentes para la instalación.

Los componentes de KES que KSWS no incluye se instalan de la siguiente manera:

- Protección AMSI, Prevención de intrusiones en el host y Motor de reparación se instalan con la configuración predeterminada.
- Los componentes Prevención de ataques de BadUSB, Control de anomalías adaptativo, Cifrado de datos y Detection and Response se ignoran.

Cuando se instala de forma remota, la aplicación KES ignora el conjunto de componentes KSWS instalados. El instalador instala los componentes que seleccione en las propiedades del paquete de instalación. Después de instalar Kaspersky Endpoint Security y migrar directivas y tareas, los ajustes de KES se configuran de acuerdo con los ajustes de KSWS.

Migración de tareas y directivas de KSWS

Puede migrar la configuración de directivas y tareas de las siguientes formas:

- Con el Asistente de conversión por lotes de directivas y tareas (en adelante, también denominado Asistente de migración).

  El Asistente de migración para KSWS solo está disponible en la Consola de administración (MMC). La configuración de directivas y tareas no puede migrarse a Web Console y Cloud Console.

  El asistente de conversión por lotes funciona de manera diferente para las diferentes versiones de Kaspersky Security Center. Recomendamos actualizar la solución a la versión 14.2 o superior. En esta versión de Kaspersky Security Center, el asistente de conversión por lotes de directivas y tareas le permite migrar directivas a un perfil en lugar de a una directiva. En esta versión de Kaspersky Security Center, el asistente de conversión por lotes de directivas y tareas también le permite migrar una gama más amplia de configuraciones de directivas.

- Con el Asistente de nueva directiva para Kaspersky Endpoint Security para Windows.

  El Asistente de nueva directiva le permite crear una directiva KES sobre la base de una directiva KSWS.

Los procedimientos de migración de directivas de KSWS son diferentes cuando se utiliza el asistente de migración y el asistente de nueva directiva.

Asistente de conversión por lotes de directivas y tareas

El asistente de migración transfiere la configuración de la directiva de KSWS al perfil de directiva en lugar de la configuración de la directiva de KES. El *perfil de directiva* es un conjunto de configuraciones de directivas que se activa en un equipo si este cumple con las reglas de activación configuradas. La etiqueta de dispositivo `UpgradedFromKSWS` se selecciona como el criterio de activación del perfil de directiva. Kaspersky Security Center añade automáticamente la etiqueta `UpgradedFromKSWS` a todos los equipos en los que instala KES sobre KSWS usando la tarea de instalación remota. Si elige un método de instalación diferente, puede asignar la etiqueta a los dispositivos manualmente.

Para añadir una etiqueta a un dispositivo:

1. Cree una nueva etiqueta para servidores: `UpgradedFromKSWS`.

   Para obtener más información sobre la creación de etiquetas para dispositivos, consulte la Ayuda de Kaspersky Security Center.

2. Cree un nuevo grupo de administración en la consola de Kaspersky Security Center y añada los servidores a los que desea asignar la etiqueta a este grupo.

   Puede agrupar servidores utilizando la herramienta de selección. Para obtener más información sobre cómo trabajar con selecciones, consulte la Ayuda de Kaspersky Security Center.

3. Seleccione todos los servidores del grupo de administración en la consola de Kaspersky Security Center, abra las propiedades de los servidores seleccionados y asigne la etiqueta.

Si está migrando varias directivas de KSWS, cada directiva se convierte en un perfil dentro de una directiva general. Si la directiva de KSWS ya contiene perfiles, estos también se migran como perfiles. Como resultado, obtendrá una directiva única que incluye perfiles correspondientes a todas las directivas de KSWS.

Cómo usar el Asistente de conversión por lotes de directivas y tareas para migrar la configuración de directivas de KSWS.

1. En la Consola de administración, elija el Servidor de administración y haga clic con el botón derecho para abrir el menú contextual.

2. Seleccione **Todas las tareas → Asistente de conversión por lotes de directivas y tareas**.

Se iniciará el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Elija la aplicación para la que necesita convertir directivas y tareas

En este paso, debe elegir Kaspersky Endpoint Security para Windows. Ir al paso siguiente.

Paso 2. Conversión de directivas

El asistente de migración crea perfiles de directivas de KSWS dentro de una directiva de KES. Elija las directivas de Kaspersky Security for Windows Server que desea convertir a perfiles de directivas. Ir al paso siguiente.

A continuación, el Asistente de migración comenzará a convertir las directivas. Los nombres de los nuevos perfiles de directivas se corresponderán con las directivas originales de KSWS.

Paso 3. Informe de migración de directivas

El asistente de migración crea un informe de migración de directivas. El informe de migración de directivas contiene la fecha y la hora en que se convirtieron las directivas, el nombre de la directiva KSWS original, el nombre de la directiva KES de destino y el nombre del nuevo perfil de directiva.

Paso 4. Conversión de tareas

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security para Windows. En la lista de tareas, seleccione las tareas de KSWS que desea crear para Kaspersky Endpoint Security. Las nuevas tareas recibirán el nombre *<Nombre de la tarea de KSWS> (convertida)*. Ir al paso siguiente.

Paso 5: Fin del asistente

Finalice el asistente. Como resultado, el asistente hace lo siguiente:

- Se añaden nuevos perfiles de directivas a la directiva de Kaspersky Endpoint Security.

  La directiva incluye perfiles con la configuración de Kaspersky Security for Windows Server. La directiva nueva tiene el estado *Activa*. El asistente deja sin modificar las directivas de KSWS.

- Se crean tareas nuevas de Kaspersky Endpoint Security.

  Las nuevas tareas son copias de las tareas de KSWS. El asistente deja sin modificar las tareas de KSWS.

El nuevo perfil de directiva con la configuración de KSWS se llamará *UpgradedFromKSWS <Nombre de la directiva de Kaspersky Security for Windows Server>*. En las propiedades del perfil, el asistente de migración selecciona automáticamente el la etiqueta de dispositivo `UpgradedFromKSWS` como criterio de activación. Por lo tanto, la configuración del perfil de directiva se aplica a los servidores automáticamente.

Asistente para crear una directiva basada en una directiva KSWS

Cuando se crea una directiva de KES basada en una directiva de KSWS, el asistente transfiere la configuración a la nueva directiva en consecuencia. Es decir, a una directiva de KES le corresponderá a una póliza de KSWS. El asistente no convierte la directiva en un perfil.

Cómo usar el Asistente de nueva directiva para migrar la configuración de directivas de KSWS

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, seleccione la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Haga clic en **Nueva directiva**.

   El Asistente de directivas se inicia.
5. Siga las instrucciones del Asistente de directivas.

Paso 1. Selección de la aplicación para crear la directiva de grupos

Seleccione la aplicación **Kaspersky Endpoint Security para Windows (14.2)**.

Paso 2. Nombrar la directiva de grupo

Introduzca un nombre para la directiva de grupo; por ejemplo, *Directiva de la oficina*.

Seleccione la casilla **Usar configuración de directivas para una versión anterior de la aplicación**. Haga clic en **Examinar** y elija la directiva de KSWS.

Paso 3. Participación en Kaspersky Security Network

Lea y acepte los términos de la Declaración de Kaspersky Security Network (KSN).

Paso 4. Selección del modo de uso de la aplicación en equipos

Seleccione **Modo estándar para proteger hosts**. Kaspersky Endpoint Security proporciona una directiva común para todos los modos de aplicación y tipos de sistema operativo.

Recomendamos usar diferentes directivas para diferentes modos y tipos de sistema operativo.

Paso 5. Importar la configuración

Este paso está disponible si selecciona la configuración manual de la directiva en el paso 4.

Puede crear una directiva basada en la configuración de Kaspersky Endpoint Security desde un archivo de configuración de CFG. El Asistente para nueva directiva no admite archivos de configuración cifrados. Al exportar el archivo de configuración, omita el paso de cifrado del archivo.

Al importar un archivo de configuración CFG de la aplicación, no todos los parámetros de la directiva están disponibles para el asistente. Por ejemplo, la configuración de la aplicación carece de perfiles de la directiva. Si desea transferir todas las configuraciones y perfiles a la directiva, puede importar otra directiva de un archivo KLP.

Al importar un archivo de configuración, Kaspersky Endpoint Security no transfiere contraseñas de contenedores criptográficos. Si utiliza la autenticación bidireccional al conectarse a los servidores, debe especificar las contraseñas del contenedor criptográfico desde cero.

Pasos 6-10. Configuración de la directiva

Este paso está disponible si selecciona la configuración manual de la directiva en el paso 4.

Siga los pasos para administrar la configuración de la directiva.

Paso 11. Configurar la zona de confianza

Configurar la zona de confianza. Puede añadir exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores. Las exclusiones de análisis y aplicaciones de confianza predefinidas también pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en modo Light Agent en entornos virtuales Citrix y VMware.

Paso 12. Seleccionar el estado de la directiva

- **Activa**. Después de la siguiente sincronización, la directiva se utilizará como directiva activa en el equipo.

  Los valores de la directiva activa se guardan en los equipos cliente cuando se realiza la sincronización. Un equipo puede estar sujeto a una sola directiva por vez; por ello, solo una directiva puede estar activa por grupo.

- **Inactiva**. Directiva de reserva. Puede convertirse en la directiva activa cuando resulta necesario.

  El número de directivas inactivas que pueden crearse es ilimitado. Estas no afectan la configuración de las aplicaciones instaladas en los equipos de la red. Están pensadas para usarse en situaciones de emergencia, como brotes de virus y otros casos. Por ejemplo, ante un ataque mediante unidades flash, puede activarse una directiva que impida el uso de unidades flash. En tal caso, la directiva activa cambia de estado a inactiva automáticamente.

- **Fuera de la oficina**. La directiva se activa cuando un equipo abandona el perímetro de la red de la organización.

Finalice el asistente.

Configuración adicional de directivas y tareas después de la migración

KSWS y KES tienen diferentes conjuntos de componentes y configuraciones de directivas, por lo que después de la migración debe verificar que las configuraciones de directivas cumplan con los requisitos de seguridad de su empresa.

Verifique la siguiente configuración de directiva básica:

- Protección con contraseña. La configuración de protección de contraseña de KSWS no se migra. Kaspersky Endpoint Security tiene una función de protección de contraseña integrada. Si es necesario, active Protección con contraseña y establezca una contraseña.

- Zona de confianza Los métodos utilizados por KSWS y KES para seleccionar objetos son diferentes. Al migrar, KES admite exclusiones definidas como archivos individuales o rutas a archivos/carpetas. Si KSWS tiene exclusiones configuradas como un área predefinida o una URL de script, dichas exclusiones no se migran. Después de la migración, debe añadir dichas exclusiones manualmente.

  Para asegurarse de que Kaspersky Endpoint Security funciona correctamente en los servidores, se recomienda agregar archivos importantes para el funcionamiento del servidor a la zona de confianza. Para servidores SQL, debe agregar archivos de base de datos MDF y LDF. Para servidores de Microsoft Exchange, debe agregar archivos CHK, EDB, JRS, LOG y JSL. Puede usar máscaras; por ejemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores.

- Firewall. Las funciones de firewall de KSWS están a cargo del firewall en el nivel del sistema. En KES, un componente separado es responsable de la funcionalidad del Firewall. Después de la migración, puede configurar el firewall de Kaspersky Endpoint Security.

- Kaspersky Security Network. Kaspersky Endpoint Security no admite el componente la configuración de KSN para componentes individuales. Kaspersky Endpoint Security usa KSN para todos los componentes de la aplicación. Para utilizar KSN, debe aceptar los nuevos términos y condiciones de la Declaración de Kaspersky Security Network.

- Control web. Las reglas de bloqueo para el control de categorías de tráfico web se migran a una sola regla de bloqueo en Kaspersky Endpoint Security. Kaspersky Endpoint Security ignora las reglas de autorización para el control de categorías. Kaspersky Endpoint Security no admite todas las categorías de Kaspersky Security for Windows Server. Las categorías que no existen en Kaspersky Endpoint Security no se migran. Por lo tanto, las reglas de clasificación de recursos web con categorías no admitidas no se migran. Si necesario, añada reglas de Control Web.

- Servidor proxy. La contraseña de autenticación del servidor proxy no se migra. Introduzca la contraseña que se usará para conectarse al servidor proxy manualmente.

- Listas de componentes individuales. Kaspersky Endpoint Security no admite programaciones de configuración para componentes individuales. Los componentes están siempre activados mientras Kaspersky Endpoint Security está operativo.

- Conjunto de componentes. El conjunto de funciones disponibles de Kaspersky Endpoint Security depende del tipo de sistema operativo: estación de trabajo o servidor. Por ejemplo, de las herramientas de cifrado, solo el Cifrado de unidad BitLocker está disponible en los servidores.

- Atributo . El estado del atributo no se migra. El atributo tendrá el valor predeterminado. De forma predeterminada, casi todas las configuraciones en la nueva directiva tienen una prohibición aplicada a la modificación de la configuración en las directivas secundarias y en la interfaz de la aplicación local. El atributo tiene el valor para la configuración de directivas en la sección **Managed Detection and Response (Industrial CyberSecurity)** y en el grupo de configuraciones **Soporte de usuario** (sección **Interfaz**). Si es necesario, configure la herencia de la configuración de la directiva principal.

- Trabajar con amenazas activas. La Desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Puede configurar la desinfección avanzada en la configuración de la tarea *Análisis antimalware* y en la configuración de la aplicación.

- Actualización de la aplicación. Para instalar actualizaciones y parches importantes sin reiniciar, debe cambiar el modo de actualización de la aplicación. De forma predeterminada, la función Instalar actualizaciones de aplicaciones sin reiniciar está desactivada.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security dispone de un agente incorporado para trabajar con soluciones de Detection and Response. Si necesario, transfiera la configuración de la directiva de Kaspersky Endpoint Agent a la directiva de Kaspersky Endpoint Security.

- Tareas *Actualización de las bases de datos y módulos de la aplicación*. Asegúrese de que la configuración de la tarea *Actualización de las bases de datos y módulos de la aplicación* se migró correctamente. En lugar de las tres tareas de KSWS, KES usa una sola tarea de KES. Puede optimizar las tareas *Actualización de las bases de datos y módulos de la aplicación* y eliminar tareas superfluas.

- Otras tareas. Los componentes Control de aplicaciones, Control de dispositivos y Monitor de integridad de archivos funcionan de manera diferente en KSWS y KES. KES no utiliza las tareas *Baseline File Integrity Monitor*, *Applications Launch Control Generator* o *Rule Generator for Device Control*. Por lo tanto, estas tareas no se migran. Después de la migración, puede configurar los componentes Monitor de integridad de archivos, Control de aplicaciones y Control del dispositivo.

Migración de la zona de confianza de KSWS

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo. Puede migrar objetos de la zona de confianza desde KSWS a KES usando el *asistente de conversión por lotes de directivas y tareas* o el *asistente para crear una nueva directiva de KES en función de la directiva de KSWS*. KSWS y KES tienen diferentes conjuntos de componentes y funciones, por lo que después de la migración debe verificar que las exclusiones satisfagan los requisitos de seguridad de su empresa. Los métodos para añadir exclusiones a la zona de confianza también son distintos para KES y KSWS. El asistente de migración no dispone de herramientas para migrar todas las exclusiones de KSWS. Esto significa que, tras la migración, debe añadir manualmente algunas de las exclusiones de KSWS.

Para asegurarse de que Kaspersky Endpoint Security funciona correctamente en los servidores, se recomienda agregar archivos importantes para el funcionamiento del servidor a la zona de confianza. Para servidores SQL, debe agregar archivos de base de datos MDF y LDF. Para servidores de Microsoft Exchange, debe agregar archivos CHK, EDB, JRS, LOG y JSL. Puede usar máscaras; por ejemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores.

Métodos de creación de zonas de confianza de KES y KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(no migra)*	
• Disk, folder or network location	→	**Archivo o carpeta**
• File	→	**Archivo o carpeta**
• Script file or web address	*(no migra)*	
Detected object	→	**Tipos de objetos detectados**
Trusted processes	→	**Aplicaciones de confianza**

Migración de objetos analizados

Las exclusiones de KSWS que tienen el método **Object to scan** seleccionado en sus propiedades se migran a las exclusiones de KES que tienen el método **Archivo o carpeta** seleccionado en sus propiedades, con ciertas limitaciones. La migración de una exclusión de una exclusión depende del método de selección de objetos:

- Predefined scope – *no migra*.

  Después de la migración, debe añadir dichas exclusiones manualmente. Las exclusiones como áreas predefinidas se deben configurar en la configuración de la tarea *Análisis antimalware*.

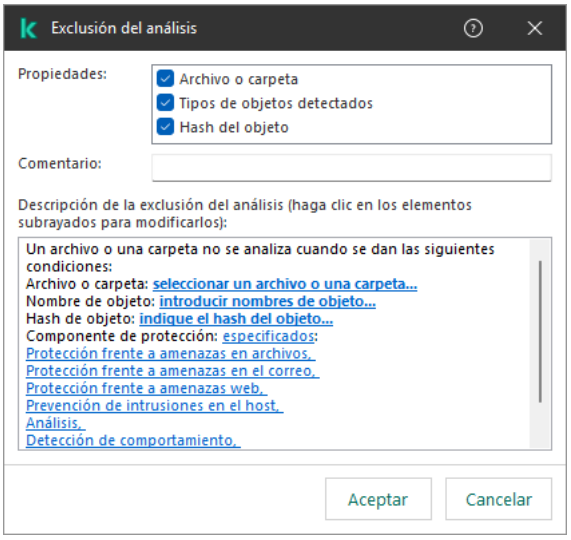
- Disk, folder or network location: migra a exclusiones de KES que tienen el método "Archivo o carpeta" seleccionado en las propiedades.

- File: migra a exclusiones de KES que tienen el método "Archivo o carpeta" seleccionado en las propiedades.

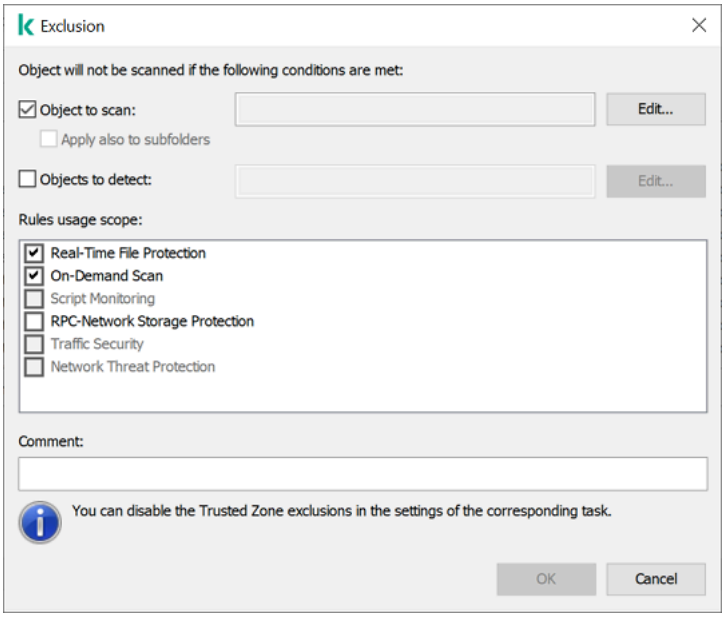
- Script file or web address – *no migra*.

  Después de la migración, debe añadir dichas exclusiones manualmente. Las exclusiones como direcciones web de scripts se deben añadir a las direcciones web de confianza de Protección frente a amenazas web.

Si la casilla **Apply also to subfolders** está seleccionada para el objeto analizado, esta configuración se migra a exclusiones de KES (casilla **Incluir subcarpetas**).



Configuración de exclusiones de KES



Configuración de exclusiones de KSWS

Migración de objetos detectados

Las exclusiones de KSWS que tienen el método **Detected object** seleccionado en sus propiedades se migran a las exclusiones de KES que tienen el método **Tipos de objetos detectados** seleccionado en sus propiedades. El nombre del objeto detectado corresponde a la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`). Kaspersky Endpoint Security admite máscaras con el signo de interrogación `?` (equivale a cualquier carácter individual) y el asterisco `*` (equivale a cualquier secuencia de caracteres).

Migración del alcance de uso de las exclusiones

El alcance de uso de una exclusión es un conjunto de componentes a los que se aplica la exclusión. KES y KSWS tienen distintos conjuntos de componentes, por lo que el asistente de migración no puede migrar el alcance de uso de la exclusión. Por tanto, si se selecciona al menos un componente en el alcance de uso de KSWS, KES aplica la exclusión a todos los componentes de la aplicación.

Puede configurar el alcance de uso de KSWS en la configuración de la zona de confianza y también en la configuración de los componentes de protección KSWS. Para ello, puede seleccionar o desactivar la casilla **Apply Trusted Zone** en la sección correspondiente de la directiva. La configuración de los componentes de protección KES no incluye dicha casilla. Esto significa que el estado de la zona de confianza en la configuración del componente individual se pierde al realizar la migración. Tras completar la migración, seleccione los componentes a los que se aplica la exclusión en la configuración de la zona de confianza de la directiva de KES.

Migración de comentarios

Los comentarios de la zona de confianza de KSWS se migran a los comentarios de la exclusión de KES sin modificación.

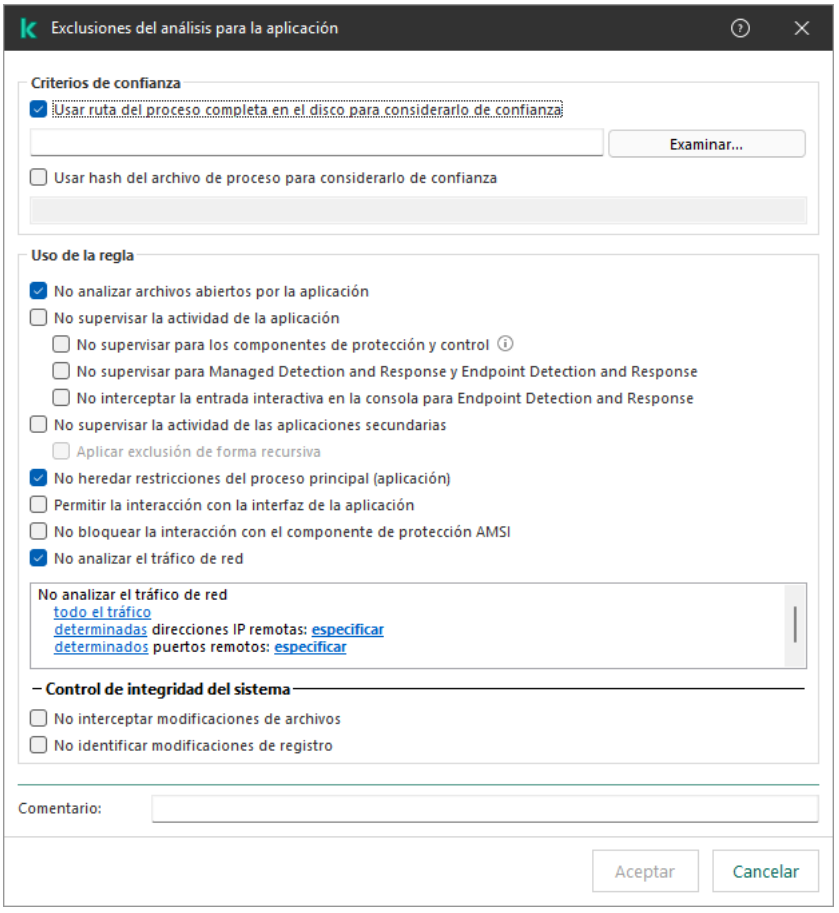
Migración de procesos de confianza

Los procesos de confianza de KSWS se migran a los procesos de confianza de KES con algunas limitaciones. La migración de los procesos de confianza depende del método de selección de objetos:

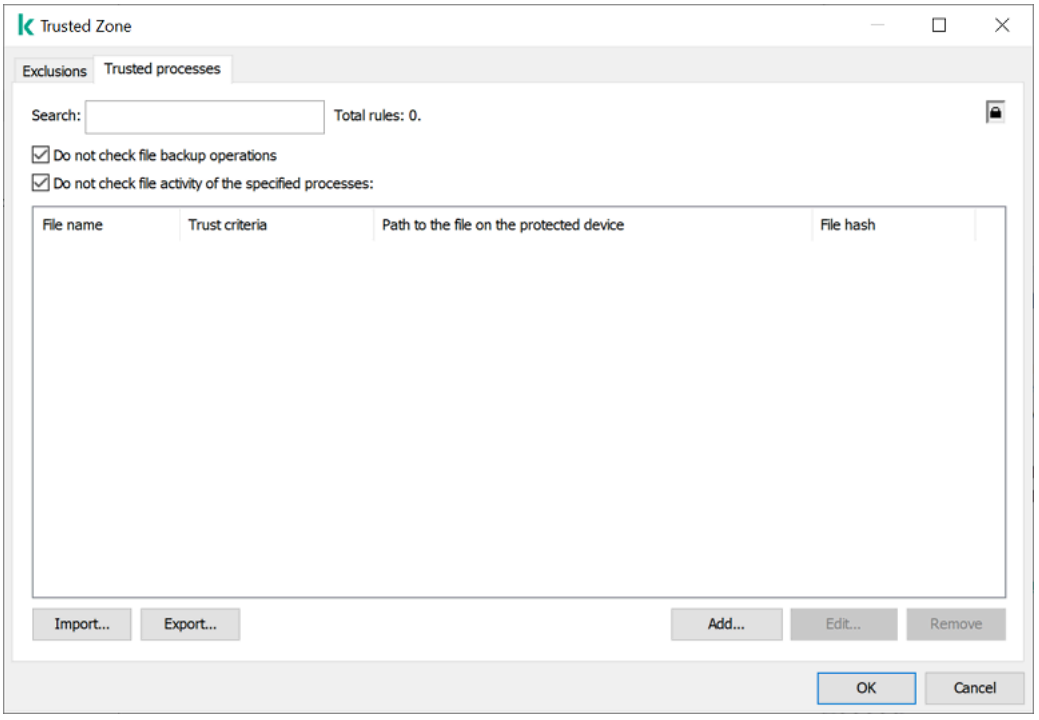
- Path to the file on the protected device: migra a aplicaciones de confianza de KES.
- File hash – *no migra*.

Si KSWS tiene procesos de confianza configurados como un hash de archivo, estos procesos de confianza no se migran. Después de la migración, debe añadir los procesos de confianza manualmente.

Si la casilla **Do not check file backup operations** está seleccionada en la configuración de procesos de confianza, esta configuración se migra a las exclusiones de confianza de KES (casilla **No supervisar la actividad de la aplicación**).



Configuración de aplicaciones de confianza de KES



Configuración de procesos de confianza de KSWS

Migración de las reglas de Control de inicio de aplicaciones de KSWS

El Control de inicio de aplicaciones de KSWS bloquea de forma predeterminada. Es decir, el Control de inicio de aplicaciones bloquea automáticamente todas las aplicaciones que no están especificadas en las reglas como aplicaciones permitidas. Por lo tanto, el asistente de migración para el Control de aplicaciones de KES establece automáticamente el modo de control **Lista de permitidos**, que corresponde al principio de bloqueo de forma predeterminada.

Puede migrar reglas de KSWS a KES usando el *asistente de conversión por lotes de directivas y tareas* o el *asistente para crear una nueva directiva de KES en función de la directiva de KSWS*.

Migrar el modo de Control de inicio de aplicaciones

El modo de Control de inicio de aplicaciones de KSWS migra a Control de aplicaciones de KES de la siguiente manera:

- **Statistics only** → **Probar reglas**;
- **Active** → **Aplicar reglas**.

Migración de reglas predefinidas de Control de inicio de aplicaciones de KSWS

De manera predeterminada, el Control de ejecución de aplicaciones de KSWS incluye dos reglas:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Las reglas predefinidas permiten la ejecución de *scripts*, *paquetes MSI* y *archivos ejecutables* firmados por un certificado raíz de confianza. Si al menos una regla de KSWS predefinida es del tipo **Allow**, el asistente de migración crea una nueva regla de admisión, **Aplicaciones con certificados raíz de confianza**. Esto quiere decir que el Control de aplicaciones de KES utiliza una regla única para autorizar los scripts de confianza en ejecución, los paquete de MSI y los archivos ejecutables.

Si ambas reglas predefinidas de KSWS tienen el tipo **Deny**, KES ignora las reglas predefinidas.

Migración de reglas personalizadas de Control de inicio de aplicaciones de KSWS

Las reglas de Control de inicio de aplicaciones de KSWS regulan la ejecución de archivos de acuerdo con los siguientes criterios:

- firma con certificado digital;
- hash SHA256;
- ruta del archivo.

Las reglas se crean de forma diferente en KSWS y KES; por tanto, el asistente de migración crea *categorías de aplicaciones*, que incluyen condiciones y exclusiones de las reglas de KSWS, y añaden estas categorías de la aplicación a las reglas de KES. El asistente usa las condiciones **Certificado**, **Ruta de la carpeta** y **Hash del archivo** en las categorías de aplicación. Las nuevas categorías de aplicaciones están disponibles en la Consola de administración de Kaspersky Security Center, en la sección **Administración de aplicaciones → Categorías de aplicaciones**.

El asistente de migración agrupa las reglas de KSWS por tipo y por usuario. A continuación, el asistente crea categorías de la aplicación que incluyen condiciones y exclusiones de las reglas de KSWS y añade las categorías de la aplicación a las nuevas reglas de KES. El asistente especifica los nombres de las reglas de KSWS en el campo **Descripción** de las reglas de KES.

Migración de la configuración avanzada de Control de inicio de aplicaciones de KSWS

El principio de funcionamiento del Control de inicio de aplicaciones de KSWS y del Control de aplicaciones de KES es diferente, por lo que el asistente de migración puede migrar un subconjunto de configuraciones.

Configuración de Control de inicio de aplicaciones

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(no migra)* Kaspersky Endpoint Security analiza la aplicación cada vez que intenta ejecutarse.
Deny the command interpreters launch with no command to execute	*(no migra)* Kaspersky Endpoint Security permite ejecutar intérpretes de comandos si no están prohibidos por Control de aplicaciones.
Apply rules to executable files	*(no migra)* El alcance de la aplicación de la regla no se puede configurar en la configuración de Control de aplicaciones de KES. El Control de aplicaciones de KES aplica reglas a todos los tipos de archivos: archivos ejecutables, scripts y paquetes de MSI. Si todos los tipos de archivos se incluyen en el alcance de la aplicación de la regla en KSWS, KES traslada las reglas de KSWS durante la migración. Si se excluye algún tipo de archivo del alcance de la aplicación de la regla en KSWS, KES también traslada las reglas de KSWS durante la migración, pero se selecciona **Probar reglas** como la acción de Control de aplicaciones.
Monitor loading of DLL modules	**Supervisar la carga de los módulos DLL (incrementa significativamente la carga del sistema)**

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Apply rules to scripts and MSI packages	*(no migra)* El alcance de la aplicación de la regla no se puede configurar en la configuración de Control de aplicaciones de KES. El Control de aplicaciones de KES aplica reglas a todos los tipos de archivos: archivos ejecutables, scripts y paquetes de MSI. Si todos los tipos de archivos se incluyen en el alcance de la aplicación de la regla en KSWS, KES traslada las reglas de KSWS durante la migración. Si se excluye algún tipo de archivo del alcance de la aplicación de la regla en KSWS, KES traslada las reglas de KSWS durante la migración, pero se selecciona **Probar reglas** como la acción de Control de aplicaciones.
Deny applications untrusted by KSN	*(no migra)* Kaspersky Endpoint Security no tiene en cuenta la reputación de las aplicaciones y permite o deniega la ejecución de aplicaciones de acuerdo con las reglas.
Allow applications trusted by KSN	Durante la migración, KES añade una regla de permiso nueva. La categoría KL **Otro software\Aplicaciones de confianza de acuerdo con la reputación en KSN** se especifica como condición de activación de reglas.
Users and / or user groups allowed to run applications trusted by KSN	**Usuarios y sus derechos** en una regla de permiso de Control de aplicaciones que incluye la categoría KL **Otro software\Aplicaciones de confianza de acuerdo con la reputación en KSN**.
Automatically allow software distribution via applications and packages listed	El Control de distribución de software en KSWS y KES funciona diferente. Durante la migración, KES añade reglas nuevas para las aplicaciones que tienen activada la distribución automática de software. El hash del archivo está especificado como la condición de activación de la regla.
Always allow software distribution via Windows Installer	El Control de distribución de software en KSWS y KES funciona diferente. Durante la migración, KES añade reglas nuevas para las aplicaciones que tienen activada la distribución automática de software (**Software distribution applications and packages allowed**). El hash del archivo está especificado como la condición de activación de la regla. La casilla **Actualizadores de confianza** está activada en las propiedades de la cuenta.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(no migra)*
Software distribution applications and packages allowed	El Control de distribución de software en KSWS y KES funciona diferente. Durante la migración, KES añade reglas nuevas para las aplicaciones que tienen activada la distribución automática de software. El hash del archivo está especificado como la condición de activación de la regla. La casilla **Actualizadores de confianza** está activada en las propiedades de la cuenta.
Schedule settings	*(no migra)* Si se configura una programación para el componente en la configuración de KSWS, el componente de Control de aplicaciones se activa durante la migración. Si no se configura una programación para el componente en la configuración de KSWS, el Control de aplicaciones estará desactivado durante la migración. No es posible configurar una programación por separado para el componente. El componente está siempre activado mientras Kaspersky Endpoint Security está operativo.

Instalación de KES en lugar de KSWS

Puede instalar Kaspersky Endpoint Security de las siguientes maneras:

- Instalando KES después de eliminar KSWS (recomendado).
- Instalando KES encima de KSWS

Eliminación de Kaspersky Security for Windows Server

Puede eliminar la aplicación de forma remota utilizando la tarea *Desinstalar aplicación en remoto* o localmente en el servidor. Es posible que deba reiniciar el servidor después de eliminar KSWS. Si desea instalar Kaspersky Endpoint Security sin reiniciar, asegúrese de que Kaspersky Security for Windows Server se ha eliminado por completo. Si la aplicación no se elimina por completo, la instalación de Kaspersky Endpoint Security puede provocar un funcionamiento defectuoso del servidor. También se recomienda asegurarse de que la aplicación se elimine por completo si ha utilizado la utilidad kavremover. La utilidad kavremover no soporta la administración de KSWS.

Si la Protección con contraseña está habilitada para restringir el acceso a KSWS, introduzca la contraseña de desinstalación en la configuración del paquete de instalación de KES.

Después de eliminar KSWS, instale Kaspersky Endpoint Security para Windows utilizando cualquier método disponible.

Instalación de Instale Kaspersky Endpoint Security

Al instalar KES de forma remota, los componentes que ha seleccionado en las propiedades del paquete de instalación se instalan en el servidor. Recomendamos seleccionar los componentes predeterminados en las propiedades del paquete de instalación. No es necesario reiniciar al instalar KES sobre KSWS.

Antes de la instalación local, Kaspersky Endpoint Security comprueba el equipo para buscar aplicaciones de Kaspersky. Si Kaspersky Security for Windows Server está instalado en el equipo, KES detecta el conjunto de componentes de KSWS que están instalados y selecciona los mismos componentes para la instalación. No es necesario reiniciar al instalar KES sobre KSWS.

Si falla la instalación de KES sobre KSWS, puede revertir la instalación. Después de revertir la instalación, se recomienda reiniciar el servidor y volver a intentarlo.

La configuración y las tareas de KSWS no se migran cuando Kaspersky Endpoint Security para Windows está instalado. Para migrar la configuración y las tareas, ejecute el asistente de conversión por lotes de directivas y tareas.

Puede comprobar la lista de componentes instalados en la sección **Seguridad** de la interfaz de la aplicación, usando el comando `status`, o en la consola de Kaspersky Security Center en las propiedades del equipo. Puede cambiar el conjunto de componentes después de la instalación utilizando los *Cambiar componentes de la aplicación*.

Migrar la configuración [KSWS + KEA] a la configuración [KES + agente incorporado]

Para admitir el uso de Kaspersky Endpoint Security para Windows como parte de EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA y MDR, se ha añadido un agente incorporado a la aplicación. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con estas soluciones.

Al migrar de KSWS a KES, las soluciones EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA y MDR continúan funcionando con agentes incorporados de Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo.

La migración de la configuración de [KSWS+KEA] a [KES+agente incorporado] implica los siguientes pasos:

1. **Migración de KSWS a KES**

   La migración de KSWS a KES implica instalar Kaspersky Endpoint Security en lugar de Kaspersky Security for Windows Server.

   Los administradores suelen activar la protección con contraseña para restringir el acceso a KSWS y KEA. A partir de Kaspersky Security Center Linux 15.1, puede introducir la contraseña de desinstalación de la aplicación en la configuración de la tarea *Instalar aplicación en remoto*. La tarea permite introducir solo una contraseña de desinstalación. Es decir, si se establece la misma contraseña para KSWS y KEA, las aplicaciones KSWS y KEA se eliminan correctamente. Si las contraseñas son diferentes, la eliminación de una de las aplicaciones falla con un error de acceso. Para completar la migración, debe desactivar la protección con contraseña para la aplicación cuya contraseña no pudo introducir en la configuración de la tarea *Instalar aplicación en remoto*.

   Para realizar la migración, debe seleccionar los componentes necesarios para soportar las soluciones de Detection and Response como parte de Kaspersky Endpoint Security. Tras instalar la aplicación, Kaspersky Endpoint Security pasa a utilizar el agente incorporado y elimina Endpoint Agent de Kaspersky.

2. **Migrar las directivas y tareas**

   La migración de las directivas y tareas de [KSWS+KEA] a [KES+agente integrado] implica los siguientes pasos:

   1. Migración de directivas y tareas de KSWS a KES mediante el asistente de conversión por lotes de directivas y tareas (solo disponible en la Consola de administración (MMC)).

      Como resultado, se añade un perfil de directiva con el nombre *UpgradedFromKSWS <Nombre de la directiva de Kaspersky Security for Windows Server>* a la directiva de KES. También se crean nuevas tareas de KES con los nombres *<Nombre de tarea de KSWS> (converted)*.

   2. Migración de directivas y tareas de KEA a KES mediante el asistente de migración de Kaspersky Endpoint Agent (solo disponible en Web Console y Cloud Console).

      Como resultado, se crea una nueva directiva con el nombre *<Nombre de la directiva de Kaspersky Endpoint Security> &<Nombre de la directiva de Kaspersky Endpoint Agent>*. También se crean nuevas tareas y tareas de KES.

3. **Funcionalidad de licencias**

Si utiliza una licencia común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Agent, la funcionalidad EDR Optimum se activa de manera automática después de actualizar la aplicación a la versión 11.7.0. No necesita realizar ninguna otra acción.

Si utiliza una licencia independiente adicional de Kaspersky Endpoint Detection and Response Optimum para activar la funcionalidad EDR Optimum, debe asegurarse de que la clave del complemento EDR Optimum se añada al repositorio de Kaspersky Security Center y de que la funcionalidad de distribución automática de claves de licencia esté activada. Después de actualizar la aplicación a la versión 11.7.0, la funcionalidad EDR Optimum se activa de manera automática.

Si utiliza una licencia de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Agent, y una licencia diferente para activar Kaspersky Endpoint Security para Windows, debe reemplazar la clave para Kaspersky Endpoint Security para Windows con la clave común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. Puede reemplazar la clave con la tarea *Añadir clave*.

No necesita activar la funcionalidad Kaspersky Sandbox. Kaspersky Sandbox estará disponible de forma inmediata después de actualizar y activar Kaspersky Endpoint Security para Windows.

Solo se puede usar la licencia de Kaspersky Anti Targeted Attack Platform para activar Kaspersky Endpoint Security como parte de la solución Kaspersky Anti Targeted Attack Platform. Después de actualizar la aplicación a la versión 12.1, la funcionalidad EDR (KATA) se activa de manera automática. No necesita realizar ninguna otra acción.

4. **Revisar el estado de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox**

   Si, después de la actualización, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

   - Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.
   - Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*.
   - Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

   Asegúrese de que la funcionalidad EDR Optimum esté activada mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, compruebe que la funcionalidad de distribución automática de claves de licencia de EDR Optimum esté activada.

Asegurarse de que Kaspersky Security for Windows Server se eliminó con éxito

Asegúrese de que Kaspersky Security for Windows Server esté completamente eliminado:

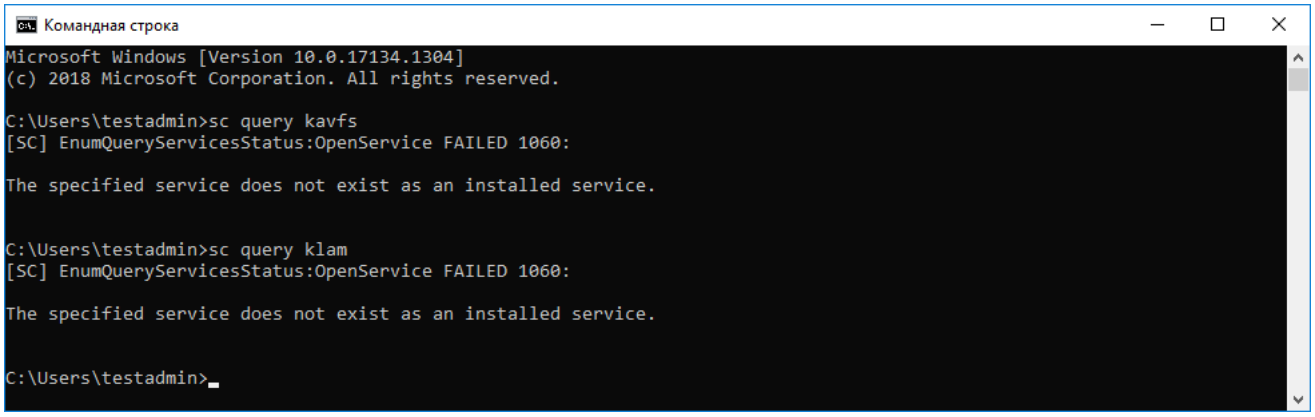
- La carpeta `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` no existe.
- Los siguientes servicios no están presentes:
  - Kaspersky Security Service (KAVFS)
  - Kaspersky Security Management servicio (KAVFSGT)

- Kaspersky Security Exploit Prevention servicio (KAVFSSLP)
- Kaspersky Security Script Checker servicio (KAVFSSCS)

Puede verificar los servicios en ejecución en el Administrador de tareas o emitiendo el comando `sc query` (consulte la figura a continuación).

- Los siguientes controladores no están disponibles:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

  Puede comprobar los controladores instalados en la carpeta `C:\Windows\System32\drivers` o emitiendo el comando `sc query`. Si falta un servicio o un controlador, obtendrá la siguiente respuesta:



Asegurarse de que los servicios y controladores de Kaspersky Security for Windows Server se eliminaron correctamente

Si los archivos de la aplicación o de los controladores permanecen en el servidor, elimínelos manualmente. Si los servicios de Kaspersky Security for Windows Server todavía se están ejecutando en el servidor, detenga (`sc stop`) y elimine (`sc delete`) los servicios manualmente. Para detener el controlador klam.sys, use el comando `fltmc unload klam`.

Activación de KES con una clave de KSWS

Después de instalar la aplicación, puede activar Kaspersky Endpoint Security para Windows (KES) con una clave de licencia de Kaspersky Security for Windows Server (KSWS). El proceso de activación después de la migración depende del método de activación de KSWS (consulte la tabla a continuación).

Kaspersky Endpoint Security no es compatible con la *licencia de Kaspersky Security for Storage*. Para trabajar con esta licencia debe usar Kaspersky Security for Windows Server.

Para activar KES con la clave de KSWS solo puede utilizar la código de activación. Si está utilizando un archivo de clave para activar la aplicación, debe ponerse en contacto con el Soporte técnico para conseguir un archivo de clave de Kaspersky Endpoint Security.

Activación de Kaspersky Endpoint Security para Windows con una clave de Kaspersky Security for Windows Server

Método de activación de Kaspersky Security for Windows Server	Migración de la clave de Kaspersky Endpoint Security para Windows.
Distribución automática de la clave de licencia de KSWS a los equipos.	Si la distribución automática de claves está activada en las propiedades de la clave de licencia de KSWS, KES se activa automáticamente con la clave de KSWS.
La clave de KSWS se añade mediante una tarea.	Si su KSWS se activa con la tarea, la clave de licencia de KSWS se eliminará durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede añadir una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.
La clave de KSWS se añade localmente en la interfaz de la aplicación.	Si su KSWS se activa localmente mediante el Asistente de activación de aplicaciones, la clave de licencia de KSWS se eliminará durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede añadir una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.
La clave de KSWS se añade al paquete de instalación.	Si su KSWS se activa con la clave del paquete de instalación, la clave de licencia de KSWS se eliminará durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede añadir una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.
Imagen de máquina virtual pagada (Amazon Machine Image – AMI) en Amazon Web Services (AWS).	Si compró Kaspersky Security Center como imagen de máquina virtual pagada (Amazon Machine Image - AMI) en Amazon Web Services (AWS), no es necesario activar KES. En este caso, Kaspersky Security Center usa suscripción a AWS que ya se ha añadido a la aplicación.
Imagen gratuita de Kaspersky Security Center lista para usar con su propia licencia (modelo Bring Your Own License – BYOL).	Si está utilizando una imagen gratuita de Kaspersky Security Center lista para usar con su propia licencia en un entorno de nube (modelo Bring Your Own License – BYOL), debe activar la aplicación usando cualquier método disponible. Necesitará una licencia de Kaspersky Hybrid Cloud Security.

Consideraciones especiales para migrar servidores de carga alta

En servidores de carga alta, es importante monitorear el rendimiento y evitar fallos. Después de la migración a Kaspersky Endpoint Security para Windows, recomendamos desactivar temporalmente los componentes de la aplicación que utilizan una cantidad sustancial de recursos del servidor en comparación con otros componentes. Tras asegurarse de que el servidor funciona con normalidad, puede volver a activar los componentes de la aplicación.

Recomendamos migrar servidores de carga alta como se indica a continuación:

1. Cree una directiva de Kaspersky Endpoint Security con la configuración predeterminada.

   La configuración predeterminada se considera óptima. Los expertos de Kaspersky recomiendan esta configuración. La configuración predeterminada proporciona el nivel de protección recomendado y el uso óptimo de los recursos.

2. En la configuración de la directiva, desactive los siguientes componentes: Protección frente a amenazas en la red, Detección de comportamiento, Prevención de exploits, Motor de reparación y Control de aplicaciones.

   Si su organización tiene implementada la solución Kaspersky Managed Detection and Response (MDR), cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security.

3. Elimine Kaspersky Security for Windows Server del servidor.

4. Instale Kaspersky Endpoint Security para Windows con el conjunto predeterminado de componentes.

   Si su organización tiene implementadas soluciones de Detection and Response, seleccione los componentes relevantes en las propiedades del paquete de instalación.

5. Compruebe la configuración de la aplicación:

   - La aplicación se activa con la clave de licencia KSWS.
   - La nueva directiva se ha aplicado. Los componentes seleccionados previamente están desactivados.

6. Asegúrese de que el servidor esté funcionando. Asegúrese de que Kaspersky Endpoint Security para Windows no utilice más del 1 % de los recursos del servidor.

7. Si necesario, cree exclusiones de análisis, añada aplicaciones de confianza y cree una lista de direcciones web de confianza.

8. Active los componentes Detección de comportamiento, Prevención de exploits y Motor de reparación. Asegúrese de que Kaspersky Endpoint Security para Windows no utilice más del 1 % de los recursos del servidor.

9. Active el componente Protección frente a amenazas en la red. Asegúrese de que Kaspersky Endpoint Security para Windows no utilice más del 2 % de los recursos del servidor.

10. Active el componente Control de aplicaciones en el modo de prueba de reglas.

11. Asegúrese de que Control de aplicaciones esté funcionando. Si necesario, agregue nuevas reglas de Control de aplicaciones y desactive el modo de prueba de reglas después de confirmar que Control de aplicaciones está funcionando.

Después de migrar de KSWS a KES, asegúrese de que la aplicación funciona correctamente. Verifique el estado del servidor en la consola (debe ser *Sin inconvenientes*). Asegúrese de que no se notifiquen errores de la aplicación; verifique también la hora de la última conexión al Servidor de administración, la hora de la última actualización de la base de datos y el estado de protección del servidor.

Administrar la aplicación en un servidor en modo Server Core

Un servidor en modo Server Core no tiene una GUI. Por lo tanto, solo puede administrar la aplicación de forma remota utilizando la consola de Kaspersky Security Center o localmente en la línea de comandos.

Administrar la aplicación mediante la consola de Kaspersky Security Center

Instalar la aplicación usando la consola de Kaspersky Security Center no es diferente de instalarlo de la manera normal. Cuando se crea un paquete de instalación, puede añadir una clave de licencia para activar la aplicación. Puede usar una clave de Kaspersky Endpoint Security para Windows o una clave de Kaspersky Security for Windows Server.

En un servidor en modo Server Core, los siguientes componentes de la aplicación no están disponibles: Protección frente a amenazas web, Protección frente a amenazas en el correo, Control Web, Prevención de ataques de BadUSB, Cifrado de archivos (FLE), Cifrado de disco de Kaspersky (FDE).

Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación. La aplicación no puede mostrar una ventana para solicitar al usuario que reinicie el servidor. Puede obtener información sobre la necesidad de reiniciar el servidor desde los informes en la consola de Kaspersky Security Center.

Administrar la aplicación en el servidor en modo Server Core no es diferente de administrar un equipo. Puede utilizar directivas y tareas para configurar la aplicación.

La administración de la aplicación en servidores en modo Server Core implica las siguientes consideraciones especiales:

- El servidor en modo Server Core no tiene una GUI y, por lo tanto, Kaspersky Endpoint Security no muestra una advertencia que indique al usuario que se necesita una desinfección avanzada. Para desinfectar una amenaza, debe activar la tecnología de Desinfección avanzada en la configuración de la aplicación y activar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis antimalware*. Luego, debe iniciar la tarea *Análisis antimalware*.

- El cifrado de unidad BitLocker solo está disponible con un módulo de plataforma segura (TPM). No se puede usar un PIN/contraseña para el cifrado porque la aplicación no puede mostrar la ventana de solicitud de contraseña para la autenticación previa al inicio. Si el sistema operativo tiene activado el modo de compatibilidad con los Estándares federales de procesamiento de la información (FIPS), instale una unidad extraíble para guardar la clave de cifrado antes de comenzar a cifrar la unidad.

Administración de la aplicación desde la línea de comandos

Cuando no puede usar una GUI, puede administrar Kaspersky Endpoint Security desde la línea de comandos.

Para instalar la aplicación en un servidor en modo Server Core, ejecute el siguiente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Para activar la aplicación, ejecute el siguiente comando:

```
avp.com license /add <activation code or key file>
```

Para verificar los estados del perfil de la aplicación, ejecute el siguiente comando:

```
avp.com status
```

Para ver la lista de comandos de administración de aplicaciones, ejecute el siguiente comando:

```
avp.com help
```

Migración de [KSWS+KEA] a [KES+agente incorporado]

Al realizar la migración desde Kaspersky Security for Windows Server (KSWS) a Kaspersky Endpoint Security (KES), puede seguir estas recomendaciones para configurar la protección del servidor y optimizar el rendimiento. Aquí veremos un ejemplo de migración para una sola organización.

Infraestructura de la organización

La empresa tiene instalados los siguientes equipos:

- Kaspersky Security Center 14.2

  El administrador administra las soluciones de Kaspersky mediante la Consola de administración (MMC). También se despliega Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)

  En Kaspersky Security Center se crean tres grupos de administración que contienen servidores de la organización: dos grupos de administración para servidores SQL y un grupo de administración para servidores de Microsoft Exchange. Cada grupo de administración está gestionado por su propia directiva. Las tareas *Database Update* y *On-demand scan* se crean para todos los servidores de la organización.

  La clave de activación de KSWS se agrega a Kaspersky Security Center. La distribución automática de claves está activada.

- Servidores SQL con Kaspersky Security for Windows Server 11.0.1 y Kaspersky Endpoint Agent 3.11 instalados. Los servidores SQL se combinan en dos clústeres.

  KSWS es administrado por las directivas *SQL_Policy(1)* y *SQL_Policy(2)*. También se crean las tareas *Database Update*, *On-demand scan*.

- Un servidor de Microsoft Exchange con Kaspersky Security for Windows Server 11.0.1 y Kaspersky Endpoint Agent 3.11 instalados.

  KSWS es administrado por la directiva *Exchange_Policy*. También se crean las tareas *Database Update*, *On-demand scan*.

Planificación de la migración

La migración implica los siguientes pasos:

1. Migración de tareas y directivas de KSWS mediante el Asistente de conversión por lotes de directivas y tareas.
2. Migración de la directiva de Kaspersky Endpoint Agent mediante el Asistente de conversión por lotes de directivas y tareas.
3. Uso de etiquetas para activar perfiles de directivas en las propiedades de la nueva directiva.
4. Instalación de KES en lugar de KSWS.
5. Activación de EDR Optimum.
6. Confirmación de que KES funciona.

El escenario de migración se realiza inicialmente en uno de los clústeres de servidores SQL. A continuación, el escenario de migración se realiza en el otro clúster de servidores SQL. Posteriormente, el escenario de migración se realiza en Microsoft Exchange.

Migración de tareas y directivas de KSWS mediante el Asistente de conversión por lotes de directivas y tareas

Para migrar tareas de KSWS, puede usar el Asistente de conversión por lotes de directivas y tareas (el asistente de migración). Como resultado, en lugar de las directivas *SQL_Policy(1)*, *SQL_Policy(2)*, y *Exchange_Policy*, obtendrá una única directiva con tres perfiles para servidores SQL y Microsoft Exchange respectivamente. El nuevo perfil de directiva con la configuración de KSWS se llamará *UpgradedFromKSWS <Nombre de la directiva de Kaspersky Security for Windows Server>*. En las propiedades del perfil, el asistente de migración selecciona automáticamente el la etiqueta de dispositivo `UpgradedFromKSWS` como criterio de activación. Por lo tanto, la configuración del perfil de directiva se aplica a los servidores automáticamente.

Migración de la directiva de Kaspersky Endpoint Agent mediante el Asistente de conversión por lotes de directivas y tareas

Para migrar directivas de Kaspersky Endpoint Agent, puede usar el Asistente de conversión por lotes de directivas y tareas. El Asistente de migración de directivas y tareas para Kaspersky Endpoint Agent solo está disponible en Web Console.

Uso de etiquetas para activar perfiles de directivas en las propiedades de la nueva directiva

Seleccione la etiqueta del dispositivo que asignó anteriormente como condición de activación del perfil. Abra las propiedades de la directiva y seleccione *Reglas generales para la activación de perfiles de directivas* como condición de activación del perfil.

Instalación de KES en lugar de KSWS

Antes de instalar KES, debe desactivar la protección con contraseña en las propiedades de la directiva de KSWS.

La instalación de KES implica los siguientes pasos:

1. Prepare el paquete de instalación. En las propiedades del paquete de instalación, seleccione el kit de distribución de Kaspersky Endpoint Security para Windows 12.0 y seleccione el conjunto predeterminado de componentes.

2. Cree una tarea *Instalar aplicación en remoto* para uno de los grupos de administración del servidor SQL.

3. En las propiedades de la tarea, seleccione el paquete de instalación y el archivo de clave de licencia.

4. Espere hasta que la tarea se complete correctamente.

5. Repita la instalación de KES para los grupos de administración restantes.

Kaspersky Security Center agrega automáticamente la etiqueta `UpgradedFromKSWS` a los nombres de los equipos en la consola después de que se complete la instalación de KES.

Para comprobar la instalación de KES, puede utilizar el *Informe sobre el despliegue de protección*. También puede comprobar el estado del dispositivo. Para confirmar la activación de la aplicación, puede utilizar el *Informe sobre el uso de claves de licencia*.

Activación de EDR Optimum

Puede activar la funcionalidad EDR Optimum mediante una licencia independiente de Kaspersky Endpoint Detection and Response Optimum Add-on. Debe confirmar que la clave EDR Optimum se añada al repositorio de Kaspersky Security Center y que la funcionalidad de distribución automática de claves de licencia esté activada.

Para comprobar la activación de EDR Optimum, puede utilizar el *Informe sobre el estado de los componentes de la aplicación*.

Confirmación de que KES funciona

Para confirmar que KES funciona, puede verificar y ver que no se notifican errores. El estado del dispositivo debe ser *Sin inconvenientes*. Tareas de actualización y análisis antimalware y completadas con éxito.

Modo Light Agent para proteger máquinas virtuales

A partir de la versión 12.8, puede usar Kaspersky Endpoint Security para Windows como parte de Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* es una solución integrada que proporciona una protección completa de las máquinas virtuales contra varios tipos de amenazas a la seguridad de la información, ataques de red y ataques de phishing. Para usar esta solución, debe instalar la aplicación en modo Light Agent.

No se admite la instalación de Kaspersky Endpoint Security en modo de Light Agent en máquinas virtuales basadas en Arm.

Puede usar Kaspersky Endpoint Security en el modo Light Agent como parte de Kaspersky Security for Virtualization Light Agent a partir de la versión 6.2.

Cuando inicia Light Agent, establece y mantiene una conexión a la máquina virtual SVM (Secure Virtual Machine). En la SVM se implementa un Servidor de protección. El *Servidor de protección* es el componente de la solución Kaspersky Security for Virtualization Light Agent que analiza archivos en busca de virus y otro malware, actualiza las bases de datos antivirus y administra las claves de licencia. Light Agent envía a la SVM los archivos o sus fragmentos que deben analizarse. Los resultados del análisis están disponibles para todas las máquinas virtuales con Light Agent instalado (tecnología SharedCache). Esta tecnología aumenta la eficiencia de la solución y proporciona una respuesta más rápida a las amenazas.

La infraestructura de la organización puede contener muchas máquinas virtuales con Light Agent instalado, y muchas SVM. El Servidor de integración gestiona la interacción entre las máquinas virtuales y las SVM. El *Servidor de integración* es un componente de la solución Kaspersky Security for Virtualization Light Agent que genera una lista de SVM disponibles y transfiere estos datos a Light Agents, participa en la detección de SVM por parte de Light Agents, protege la conexión entre Light Agents y SVM, y realiza otras funciones.

Consideraciones especiales para el modo Light Agent

Puede administrar Kaspersky Endpoint Security en el modo Estándar y en el modo Light Agent mediante las directivas y tareas de Kaspersky Endpoint Security. En el modo Light Agent, algunos componentes y funciones de la aplicación no están disponibles.

Actualización de las bases de datos y módulos de la aplicación

Kaspersky Endpoint Security en modo Light Agent utiliza bases de datos de malware especiales que la aplicación necesita cuando funciona como parte de la solución Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security obtiene las actualizaciones de los módulos de la aplicación y las bases de datos del Servidor de protección.

Las bases de datos y los módulos de las máquinas virtuales protegidas se actualizan mediante una tarea *Actualización de las bases de datos y módulos de la aplicación*, en la que se especifica una carpeta en la SVM como origen de actualización. Light Agent ejecuta la tarea *Actualización de las bases de datos y módulos de la aplicación* automáticamente. No puede seleccionar un origen de actualización diferente, configurar la programación de la tarea o eliminar la tarea.

La reversión de la última actualización de la base de datos de malware también se gestiona en el lado del Servidor de protección. Después de una reversión de una actualización de bases de datos y módulos de aplicación en la SVM, se inicia una tarea local especial *Actualización de las bases de datos y módulos de la aplicación* en la máquina virtual protegida. Esta tarea hace que el Light Agent vuelva a utilizar el conjunto de bases de datos de malware anterior.

Kaspersky Endpoint Security en modo Light Agent no admite la tarea *Revertir actualización*.

Activación de Light Agent

Para activar la aplicación, debe añadir una clave de licencia a la SVM a la que está conectado el Light Agent. No es necesario que active la aplicación por separado.

Otras consideraciones especiales para el modo Light Agent

- Cuando cree una directiva para la aplicación, recomendamos seleccionar el modo Light Agent. En este modo, el Asistente de nueva directiva le solicita que configure la conexión de SVM. Esta configuración es necesaria para que la aplicación funcione en modo Light Agent.
- No puede instalar componentes de cifrado de datos y Control de anomalías adaptativo en el modo Light Agent. El conjunto de componentes también depende del tipo de sistema operativo: estación de trabajo o servidor.
- Light Agent no admite la integración con las soluciones Kaspersky Endpoint Detection and Response Expert y Kaspersky Endpoint Detection and Response Expert (cloud).
- Puede administrar Light Agent en la Consola de administración (MMC) y Kaspersky Security Center Web Console. No se puede administrar el Light Agent en Kaspersky Security Center Cloud Console.
- No se admite el cambio del conjunto de componentes de la aplicación en máquinas virtuales VDI.
- Kaspersky Endpoint Security se comunica con los servidores de KSN a través de un servidor proxy de KSN. No se admite la comunicación directa con KSN.
- No se admite el modo en la nube de Kaspersky Security Network.
- No se admite el uso del servidor proxy de la aplicación al conectarse al Servidor de integración (VIIS), al Servidor de protección (SVM) y a los servidores KSN.

Configuración preliminar de la máquina virtual

Puede instalar Kaspersky Endpoint Security en una máquina virtual que utilice tecnología de plataforma virtual. Kaspersky Endpoint Security admite las plataformas virtuales VMware, Microsoft Hyper-V y Citrix. Antes de la instalación, debe realizar la configuración preliminar de las máquinas virtuales.

Compatibilidad con la tecnología de Citrix App Layering

Si tiene la intención de utilizar el Full User Layer para guardar el estado de las máquinas virtuales temporales, debe hacer lo siguiente antes de realizar la instalación en la plantilla de la máquina virtual:

1. Cree el archivo C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt y añádale las siguientes exclusiones:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. En el registro del sistema operativo, en la clave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, cree un nuevo valor de DWORD denominado MiniFilterBypass y establézcalo en 1.

3. En el registro del sistema operativo, en la clave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, cree un valor de MULTI_SZ denominado ExcludeKey y establézcalo en \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Reinicie la máquina virtual.

Para la instalación en máquinas virtuales en una infraestructura que use Citrix App Layering, debe hacer lo siguiente:

1. Instale el Agente de administración de Kaspersky Security Center y Kaspersky Endpoint Security para Windows en la plantilla de máquina virtual, en la capa de aplicaciones.

2. Cree una imagen de máquina virtual que conste de varias capas.

3. Implemente la imagen creada en hipervisores que admitan la solución Citrix App Layering.

4. Configure la creación de máquinas virtuales temporales a partir de la imagen creada.

Para obtener detalles sobre la instalación del software antivirus junto con Citrix App Layering, consulte la Documentación de Citrix App Layering.

Compatibilidad con la tecnología de Citrix Provisioning (Citrix Provisioning Services)

Para asegurarse de que la aplicación es compatible con la tecnología de Citrix Provisioning (Citrix Provisioning Services):

- Si el software Citrix Provisioning Target Device está instalado en la máquina virtual, debe eliminarlo antes de instalar la aplicación Kaspersky Endpoint Security (para obtener más detalles, visite el sitio web de soporte técnico de Citrix). Después de instalar la aplicación, debe reinstalar Citrix Provisioning Target Device. También debe reinstalar el dispositivo de destino de Citrix Provisioning al restaurar la aplicación, incluso cuando actualice el sistema operativo.

  La actualización del sistema operativo implica los siguientes pasos:

  1. Elimine el dispositivo de destino de Citrix Provisioning.
  2. Actualice el sistema operativo.
  3. Después de iniciar la máquina virtual, asegúrese de que la aplicación Kaspersky Endpoint Security esté en ejecución y funcione correctamente.
  4. Reinstale el dispositivo de destino de Citrix Provisioning.

- Al instalar la aplicación usando el Asistente de instalación o de forma remota mediante Kaspersky Security Center, debe seleccionar la casilla de verificación **Garantizar la compatibilidad con Citrix PVS**.

Compatibilidad con la tecnología de Omnissa App Volumes

Antes de realizar la instalación en la plantilla de la máquina virtual, debe crear el archivo %SVAgent%\Config\Custom\snapvol.cfg y añadirle las siguientes exclusiones:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`

- exclude_process_path=\Program Files\Kaspersky Lab
- exclude_process_name=avp.exe
- exclude_process_name=klnagent.exe
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon

Para más detalles, consulte la documentación de Omnissa.

Instalación de Instale Light Agent

No se admite la instalación de Kaspersky Endpoint Security en modo de Light Agent en máquinas virtuales basadas en Arm.

La instalación de la aplicación en el modo Light Agent es la misma que en el modo Estándar. Antes de instalar Light Agent en una máquina virtual, debe asegurarse de que Kaspersky Security Center Network Agent esté instalado. El *Agente de red* facilita la interacción entre el Servidor de administración y una máquina virtual.

Light Agent se puede instalar en el equipo de una de las siguientes maneras:

- De forma remota utilizando Kaspersky Security Center.
- De forma local, utilizando el Asistente de configuración.
- De forma local, utilizando la línea de comandos.

Para instalar Light Agent, debe seleccionar la configuración adecuada en la configuración del paquete de instalación o en el Asistente de configuración.

Al instalar Light Agent en un servidor, los componentes de protección avanzada (Detección de comportamiento, Prevención de vulnerabilidades, Motor de reparación) se excluyen de la configuración predeterminada de la aplicación. La configuración predeterminada de la aplicación proporciona el nivel de protección recomendado y el uso óptimo de los recursos del servidor. Al instalar Light Agent en una estación de trabajo, los componentes de protección avanzada se incluyen en la configuración predeterminada de la aplicación.

Al instalar Light Agent, recomendamos seleccionar exclusiones y aplicaciones de confianza predefinidas para el entorno virtual correspondiente. Las exclusiones de análisis y aplicaciones de confianza predefinidas le ayudan a configurar rápidamente la aplicación y evitar problemas de compatibilidad con el entorno virtual. También puede configurar exclusiones de análisis y aplicaciones de confianza predefinidas después de la instalación, en la directiva.

Cómo instalar Light Agent con el Asistente de configuración

1. Copie la carpeta del kit de distribución en la máquina virtual.
2. Ejecute setup_kes.exe.

   Se iniciará el Asistente de instalación.

Configuración de Kaspersky Endpoint Security



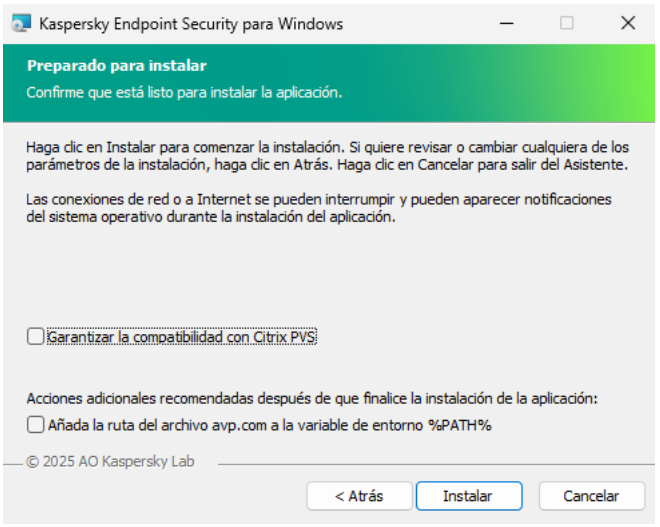
Elección de la configuración de la aplicación

Seleccione la configuración de **Light Agent para proteger entornos virtuales**. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Los componentes de Kaspersky Endpoint Security

Seleccione los componentes que desea instalar (consulte la figura a continuación). Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación. Para ello, tiene que ejecutar el Asistente de instalación de nuevo y elegir cambiar los componentes disponibles.

Configuración avanzada



Configuración de la instalación de la aplicación avanzada

Proteger el proceso de instalación de la aplicación. La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Windows Remote Desktop), se aconseja que desactive la protección del proceso de instalación.

Garantizar la compatibilidad con Citrix PVS. Puede habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual.

Añada la ruta del archivo avp.com a la variable de entorno %PATH%. Puede añadir la ruta de instalación a la variable %PATH% para un uso conveniente de la interfaz de línea de comandos.

Cómo instalar Light Agent utilizando la línea de comandos

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   o bien

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   La opción `VDI` activa el modo de protección de la VDI (Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas. De manera predeterminada, el modo de protección de VDI está activado.

Como resultado, Light Agent se instala en la máquina virtual con el conjunto de componentes predeterminado. Puede editar el conjunto de componentes y especificar la configuración avanzada mediante el archivo setup.ini. También puede especificar la configuración de instalación en la línea de comandos.

Cómo instalar Light Agent usando la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione la carpeta **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

   Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.
3. Abra las propiedades del paquete de instalación de Kaspersky Endpoint Security para Windows.

   Si necesario, cree un nuevo paquete de instalación.
4. Vaya a la sección **Configuración**.
5. Seleccione la configuración de **Light Agent para proteger entornos virtuales**. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.
6. Seleccione los componentes que desee instalar.

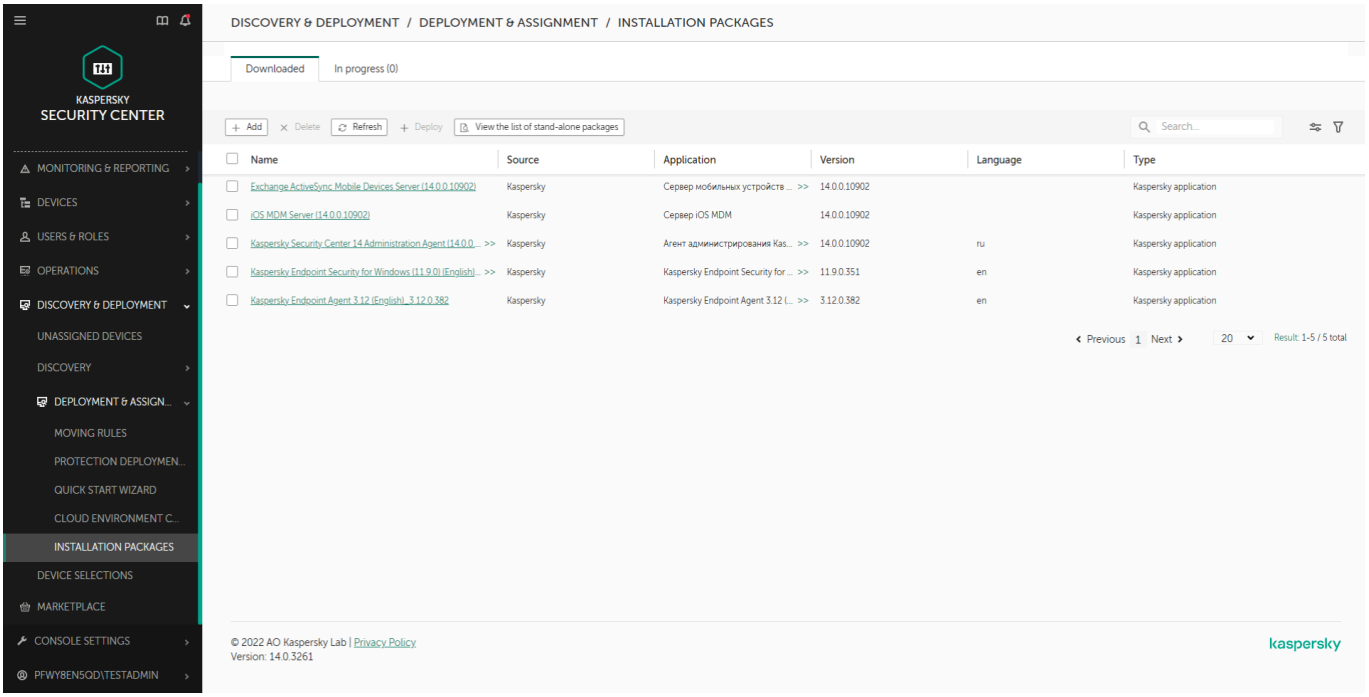
   Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación.
7. Configurar la zona de confianza. Seleccione exclusiones de análisis y aplicaciones de confianza predefinidas para el entorno virtual en el que está instalando la aplicación.

   Las exclusiones de análisis y aplicaciones de confianza predefinidas le ayudan a configurar rápidamente la aplicación y evitar problemas de compatibilidad con el entorno virtual.
8. Guarde los cambios.
9. Crear de una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que ha creado.

Cómo instalar Light Agent usando Web Console

1. En la ventana principal de Web Console, seleccione **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

Esto abre una lista de paquetes de instalación que se han descargado a Kaspersky Security Center.



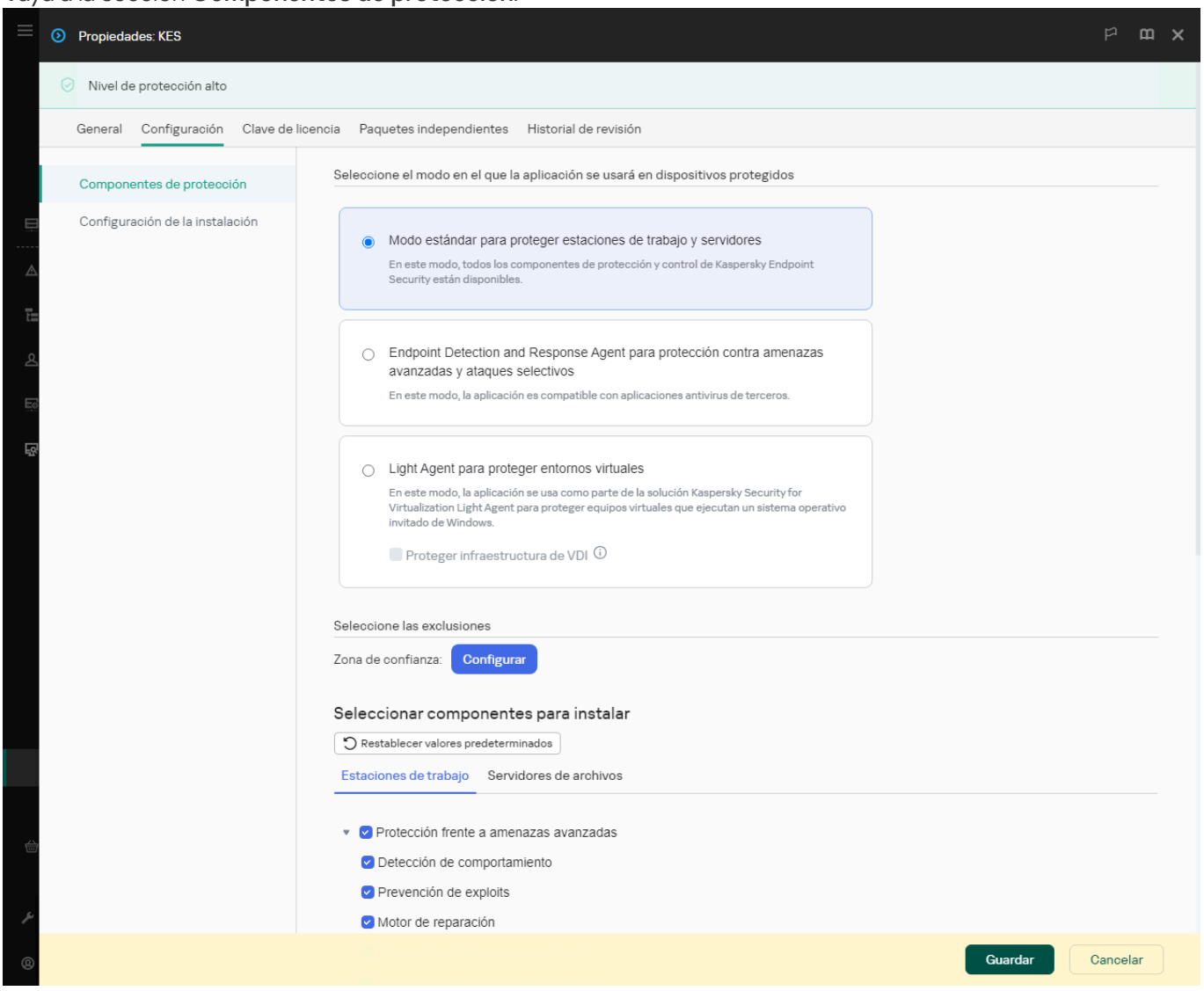
Lista de paquetes de instalación

2. Abra las propiedades del paquete de instalación de Kaspersky Endpoint Security para Windows.

   Si necesario, cree un nuevo paquete de instalación.

3. Seleccione la pestaña **Configuración**.

4. Vaya a la sección **Componentes de protección**.



Componentes incluidos en el paquete de instalación

5. Seleccione la configuración de **Light Agent para proteger entornos virtuales**. Esta configuración está destinada a la aplicación que se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent. Light Agent debe instalarse en cada máquina virtual que deba protegerse con la solución. En esta configuración, no puede utilizar los componentes de cifrado de datos ni el control de anomalías adaptativo. Si está instalando Light Agent en una plantilla de máquina virtual que se usará para crear *máquinas virtuales no persistentes*, seleccione la casilla **Proteger infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que requieren reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que requieren un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

6. Seleccione los componentes que desee instalar.

   Puede cambiar los componentes de la aplicación disponibles después de haber instalado la aplicación.

7. Configurar la zona de confianza. Seleccione exclusiones de análisis y aplicaciones de confianza predefinidas para el entorno virtual en el que está instalando la aplicación.

   Las exclusiones de análisis y aplicaciones de confianza predefinidas le ayudan a configurar rápidamente la aplicación y evitar problemas de compatibilidad con el entorno virtual.

8. Guarde los cambios.

9. Crear de una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que ha creado.

Como resultado, Light Agent se instala en la máquina virtual. Puede utilizar la interfaz de la aplicación; aparece un icono de la aplicación en el área de notificaciones . Ahora necesita configurar la conexión del Light Agent a SVM.



Ventana principal de Light Agent

Conexión de Light Agent a SVM

La solución de Kaspersky Security for Virtualization Light Agent requiere una comunicación continua entre Light Agent y SVM. Esto es necesario para analizar los archivos enviados por el Light Agent en busca de virus y otro malware. Sin una conexión de SVM, el Light Agent no puede enviar archivos para su análisis. Si no se puede establecer la conexión durante más de cinco minutos, el análisis finaliza con un error.

La conexión de un Light Agent a una SVM implica los siguientes pasos:

1. El Light Agent obtiene la lista de SVM disponibles.

2. El Light Agent determina un Servidor de protección (SVM) disponible que es óptimo para la conexión de acuerdo con el Algoritmo de selección de SVM.

3. El Light Agent comprueba la configuración de conexión de SVM adicional: etiquetas, estado de protección de la conexión, funcionalidad de la aplicación cubierta por la licencia.

4. Conexión del Light Agent a SVM.

Puede obtener información sobre el estado de la conexión del Agente Light a la SVM en Kaspersky Endpoint Security o utilizando el comando de la aplicación. La aplicación genera un evento cada vez que la conexión de SVM del Light Agent se pierde o establece, y envía estos eventos a Kaspersky Security Center. Si está utilizando un Servidor de integración para la detección de SVM, puede obtener información sobre el estado de la SVM y la cantidad de Light Agents conectados en la Consola del Servidor de integración. Para obtener detalles sobre la supervisión del estado de SVM, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Detección de SVM

Puede seleccionar uno de los métodos de detección de SVM para el Light Agent:

- Usar el Servidor de integración (VIIS).

  El *Servidor de integración* es el componente de la solución que permite la interacción de Kaspersky Security for Virtualization Light Agent con la infraestructura virtual y genera una lista de SVM disponibles para la conexión. El Light Agent establece una conexión con el Servidor de integración y obtiene la lista de direcciones de SVM.

  El Servidor de integración resulta especialmente útil en infraestructuras virtuales de gran tamaño, ya que equilibra automáticamente la carga entre las SVM, obtiene información sobre las SVM disponibles, analiza esta información y proporciona a los Light Agents una lista de Servidores de protección (SVM) óptimos para la conexión.

  Para que el Light Agent pueda obtener una lista de SVM, solo necesita introducir la dirección del Servidor de integración.

- Uso de un clúster de Servidores de integración de alta disponibilidad.

  El despliegue de un clúster de Servidores de integración de alta disponibilidad está disponible en Kaspersky Security for Virtualization Light Agent a partir de la versión 6.4. Un clúster de Servidores de integración de alta disponibilidad proporciona protección ininterrumpida del entorno virtual gracias a la conmutación por error de las SVM y los Light Agents a un Servidor de integración de reserva cuando falla el Servidor de integración principal. Un componente especial del clúster, el *balanceador de carga*, se encarga de la conmutación por error del servidor. Para obtener más información sobre los clústeres de Servidores de integración de alta disponibilidad, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

  Para que el Light Agent obtenga una lista de SVM, debe introducir la dirección del dispositivo en el que está instalado el balanceador de carga.

- Usar la lista de direcciones de SVM.

  Si necesita especificar SVM individuales a las que desea que el Light Agent se conecte, puede preparar una lista manualmente.

  Debe enumerar las direcciones de las SVM disponibles a las que el Light Agent se puede conectar.

Cómo configurar la detección de SVM por parte del Light Agent en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Directivas**.
3. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Modo Light Agent → Configuración de detección de SVM**.

5. Seleccione un método de detección de SVM.

   - **Utilizar servidor de integración**. Introduzca los parámetros de conexión al Servidor de integración en función de su infraestructura:

     - **Servidor de integración único**. Introduzca los parámetros de conexión al Servidor de integración: la dirección IPv4 o el nombre de dominio completo (FQDN) del dispositivo.

     - **Clúster de Servidores de integración de alta disponibilidad**. Introduzca la dirección IP y el puerto del balanceador de carga que forma parte del clúster.

   - **Utilizar una lista personalizada de direcciones de SVM**. Cree una lista de SVM a las que Light Agent se puede conectar. Especifique la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) de SVM. Cada elemento de la lista debe introducirse en una nueva línea o separarse del elemento anterior con un punto y coma (`;`).

     > En la lista de direcciones de SVM, especifique solo los nombres de dominio completos (FQDN) que coincidan con una única dirección IP. El uso de un nombre de dominio completo que corresponda a varias direcciones IP puede provocar errores en la solución.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar la detección de SVM por parte del Light Agent en la consola web

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Modo Light Agent** → **Configuración de detección de SVM**.

5. Seleccione un método de detección de SVM.

   - **Usar servidor de integración**. Introduzca los parámetros de conexión al Servidor de integración en función de su infraestructura:

     - **Servidor de integración único**. Introduzca los parámetros de conexión al Servidor de integración: la dirección IPv4 o el nombre de dominio completo (FQDN) del dispositivo.

     - **Clúster de Servidores de integración de alta disponibilidad**. Introduzca la dirección IP y el puerto del balanceador de carga que forma parte del clúster.

- **Usar una lista personalizada de direcciones de SVM**. Cree una lista de SVM a las que Light Agent se puede conectar. Especifique la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) de SVM. Cada elemento de la lista debe introducirse en una nueva línea o separarse del elemento anterior con un punto y coma (`;`).

  > En la lista de direcciones de SVM, especifique solo los nombres de dominio completos (FQDN) que coincidan con una única dirección IP. El uso de un nombre de dominio completo que corresponda a varias direcciones IP puede provocar errores en la solución.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar la detección de SVM por parte del Light Agent en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, en **Modo Light Agent** haga clic en el mosaico **Configuración de detección de SVM**.
3. Seleccione un método de detección de SVM.
   - **Utilizar servidor de integración**. Introduzca los parámetros de conexión al Servidor de integración en función de su infraestructura:
     - **Servidor de integración único**. Introduzca los parámetros de conexión al Servidor de integración: la dirección IPv4 o el nombre de dominio completo (FQDN) del dispositivo.
     - **Clúster de Servidores de integración de alta disponibilidad**. Introduzca la dirección IP y el puerto del balanceador de carga que forma parte del clúster.
   - **Utilizar una lista personalizada de direcciones de SVM**. Cree una lista de SVM a las que Light Agent se puede conectar. Especifique la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) de SVM. Cada elemento de la lista debe introducirse en una nueva línea o separarse del elemento anterior con un punto y coma (`;`).

     > En la lista de direcciones de SVM, especifique solo los nombres de dominio completos (FQDN) que coincidan con una única dirección IP. El uso de un nombre de dominio completo que corresponda a varias direcciones IP puede provocar errores en la solución.

4. Guarde los cambios.

Configuración del algoritmo de selección de SVM para Light Agent

La infraestructura de la organización puede tener múltiples SVM implementadas a las que los Light Agents se pueden conectar. Para equilibrar la carga en la red y los recursos de la infraestructura virtual, debe distribuir los Light Agents entre las SVM.

Algoritmos de selección de SVM

Los Light Agents pueden aplicar los siguientes algoritmos de selección de SVM para la conexión: el algoritmo estándar (de forma predeterminada) y el algoritmo ampliado.

Algoritmos de selección de SVM

<table>
<tr><th>Algoritmo estándar</th><th>Algoritmo ampliado</th></tr>
<tr><td>Si se utiliza este algoritmo, después de la instalación y el inicio, el Light Agent en la máquina virtual elige conectarse a una SVM que es local con respecto al Light Agent.
Si no se encuentran SVM locales adecuadas para la conexión, el Light Agent selecciona una SVM a la que se conecta el menor número de Light Agents, independientemente de la posición de la SVM en la infraestructura virtual.
La aplicación no determina si la SVM es local con respecto al Light Agent si el modo de protección de infraestructuras grandes está activado para el Servidor de protección en la SVM. En este caso, se recomienda utilizar el algoritmo extendido de selección de SVM y seleccionar el Servidor de integración como método de detección de SVM.
Que una SVM se considere local para un Light Agent depende del tipo de infraestructura virtual.</td><td>Si se aplica este algoritmo, puede definir las siguientes opciones de configuración de selección de SVM:
• si se debe tener en cuenta o ignorar la ubicación de la SVM en la infraestructura al elegir las SVM para la conexión
• si se tiene en cuenta la ubicación de la SVM, el método para determinar la localidad de la SVM con respecto al Light Agent
Si los Light Agents ignoran la ubicación de las SVM en la infraestructura, los Light Agents podrán conectarse a cualquier SVM disponible para la conexión.
Si los Light Agents deben tener en cuenta la ubicación de las SVM en la infraestructura, debe seleccionar el tipo de ruta de la SVM que se tendrá en cuenta al determinar la localidad de la SVM con respecto al Light Agent. Que una SVM se considere local para el Light Agent depende del tipo de infraestructura virtual.
Si los Light Agents tienen en cuenta la ubicación de las SVM en la infraestructura al elegir a qué SVM conectarse, los Light Agents solo pueden conectarse a las SVM locales.
Por ejemplo, si especifica un clúster de hipervisor como tipo de ruta de la SVM, todas las SVM implementadas en este clúster de hipervisor se considerarán locales para el Light Agent, y el Light Agent solo podrá conectarse a una de estas SVM. Si no hay ninguna SVM disponible para la conexión en el mismo clúster en el que se ejecuta el Light Agent, el Light Agent no se conecta a ninguna SVM.
Al seleccionar las SVM, los Light Agents también tienen en cuenta el número de Light Agents conectados para garantizar que los Light Agents se distribuyan de forma uniforme entre las SVM disponibles para la conexión.
Si el Light Agent utiliza el algoritmo extendido de selección de SVM, el método de detección de SVM está establecido en lista de direcciones de SVM y el modo de protección de infraestructuras grandes está activado en la SVM, la conexión de un Light Agent a esta SVM solo es posible si se ignora la ruta de la SVM.</td></tr>
<tr><td colspan="2">Basis Dynamix Enterprise</td></tr>
<tr><td>En una infraestructura virtual basada en Basis Dynamix Enterprise, la SVM que se considera local para un Light Agent es la SVM implementada en el mismo nodo que la máquina virtual que tiene instalado el Light Agent.</td><td>En una infraestructura virtual basada en Basis Dynamix Enterprise, una SVM puede considerarse local para el Light Agent en cualquiera de los siguientes casos:
• Una SVM está implementada en el mismo nodo que la máquina virtual que tiene instalado el Light Agent.
• Una SVM está implementada en la misma zona que la máquina virtual que tiene instalado el Light Agent.
• Una SVM está implementada en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent.</td></tr>
<tr><td colspan="2">Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer y Basis Dynamix Standard</td></tr>
</table>

Algoritmo estándar	Algoritmo ampliado
En una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard, la SVM que se considera local para un Light Agent es la SVM implementada en el mismo hipervisor que la máquina virtual que tiene instalado el Light Agent.	En una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard, una SVM puede considerarse local para el Light Agent en cualquiera de los siguientes casos: • Una SVM está implementada en el mismo hipervisor que la máquina virtual que tiene instalado el Light Agent. • Una SVM está implementada en el mismo clúster de hipervisor que la máquina virtual que tiene instalado el Light Agent. • Una SVM está implementada en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent.
SVM de OpenStack y VK Private Cloud	
En una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud, puede especificar cómo determinar la localidad de la SVM con respecto al Light Agent mediante el parámetro `StandardAlgorithmSvmLocality` de la sección `HypervisorSpecificSettings:Openstack` del archivo de configuración appsettings.json del Servidor de integración. En función de la versión del Servidor de integración, el archivo se encuentra en una de las siguientes rutas: • /var/opt/kaspersky/viis/common/ para el Servidor de integración basado en Linux • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ para el Servidor de integración basado en Windows El parámetro `StandardAlgorithmSvmLocality` puede tener los siguientes valores: • `ServerGroup` – si se selecciona este valor, una SVM se considera local para el Light Agent si se encuentra dentro del mismo grupo de servidores que la máquina virtual que tiene instalado el Light Agent. Este valor se utiliza de forma predeterminada. • `Project` – si se selecciona este valor, una SVM se considera local para el Light Agent si está implementada dentro del mismo proyecto de OpenStack que la máquina virtual que tiene instalado el Light Agent. • `AvailabilityZone` – si se selecciona este valor, una SVM se considera local para el Light Agent si se encuentra dentro de la misma zona de disponibilidad que la máquina virtual que tiene instalado el Light Agent.	En una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud, una SVM puede considerarse local para el Light Agent en cualquiera de los siguientes casos: • Una SVM se encuentra en el mismo grupo de servidores que la máquina virtual que tiene instalado el Light Agent. • Una SVM está implementada en el mismo proyecto de OpenStack que la máquina virtual que tiene instalado el Light Agent. • Una SVM se encuentra en la misma zona de disponibilidad que la máquina virtual que tiene instalado el Light Agent.

Además de los algoritmos de conexión de SVM, puede regular la conexión de Light Agents a SVM mediante etiquetas.

Configuración del algoritmo de selección de SVM

Cómo configurar el algoritmo de selección de SVM para Light Agent en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Modo Light Agent** → **Algoritmo de selección de SVM**.
4. Seleccione el algoritmo:
   - **Utilizar el algoritmo de selección de SVM estándar**. Light Agent selecciona las SVM, implementadas en el mismo hipervisor.
   - **Utilizar el algoritmo de selección de SVM ampliado**. Light Agent selecciona las SVM implementadas en el tipo de ruta de SVM seleccionado (de forma predeterminada, **Hypervisor**).

5. Si es necesario, seleccione la ruta de SVM para el algoritmo de selección de SVM ampliado:

- **Hypervisor**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo hipervisor que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - La SVM se encuentra en el mismo grupo de servidores que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en el mismo nodo que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

  Si no hay ninguna SVM disponible para la conexión en el mismo hipervisor o en el mismo grupo de servidores donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Clúster**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo clúster de hipervisores que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Las SVM están implementadas en el mismo proyecto de OpenStack que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en la misma zona que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

  Si no hay ninguna SVM disponible para la conexión en el mismo clúster de hipervisores o en el mismo proyecto de OpenStack donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Centro de datos**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Las SVM se encuentran en la misma zona de disponibilidad que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

Si no hay SVM disponibles para la conexión en el mismo centro de datos o zona de disponibilidad donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Ignorar**. Light Agent ignora la ruta de SVM para conectarse al Servidor de protección. Los Light Agents tienen en cuenta otros criterios: etiquetas, el número de Light Agents conectados a una SVM, etc.

6. Guarde los cambios.

Cómo configurar el algoritmo de selección de SVM para Light Agent en la consola web

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Modo Light Agent** → **Algoritmo de selección de SVM**.
5. Seleccione el algoritmo:

   - **Usar el algoritmo de selección de SVM estándar**. Light Agent selecciona las SVM, implementadas en el mismo hipervisor.
   - **Usar el algoritmo de selección de SVM ampliado**. Light Agent selecciona las SVM implementadas en el tipo de ruta de SVM seleccionado (de forma predeterminada, **Hypervisor**).
6. Si es necesario, seleccione la ruta de SVM para el algoritmo de selección de SVM ampliado:

   - **Hypervisor**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

     - Las SVM están implementadas en el mismo hipervisor que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).
     - La SVM se encuentra en el mismo grupo de servidores que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).
     - La SVM se encuentra en el mismo nodo que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

     Si no hay ninguna SVM disponible para la conexión en el mismo hipervisor o en el mismo grupo de servidores donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Clúster**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo clúster de hipervisores que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Las SVM están implementadas en el mismo proyecto de OpenStack que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en la misma zona que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

  Si no hay ninguna SVM disponible para la conexión en el mismo clúster de hipervisores o en el mismo proyecto de OpenStack donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Centro de datos**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Las SVM se encuentran en la misma zona de disponibilidad que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

  Si no hay SVM disponibles para la conexión en el mismo centro de datos o zona de disponibilidad donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Omitir**. Light Agent ignora la ruta de SVM para conectarse al Servidor de protección. Los Light Agents tienen en cuenta otros criterios: etiquetas, el número de Light Agents conectados a una SVM, etc.

7. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar el algoritmo de selección de SVM para Light Agent en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .

2. En la ventana de configuración de la aplicación, en **Modo Light Agent** haga clic en el mosaico **Configuración de detección de SVM**.

3. Seleccione el algoritmo:

   - **Utilizar el algoritmo de selección de SVM estándar**. Light Agent selecciona las SVM, implementadas en el mismo hipervisor.

   - **Utilizar el algoritmo de selección de SVM ampliado**. Light Agent selecciona las SVM implementadas en el tipo de ruta de SVM seleccionado (de forma predeterminada, **Hypervisor**).

4. Si es necesario, seleccione la ruta de SVM para el algoritmo de selección de SVM ampliado:

- **Hypervisor**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo hipervisor que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - La SVM se encuentra en el mismo grupo de servidores que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en el mismo nodo que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

  Si no hay ninguna SVM disponible para la conexión en el mismo hipervisor o en el mismo grupo de servidores donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Clúster**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo clúster de hipervisores que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Las SVM están implementadas en el mismo proyecto de OpenStack que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en la misma zona que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

  Si no hay ninguna SVM disponible para la conexión en el mismo clúster de hipervisores o en el mismo proyecto de OpenStack donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Centro de datos**. El Light Agent selecciona una SVM a la que conectarse que cumpla los criterios (según el tipo de infraestructura virtual):

  - Las SVM están implementadas en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual basada en Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Las SVM se encuentran en la misma zona de disponibilidad que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud).

  - La SVM se encuentra en el mismo centro de datos que la máquina virtual que tiene instalado el Light Agent (en una infraestructura virtual Basis Dynamix Enterprise).

Si no hay SVM disponibles para la conexión en el mismo centro de datos o zona de disponibilidad donde se encuentra la máquina virtual con el Light Agent, el Light Agent no se conecta a la SVM.

- **Ignorar**. Light Agent ignora la ruta de SVM para conectarse al Servidor de protección. Los Light Agents tienen en cuenta otros criterios: etiquetas, el número de Light Agents conectados a una SVM, etc.

5. Guarde los cambios.

Distribución de las conexiones de Light Agents a SVM (etiquetas)

Se pueden conectar varios Light Agents a una SVM. Para equilibrar las conexiones del Light Agent, puede especificar una lista de SVM independiente. Si está utilizando un servidor de integración para el descubrimiento de SVM, puede utilizar *etiquetas* para equilibrar las conexiones del Light Agent a las SVM. Es decir, para un Light Agent, puede asignar una lista de SVM para conectarse mediante una etiqueta. Para hacerlo, debe asignar una etiqueta al Light Agent y especificar esta etiqueta en la configuración de SVM. Para obtener detalles sobre cómo especificar etiquetas en la configuración de SVM, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Ejemplo: la solución Kaspersky Endpoint Detection and Response Optimum se implementa en su infraestructura para los hosts de máquinas virtuales designados. En este caso, puede asignar la etiqueta `[EDROptimum]` al Light Agent para que se conecte a las SVM que tienen añadida la clave de licencia de EDR Optimum (complemento de EDR Optimum). Como resultado, puede usar la funcionalidad EDR Optimum en la máquina virtual con el Light Agent. Al conectar el Light Agent a una SVM sin una clave de licencia de EDR Optimum, la funcionalidad de Kaspersky Endpoint Detection and Response Optimum no está disponible.

Cómo asignar una etiqueta de conexión de SVM a un Light Agent en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Modo Light Agent** → **Etiqueta de conexión de SVM**.
4. Seleccione la casilla de verificación **Usar etiqueta de conexión** e introduzca una etiqueta de conexión a SVM.

   Para una etiqueta, puede introducir una cadena de texto de hasta 255 caracteres. Puede usar cualquier carácter excepto `;`.
5. Guarde los cambios.

Cómo asignar una etiqueta de conexión de SVM a un Light Agent en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Modo Light Agent** → **Etiqueta de conexión de SVM**.

5. Seleccione la casilla de verificación **Usar etiqueta de conexión** e introduzca una etiqueta de conexión a SVM.

   Para una etiqueta, puede introducir una cadena de texto de hasta 255 caracteres. Puede usar cualquier carácter excepto `;`.

6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo asignar una etiqueta de conexión de SVM a un Light Agent en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, en **Modo Light Agent** haga clic en el mosaico **Etiqueta de conexión de SVM**.
3. Seleccione la casilla de verificación **Usar etiqueta de conexión** e introduzca una etiqueta de conexión a SVM.

   Para una etiqueta, puede introducir una cadena de texto de hasta 255 caracteres. Puede usar cualquier carácter excepto `;`.

4. Guarde los cambios.

Protección de la conexión entre un Light Agent y SVM

Puede configurar el cifrado de la conexión entre Light Agents y el Servidor de protección. Para hacerlo, debe activar el cifrado del canal de datos entre el Light Agent y el Servidor de protección en la configuración del Servidor de protección de la SVM y en la configuración del Light Agent.

Un Light Agent para el que la protección de conexión esté activada solo puede conectarse a las SVM para las que esté activado el cifrado del canal de datos entre el Light Agent y el Servidor de protección. Un Light Agent para el que la protección de conexión esté desactivada solo puede conectarse a las SVM para las que el cifrado de canal está desactivado o se permite una conexión no segura entre el Servidor de protección y el Light Agent.

Para obtener detalles sobre la configuración de la protección de la conexión en el Servidor de protección, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Proteger la conexión mediante cifrado puede reducir el rendimiento de Kaspersky Security for Virtualization Light Agent.

Cómo configurar la protección de la conexión en un Light Agent en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Modo Light Agent** → **Protección de la conexión**.
4. Seleccione la casilla **Cifrar canal de datos entre Light Agent y el servidor de protección**.
5. Guarde los cambios.

Cómo configurar la protección de la conexión en un Light Agent en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Modo Light Agent** → **Protección de la conexión**.
5. Seleccione la casilla **Cifrar canal de datos entre Light Agent y el servidor de protección**.
6. Para aplicar la directiva a los equipos, cierre los iconos de candado y guarde los cambios.

Cómo configurar la protección de la conexión en un Light Agent en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, en **Modo Light Agent** haga clic en el mosaico **Protección de la conexión**.
3. Seleccione la casilla **Cifrar canal de datos entre Light Agent y el servidor de protección**.
4. Guarde los cambios.

Activación de Light Agent

Si Kaspersky Endpoint Security se utiliza en modo Light Agent para proteger entornos virtuales, no es necesario activar la aplicación por separado. Para activar la aplicación, debe añadir una clave de licencia a la SVM. Puede añadir una clave de licencia a SVM mediante la tarea especial en la consola de Kaspersky Security Center. No puede administrar las claves de licencia en la interfaz de Light Agent; sin embargo, puede ver la información de la licencia (consulte la figura a continuación). También puede ver la información de licencia de Light Agent en la línea de comandos (consulte las instrucciones a continuación). El Light Agent obtiene esta información de la SVM. Para obtener detalles sobre la activación de la solución y la administración de claves de licencia, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

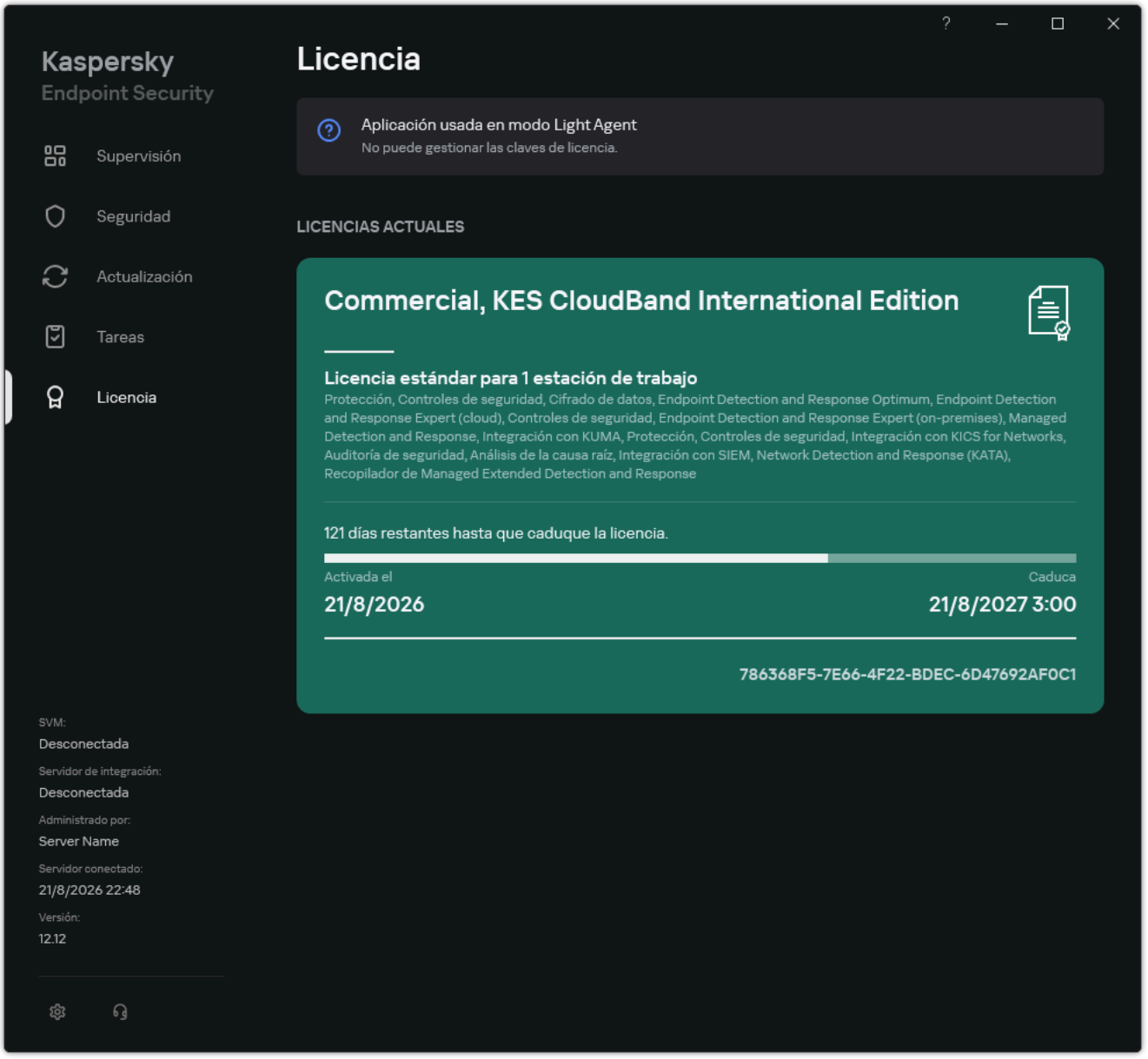
Para ver la información de licencia del Light Agent:

1. Ejecute el intérprete de la línea de comandos (cmd) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

3. Ejecute el siguiente comando:

```
avp.com LICENSE /CHECK
```

Como resultado, Kaspersky Endpoint Security muestra la información de la licencia: dirección de la SVM a la que está conectado el Light Agent, la cantidad de días hasta que caduque la licencia y otra información. Si encuentra algún problema al activar Light Agent, consulte la base de conocimientos de soporte técnico.



Ventana Licencia

Guía de migración de KSVLA Light Agent a KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent incluye el componente Light Agent para Windows 5.2 (en adelante, también denominado "KSVLA Light Agent"). En Kaspersky Security for Virtualization Light Agent 6.2, Kaspersky Endpoint Security en modo Light Agent se utiliza como componente Light Agent. Para actualizar la solución a la versión 6.2, debe migrar de Light Agent 5.2 a Kaspersky Endpoint Security en modo Light Agent (en adelante, también denominado "KES Light Agent"). Para obtener detalles sobre la actualización de la versión de Kaspersky Security for Virtualization Light Agent , consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Requisitos de software

Antes de comenzar la migración de KSVLA Light Agent a KES Light Agent, asegúrese de que su servidor cumpla con los requisitos de hardware y software de Kaspersky Endpoint Security para Windows. Las listas de versiones de sistemas operativos compatibles son diferentes para KES y KSWS. Por ejemplo, KES no es compatible con servidores que ejecutan Windows Server 2003.

Requisitos mínimos de software para migrar de KSVLA Light Agent a KES Light Agent:

- Kaspersky Endpoint Security para Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (incluidos los componentes Servidor de protección y Servidor de integración).
- Kaspersky Security Center 14.2

  Si tiene instalada una versión anterior de Kaspersky Security Center, actualícela a la 14.2 o posterior. En esta versión de Kaspersky Security Center, el asistente de conversión por lotes de directivas y tareas le permite migrar directivas a un perfil en lugar de a una directiva. En esta versión de Kaspersky Security Center, el asistente de conversión por lotes de directivas y tareas también le permite migrar una gama más amplia de configuraciones de directivas.

Pasos de migración

La migración de KSVLA Light Agent a KES Light Agent se realiza de forma semiautomática. Esto es necesario debido a las diferentes arquitecturas de las aplicaciones.

Migre de KSVLA Light Agent a KES Light Agent en el siguiente orden:

1. **Migrar tareas y directivas de KSVLA Light Agent**

   Para migrar la configuración de directivas, debe ejecutar el asistente de conversión por lotes de directivas y tareas (el asistente de migración). Después de migrar la configuración de la directiva, debe configurar manualmente los ajustes que el asistente de migración no puede migrar automáticamente (por ejemplo, la configuración de actualización de la base de datos). Después de la migración, también se recomienda verificar si el asistente de migración ha migrado correctamente todas las configuraciones.

   > Si la protección con contraseña está activada para restringir el acceso a KSVLA Light Agent, antes de instalar KES Light Agent debe desactivar la protección con contraseña en la directiva de KSVLA Light Agent. No puede introducir la contraseña de desinstalación en la configuración del paquete de instalación de KES Light Agent. Después de completar la instalación de KES Light Agent sobre KSVLA Light Agent, debe activar la protección con contraseña en la directiva de KES.

2. **Instalar Kaspersky Endpoint Security en modo Light Agent**

   Puede instalar KES Light Agent de las siguientes maneras:

   - Instalar KES Light Agent después de eliminar KSVLA Light Agent (recomendado)
   - Instalar KES Light Agent sobre el KSVLA Light Agent

3. **Confirme que la aplicación funciona correctamente después de la migración**

   Después de migrar de KSVLA Light Agent a KES Light Agent, asegúrese de que la aplicación funciona correctamente. Active la directiva convertida. Compruebe el estado de la máquina virtual en la consola de Kaspersky Security Center (debe ser *Sin inconvenientes*). Asegúrese de que no se notifiquen errores para la aplicación; compruebe también la hora de la última conexión a SVM y el estado de protección de la máquina virtual. No es necesario activar el Light Agent, ya que la clave de licencia se añade en la SVM.

Instalación de KES Light Agent en lugar de KSVLA Light Agent

Puede instalar KES Light Agent de las siguientes maneras:

- Instalar KES Light Agent después de eliminar KSVLA Light Agent (recomendado)
- Instalar KES Light Agent sobre el KSVLA Light Agent

Eliminación de KSVLA Light Agent

Puede eliminar la aplicación de forma remota utilizando la tarea *Instalar aplicación en remoto* localmente en la máquina virtual o en la plantilla de la máquina virtual. Después de eliminar KSVLA Light Agent, es posible que deba reiniciar la máquina virtual.

Después de eliminar KSVLA Light Agent, instale KES Light Agent utilizando cualquier método adecuado.

Si la protección con contraseña está activada para restringir el acceso a KSVLA Light Agent, antes de instalar KES Light Agent debe desactivar la protección con contraseña en la directiva de KSVLA Light Agent. No puede introducir la contraseña de desinstalación en la configuración del paquete de instalación de KES Light Agent. Después de completar la instalación de KES Light Agent sobre KSVLA Light Agent, debe activar la protección con contraseña en la directiva de KES.

Al instalar Kaspersky Endpoint Security, debe seleccionar el modo **Light Agent para proteger entornos virtuales**. Antes de instalar KES Light Agent en un equipo virtual, el instalador detecta KSVLA Light Agent como software incompatible y lo elimina. No se admite la migración de la configuración de KSVLA Light Agent. Es decir, cuando instala KES Light Agent, el conjunto de componentes que se instala lo determina su selección en las propiedades del paquete de instalación o en el asistente de instalación. Después de eliminar KSVLA Light Agent, debe reiniciar la máquina virtual.

La configuración y las tareas de KSVLA Light Agent no se migran cuando se instala KES Light Agent. Para migrar la configuración y las tareas, ejecute el asistente de conversión por lotes de directivas y tareas.

Puede comprobar la lista de componentes instalados en la sección **Seguridad** de la interfaz de la aplicación, usando el comando `status`, o en la consola de Kaspersky Security Center en las propiedades del equipo. Puede cambiar el conjunto de componentes después de la instalación utilizando los *Cambiar componentes de la aplicación*.

Correspondencia de los componentes de KSVLA Light Agent y de KES Light Agent

Los conjuntos de componentes de KSVLA Light Agent y KES Light Agent son prácticamente los mismos. KES Light Agent tiene más parámetros que KSVLA Light Agent. Después de la migración, la nueva configuración tiene valores predeterminados.

Correspondencia de los componentes de KSVLA Light Agent y de KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Núcleo de la aplicación
File Anti-Virus	Protección frente a amenazas en archivos
Mail Anti-Virus	Protección frente a amenazas en el correo
Web Anti-Virus	Protección frente a amenazas web
Firewall	Firewall
Network Attack Blocker	Protección frente a amenazas en la red
Application Privilege Control	Prevención de intrusiones en el host
Applications Launch Control	Control de aplicaciones
Web Control	Control Web
Device Control	Control de dispositivos
System Watcher	En Kaspersky Endpoint Security, este componente se divide en los siguientes componentes: • Prevención de exploits • Detección de comportamiento • Motor de reparación

Light Agent 5.2	KES Light Agent
System Integrity Monitoring	Control de integridad del sistema
Integration with Kaspersky Endpoint Agent	*(no compatible)* A partir de Kaspersky Endpoint Security para Windows 11.9.0, el paquete de distribución de Kaspersky Endpoint Agent ya no forma parte del kit de distribución.
AMSI Protection	Protección AMSI

Migración de tareas y directivas de KSVLA Light Agent

Puede migrar la configuración de las directivas y tareas de KSVLA Light Agent mediante el Asistente de conversión por lotes de directivas y tareas (en adelante, también denominado "Asistente de migración").

El Asistente de migración para KSVLA Light Agent solo está disponible en la Consola de administración (MMC). La configuración de directivas y tareas no puede migrarse a Web Console y Cloud Console.

Las siguientes consideraciones especiales afectan a la migración de directivas y tareas:

- Una nueva directiva tiene el nombre *<Directiva> (converted)*.
- La directiva nueva tiene el estado *Directiva inactiva*.
- La prohibición de modificar la configuración (el "candado") no se migra. El Asistente de migración establece valores predeterminados.
- Los perfiles de directivas no se migran. Debe añadir los perfiles de directivas manualmente.
- Administración de zona de confianza mejorada. En KSVLA Light Agent puede añadir exclusiones predefinidas solo al crear una directiva. Posteriormente, en las propiedades de la directiva, podría configurar exclusiones predefinidas previamente añadidas o añadir exclusiones manualmente. No pueden añadir exclusiones predefinidas en las propiedades de la directiva. En KES Light Agent, las exclusiones predefinidas están disponibles tanto durante la creación de la directiva como en las propiedades de la directiva creada. También puede seleccionar exclusiones predefinidas en el paquete de instalación.
- La configuración de la interfaz de usuario de la aplicación en Kaspersky Endpoint Security se movió del instalador a la directiva. Si necesita, por ejemplo, ocultar la interfaz de usuario de la aplicación, administre la configuración de directivas.
- Los conjuntos de funciones para configurar el control de acceso basado en derechos (RBAC) son diferentes en Kaspersky Endpoint Security y en KSVLA Light Agent. Debe configurar los derechos de acceso de los usuarios a las áreas funcionales desde cero.

Cómo usar el Asistente de conversión por lotes de directivas y tareas para migrar la configuración de directivas de KSVLA Light Agent.

1. En la Consola de administración, elija el Servidor de administración y haga clic con el botón derecho para abrir el menú contextual.
2. Seleccione **Todas las tareas → Asistente de conversión por lotes de directivas y tareas**.

Se iniciará el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Elija la aplicación para la que necesita convertir directivas y tareas

En este paso, debe elegir Kaspersky Endpoint Security para Windows. Ir al paso siguiente.

Paso 2. Conversión de directivas

Seleccione la directiva de Kaspersky Security for Virtualization 5.2 Light Agent para Windows que desea convertir. Ir al paso siguiente.

A continuación, el Asistente de migración comenzará a convertir las directivas. Durante la conversión, el Asistente de migración le solicita que acepte las condiciones de la Declaración KSN. Una nueva directiva tiene el nombre *<Directiva> (converted)*.

Paso 3. Conversión de tareas

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security para Windows. En la lista de tareas, seleccione las tareas de KSVLA Light Agent que desea crear para Kaspersky Endpoint Security. Las nuevas tareas recibirán el nombre *<Nombre de la tarea> (converted)*. Ir al paso siguiente.

Paso 4: Fin del asistente

Finalice el asistente.

Después de migrar una directiva, debe abrir las propiedades de la misma, verificar su configuración y guardarla. Si no completa estos pasos, KES Light Agent puede ignorar la directiva convertida.

Preste especial atención a la migración de la configuración de la conexión SVM de Light Agent, listas de exclusión, aplicaciones de confianza, direcciones web de confianza y reglas de control de aplicaciones.

Migrar la configuración [KSVLA Light Agent+KEA] a la configuración [KES Light Agent+agente incorporado]

Para admitir el uso de Kaspersky Endpoint Security para Windows como parte de EDR (KATA), EDR Optimum y Kaspersky Sandbox, se ha añadido un agente integrado a la aplicación. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con estas soluciones.

Al migrar de KSVLA Light Agent a KES Light Agent, las soluciones EDR (KATA), EDR Optimum y Kaspersky Sandbox continúan funcionando con agentes incorporados de Kaspersky Endpoint Security. Además, Kaspersky Endpoint Agent se eliminará del equipo.

Antes de migrar de KSVLA Light Agent a KES Light Agent, debe actualizar todos los componentes de Kaspersky Security for Virtualization a la versión 6.2, incluidos el Servidor de protección y el Servidor de integración. Para obtener detalles sobre la actualización de la versión de Kaspersky Security for Virtualization Light Agent , consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

La migración de la configuración de [KSVLAv Light Agent+KEA] a [KES Light Agent+agente incorporado] implica los siguientes pasos:

1. **Migrar las directivas y tareas**

   La migración de las directivas y tareas de [KSVLA Light Agent+KEA] a [KES Light Agent+agente incorporado] implica los siguientes pasos:

   1. Migración de directivas y tareas de KSVLA Light Agent a KES Light Agent mediante el asistente de conversión por lotes de directivas y tareas (solo disponible en la Consola de administración [MMC]).

      Como resultado, se crea una nueva directiva con el nombre *<Directiva> (converted)*. También se crean nuevas tareas de KES con los nombres *<Nombre de tarea> (converted)*.

   2. Migración de directivas y tareas de KEA a KES mediante el asistente de migración de Kaspersky Endpoint Agent (solo disponible en Web Console y Cloud Console).

      Como resultado, se crea una nueva directiva con el nombre *<Nombre de la directiva de Kaspersky Endpoint Security> &<Nombre de la directiva de Kaspersky Endpoint Agent>*. También se crean nuevas tareas y tareas de KES.

2. **Migración de KSVLA Light Agent a KES Light Agent**

   La migración de KSVLA Light Agent a KES Light Agent implica instalar KES Light Agent en lugar de KSVLA Light Agent.

   Los administradores suelen activar la protección con contraseña para restringir el acceso a KSVLA Light Agent y KEA. Solo puede introducir la contraseña de desinstalación de KEA en las propiedades de la tarea *Instalar aplicación en remoto*. Para la migración, debe desactivar la protección con contraseña para KSVLA Light Agent.

   Para realizar la migración, debe seleccionar los componentes necesarios para soportar las soluciones de Detection and Response como parte de Kaspersky Endpoint Security. Tras instalar la aplicación, Kaspersky Endpoint Security pasa a utilizar el agente incorporado y elimina Endpoint Agent de Kaspersky.

3. **Funcionalidad de licencias**

   Si la aplicación se utiliza en modo Light Agent, no es necesario activar la aplicación. Para activar la aplicación, debe añadir una clave de licencia a la SVM. También debe añadir la clave de licencia para activar funciones adicionales (por ejemplo, EDR Optimum) a la SVM. Es decir, como parte de la migración, la concesión de licencia para las funciones se produce automáticamente.

4. **Revisar el estado de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox**

Si, después de la actualización, el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga la versión del Agente de red 13.2 o superior instalada.
- Compruebe el estado operativo del agente integrado consultando el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale el componente con la tarea *Cambiar componentes de la aplicación*.
- Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.
- Asegúrese de que la funcionalidad EDR Optimum esté activada mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No está alcanzado por la licencia*, compruebe que la funcionalidad de distribución automática de claves de licencia de EDR Optimum esté activada.
- Compruebe el estado de la conexión de la máquina virtual a la SVM. Puede obtener información sobre el estado de la conexión del Agente Light a la SVM en Kaspersky Endpoint Security o utilizando el comando de la aplicación.

Administración de la aplicación desde la línea de comandos

Kaspersky Endpoint Security se puede administrar a través de la línea de comandos. Para ver la lista de comandos de administración disponibles, utilice el comando `avp.com HELP`. Para conocer la sintaxis de un comando específico, escriba `avp.com HELP <command>`.

Se deben anular los caracteres especiales en el comando. Para escapar los caracteres `&`, `|`, `(`, `)`, `<`, `>`, `^`, utilice el carácter `^` (por ejemplo, para usar el carácter `&`, introduzca `^&`). Para anular el carácter `%`, introduzca `%%`.

Las alternativas al valor `1` son los valores `yes`, `on`, `enable`, `enabled` y `true`. Las alternativas al valor `0` son los valores `no`, `off`, `disable`, `disabled` y `false`.

Setup. Instalación de la aplicación

La instalación de la aplicación desde la línea de comandos consta de los siguientes pasos:

1. **Elección de un paquete de distribución**

   Kaspersky proporciona paquetes de distribución para diferentes localizaciones que son compatibles con distintas arquitecturas de CPU e incluyen diversos módulos de cifrado.

   El kit de distribución incluye los siguientes paquetes de distribución:

   - **AES256**

     Este paquete de distribución está diseñado para instalarse en equipos con arquitectura x86/x64. Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado AES (Advanced Encryption Standard) con una longitud de clave efectiva de 256 bits.

   - **AES56**

     Este paquete de distribución está diseñado para instalarse en equipos con arquitectura x86/x64. Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado AES con una longitud de clave efectiva de 56 bits.

   - **Arm64**

     Este paquete de distribución está diseñado para su instalación en equipos basados en Arm. Este paquete de distribución no está diseñado para instalarse en servidores.

2. **Transferencia del paquete de distribución de la aplicación al almacenamiento del equipo**

   El paquete de distribución es un archivo autoextraíble en formato EXE. Para ver el contenido del paquete de distribución, debe extraer el archivo en una carpeta independiente. Para instalar la aplicación, necesita todos los archivos del paquete de distribución, incluido el archivo bases.cab.

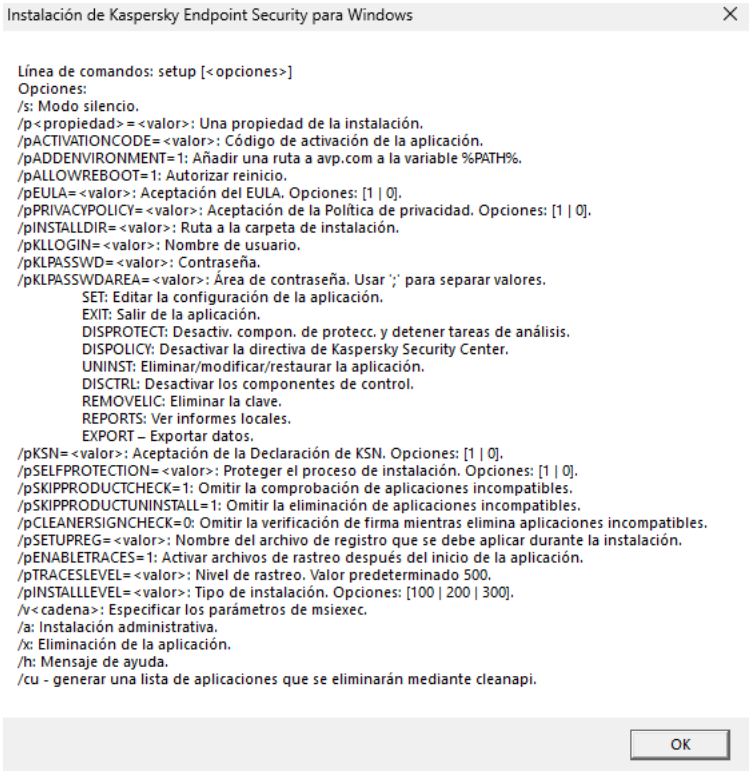
3. **Ejecución del comando de instalación**

Kaspersky Endpoint Security se puede instalar desde la línea de comandos en una de las siguientes formas:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que la instalación se inicie en el modo silencioso, su participación en el proceso de instalación ya no se requiere (instalación silenciosa). Para instalar la aplicación en modo silencioso, utilice las claves `/s` y `/qn`.

> Antes de instalar la aplicación en modo silencioso, abra y lea el Contrato de licencia de usuario final y el texto de la Política de privacidad. Encontrará ambos documentos en el kit de distribución de Kaspersky Endpoint Security. Instale la aplicación únicamente si ha leído y comprende y acepta en su totalidad las disposiciones y los términos del Contrato de licencia de usuario final; si comprende y acepta el hecho de que sus datos se procesarán y transmitirán (incluso a otros países) según lo descrito en la Política de privacidad; y si ha leído y comprende en su totalidad la Política de privacidad. Si no está de acuerdo con las disposiciones y los términos del Contrato de licencia de usuario final y de la Política de privacidad, no instale ni utilice Kaspersky Endpoint Security.

Para ver la lista de comandos de administración disponibles, utilice el comando `/h`. Para obtener ayuda con la sintaxis del comando de instalación, ingrese `setup_kes.exe /h`. Como resultado, el instalador muestra una ventana con una descripción de las opciones del comando (vea la imagen más abajo).



Descripción de las opciones del comando de instalación

Para instalar la aplicación o actualizar una versión anterior de la aplicación:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.

3. Ejecute el siguiente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

o bien

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

Como resultado, la aplicación se instalará en el equipo. Para confirmar que la aplicación está instalada y comprobar su configuración, use el comando `status`.

Configuración de la instalación de la aplicación

`EULA=1`	Aceptación de las condiciones del Contrato de licencia de usuario final. El contenido del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Se requiere la aceptación de los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar la versión de esta.
`PRIVACYPOLICY=1`	Aceptación de la Política de privacidad. El texto de la Política de privacidad se incluye en el Kit de distribución de Kaspersky Endpoint Security. Para instalar la aplicación o actualizar su versión, debe aceptar la Política de privacidad.
`KSN`	Aceptación o rechazo de la participación en Kaspersky Security Network (KSN). Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security solicitará la confirmación de su consentimiento o el rechazo de la participación en KSN cuando se inicie Kaspersky Endpoint Security por primera vez. Valores disponibles: • `1`: aceptación de la participación en KSN. • `0`: rechazo de la participación en KSN (valor predeterminado). El paquete de distribución de Kaspersky Endpoint Security se optimiza para su uso con Kaspersky Security Network. Si optara por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que la instalación se haya completado.
`CONFIGPATH=<path to the configuration file>`	Instalación de la aplicación con configuraciones predefinidas. Para hacerlo, debe subir un archivo que defina la configuración de Kaspersky Endpoint Security. Puede crear un archivo de configuración en la interfaz local de la aplicación.
`ALLOWREBOOT=1`	Reinicio automático del equipo, si es necesario después de la instalación o la actualización de la aplicación. Si no se establece ningún valor para este parámetro, se bloquea el reinicio automático del equipo. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.
`SKIPPRODUCTCHECK=1`	Desactivación de la comprobación de software instalado. La lista de software que puede causar problemas de incompatibilidad está disponible en el archivo incompatible.txt que se incluye en el kit de distribución. Si no se establece ningún valor para este parámetro y se detecta software de la lista, la instalación de Kaspersky Endpoint Security finalizará.
`SKIPPRODUCTUNINSTALL=1`	Desactive la eliminación automática del software detectado de la lista de incompatible.txt. Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security intentará eliminar el software que puede causar problemas de incompatibilidad. No se puede actualizar la eliminación automática del software al instalar Kaspersky Endpoint Security con el instalador msiexec. Para eliminar automáticamente el software que puede causar problemas de compatibilidad, use el archivo setup_kes.exe.

`CLEANERSIGNCHECK=0|1`	Verificación de firmas digitales de los archivos de software detectados de la lista de incompatible.txt. Para eliminar el software, Kaspersky Endpoint Security ejecuta el archivo de instalación del software. Si el archivo de instalación no tiene una firma digital, Kaspersky Endpoint Security considera que el archivo no es de confianza y detiene la eliminación del software para evitar la ejecución de código potencialmente malicioso. Si la aplicación no puede verificar la firma digital del archivo de software detectado, la instalación de Kaspersky Endpoint Security se detiene con un error. El valor predeterminado difiere en función del método de instalación del software: • `0` significa que la verificación de firmas digitales está desactivada (es el valor predeterminado si se implementa a través de Kaspersky Security Center). • `1` significa que la verificación de firma digital está activada (es el valor predeterminado si la aplicación se está instalando localmente).
`STANDALONEMODE=1`	Instalación de la aplicación en la configuración de Endpoint Detection and Response Agent (EDR Agent) para la integración con las soluciones Kaspersky Endpoint Detection and Response (KATA) o Kaspersky Endpoint Detection and Response Expert (on-premises). Esta configuración es necesaria si se implementa una plataforma Endpoint Protection Platform (EPP) de terceros en su organización junto con una solución de clase Kaspersky Endpoint Detection and Response. Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones EPP de terceros.
`KLLOGIN`	Configure el nombre de usuario para acceder a las funciones y ajustes de Kaspersky Endpoint Security (el componente Protección con contraseña). El nombre de usuario se configura junto con los parámetros `KLPASSWD` y `KLPASSWDAREA`. El nombre de usuario KLAdmin se utiliza de forma predeterminada.
`KLPASSWD`	Especifique una contraseña para acceder a las funciones y ajustes de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros `KLLOGIN` y `KLPASSWDAREA`). Si especifica una contraseña, pero no un nombre de usuario con el parámetro `KLLOGIN`, se utilizará de forma predeterminada el nombre de usuario KLAdmin.
`KLPASSWDAREA`	Especifique el alcance de la contraseña para acceder a Kaspersky Endpoint Security. Cuando un usuario intenta realizar una acción que está dentro de este alcance, Kaspersky Endpoint Security solicita las credenciales de la cuenta del usuario (parámetros `KLLOGIN` y `KLPASSWD`). Si necesita especificar más de un valor, use el carácter `;`. Valores disponibles: • `SET`: modificar la configuración de la aplicación. • `EXIT`: salir de la aplicación. • `DISPROTECT`: desactivar componentes de protección y detener tareas de análisis. • `DISPOLICY`: desactivar la directiva de Kaspersky Security Center. • `UNINST`: eliminar la aplicación del equipo. • `DISCTRL`: desactivar componentes de control. • `REMOVELIC`: eliminar la clave. • `REPORTS`: consultar informes. • `EXPORT` - exportar ajustes de la aplicación. Por ejemplo, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`. La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña. Por lo tanto, es imposible configurar la cobertura la contraseña para la cuenta de KLAdmin. Si intenta configurar la cobertura de la contraseña para la cuenta de KLAdmin, la aplicación prohíbe las acciones especificadas para el grupo "Todos".
`PROTECTOSSERVICES`	Funcionalidad de protección de los servicios del sistema operativo. La protección de los servicios del sistema operativo evita que aplicaciones de terceros interfieran con el funcionamiento de los servicios del sistema operativo. Dichos servicios incluyen, por ejemplo, la aplicación del servicio de autoarranque. • `1` significa que la protección de los servicios del sistema operativo está activada (valor predeterminado). • `0` significa que la protección de los servicios del sistema operativo está desactivada.
`ENABLETRACES`	Activar o desactivar el rastreo de la aplicación. Una vez que Kaspersky Endpoint Security se inicia, los archivos de seguimiento se guardan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Valores disponibles: • `1`: el rastreo está activado. • `0`: el rastreo está desactivado (valor predeterminado).
`TRACESLEVEL`	Nivel de detalle del seguimiento. Valores disponibles: • `100` (crítico). Solo mensajes sobre errores graves. • `200` (alto). Mensajes sobre todos los errores, incluidos los errores graves. • `300` (diagnóstico). Mensajes sobre todos los errores, además de las advertencias. • `400` (importante). Todos los mensajes de error y de advertencia, así como otra información adicional. • `500` (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado). • `600` (bajo). Todos los mensajes.

ENABLEAZURESUPPORT	Activación o desactivación del modo de compatibilidad de Azure WVD. Valores disponibles: • 1: modo de compatibilidad de Azure WVD activado. • 0: modo de compatibilidad de Azure WVD desactivado (valor predeterminado). Esta función garantiza que el estado de las máquinas virtuales de Azure se muestre correctamente en la consola de Kaspersky Anti Targeted Attack Platform. Para supervisar el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar un Sensor ID único y permanente a estas máquinas virtuales. Si el modo de compatibilidad se desactiva, el Sensor ID puede cambiar después de reiniciar el equipo debido al funcionamiento de las máquinas virtuales de Azure. Esto puede hacer que aparezcan duplicados de máquinas virtuales en la consola.
AMPPL	Activa o desactiva el uso de la tecnología AM-PPL (Antimalware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para obtener más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019. Valores disponibles: • 1: los procesos de Kaspersky Endpoint Security se protegen con la tecnología AM-PPL. • 0: los procesos de Kaspersky Endpoint Security no se protegen con la tecnología AM-PPL.
UPGRADEMODE	Modo de actualización de la aplicación: • Seamless significa que la aplicación se actualiza con un reinicio del equipo (valor predeterminado). • Force significa que la aplicación se actualiza sin reiniciar. La posibilidad de actualizar la aplicación sin reiniciar se incluye a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo. La posibilidad de instalar parches sin reiniciar también se incluye a partir de la versión 11.11.0. Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. Por tanto, el modo de actualización de la aplicación se especifica en la configuración de la aplicación. Puede cambiar este parámetro en la configuración de la aplicación o en la directiva. Al actualizar una aplicación ya instalada, la prioridad del parámetro de la línea de comandos es menor que la del parámetro especificado en la configuración de la aplicación o en el archivo setup.ini. Por ejemplo, si se especifica el modo de actualización Force en la línea de comandos y el modo Seamless en la configuración de la aplicación, la actualización se instalará sin reiniciar el equipo (Seamless).
RESTAPI	Administrar la aplicación a través de la API REST. Para administrar la aplicación a través de la API REST, debe especificar el nombre de usuario (parámetro RESTAPI_User). Valores disponibles: • 1: se permite la administración a través de la API REST. • 0: se bloquea la administración a través de la API REST (valor predeterminado). Para administrar la aplicación a través de la API REST, debe permitirse la administración mediante sistemas de administración. Para ello, configure el parámetro AdminKitConnector=1. Si administra la aplicación a través de la API REST, no es posible administrarla mediante los sistemas de administración de Kaspersky.
RESTAPI_User	Nombre de usuario de la cuenta de dominio de Windows utilizada para administrar la aplicación a través de la API REST. La administración de la aplicación a través de la API REST solo está disponible para este usuario. Introduzca el nombre de usuario con el formato <DOMAIN>\<UserName> (por ejemplo, RESTAPI_User=COMPANY\Administrator). Solo puede seleccionar un usuario para que funcione con la API REST. Añadir un nombre de usuario es un requisito previo para poder administrar la aplicación a través de la API REST.
RESTAPI_Port	Puerto utilizado para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782. Asegúrese de que el puerto esté libre.
RESTAPI_Certificate	Certificado para identificar solicitudes (por ejemplo, RESTAPI_Certificate=C:\cert.pem). La interacción segura de Kaspersky Endpoint Security con el cliente REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga útil de cada solicitud.
ADMINKITCONNECTOR	Administración de aplicaciones mediante sistemas de administración. Los sistemas de administración incluyen, por ejemplo, Kaspersky Security Center. Además de los sistemas de administración de Kaspersky, puede usar soluciones de terceros. Kaspersky Endpoint Security proporciona una API para este fin. Valores disponibles: • 1: se permite la administración de aplicaciones con la ayuda de sistemas de administración (valor predeterminado). • 0: se permite la administración de aplicaciones solo a través de la interfaz local.

`EnableUniqueSensorID`	Creación de un identificador de equipo único (Sensor ID) durante la instalación o actualización de la aplicación. Sensor ID se utiliza en la solución Kaspersky Anti Targeted Attack Platform para identificar los equipos que envían telemetría al servidor. Al crear Sensor ID, la aplicación utiliza un algoritmo que tiene en cuenta la configuración del equipo, como el número de serie de la placa base. En algunos casos, por ejemplo, al usar la aplicación en un entorno virtual, Sensor ID puede estar duplicado. Como resultado, Kaspersky Anti Targeted Attack Platform no puede identificar el equipo desde el que se envía la telemetría. Para crear un Sensor ID único, debe establecer el parámetro `EnableUniqueSensorID=1`. Como resultado, la aplicación utilizará un algoritmo diferente para crear el Sensor ID, que tiene en cuenta otros datos sobre el equipo. Esto asegura un Sensor ID único. De forma predeterminada, el parámetro no está configurado. La aplicación hereda el Sensor ID en los siguientes casos: • actualización de la versión de la aplicación; • migración de la configuración [KES + KEA] a la configuración [KES + agente incorporado]. Como parte de la reparación de la aplicación, el instalador intenta heredar el Sensor ID. Si el Sensor ID no se puede restaurar, la aplicación crea un nuevo Sensor ID.
`SKIPKB5007186CHECK=1`	Desactivación de la comprobación de la actualización del sistema operativo instalado KB5007186. Antes de instalar la aplicación, el instalador verifica las actualizaciones del sistema operativo instaladas. La actualización KB5007186 está en la lista de actualizaciones del sistema operativo que pueden causar problemas a la aplicación. Para obtener información detallada, consulte la Base de conocimientos de soporte técnico. Por lo tanto, el instalador anula la instalación si se descubre esta actualización. Para continuar con la instalación, establezca `SKIPKB5007186CHECK=1`.

Ejemplo

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Cuando concluya la instalación, Kaspersky Endpoint Security se activará con una licencia de prueba (a menos que haya especificado un código de activación en el archivo setup.ini). La licencia de evaluación suele durar poco tiempo. Cuando finaliza la licencia de evaluación, se desactivan todas las funciones de Kaspersky Endpoint Security. Para continuar usando la aplicación, deberá activarla con una licencia comercial a través del Asistente de activación de la aplicación o con un comando especial.

Al instalar la aplicación o actualizar la versión de aplicación en el modo silencioso, se admite el uso de los archivos siguientes:

- setup.ini: configuración general de instalación de la aplicación.

  Para aplicar la configuración del archivo setup.ini, coloque estos archivos en la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security.

- install.cfg: configuración del funcionamiento de Kaspersky Endpoint Security

  Para aplicar los parámetros del archivo de configuración install.cfg, debe especificar la ruta al archivo en el siguiente comando de instalación de la aplicación: `CONFIGPATH=<path to the configuration file>`.

- setup.reg - claves de registro.

  Las claves del registro del archivo setup.reg se escriben en el registro solo si el valor `setup.reg` está establecido para el parámetro `SetupReg` en el archivo setup.ini. El archivo setup.reg es generado por los expertos de Kaspersky. No se recomienda modificar el contenido de este archivo. Para aplicar la configuración del archivo setup.reg, coloque estos archivos en la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security. También puede colocar el archivo setup.reg en una carpeta diferente. Si lo hace, debe especificar la ruta al archivo en el siguiente comando de instalación de la aplicación: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Eliminar la aplicación

Kaspersky Endpoint Security se puede desinstalar desde la línea de comandos de los siguientes modos:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que la desinstalación se inicie en el modo silencioso, su participación en el proceso de eliminación ya no se requiere (desinstalación silenciosa). Para desinstalar la aplicación en modo silencioso, utilice las claves `/s` y `/qn`.

Para desinstalar la aplicación en modo silencioso:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   - Si el proceso de eliminación no está protegido con contraseña:

     ```
     setup_kes.exe /s /x
     ```

     o bien

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` es el id. único de la aplicación. Puede utilizar el siguiente comando para descubrir el GUID de la aplicación en la Base de conocimientos de soporte técnico:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Si el proceso de eliminación está protegido con contraseña:

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     o bien

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

   También puede utilizar el parámetro `SAVEQB` para guardar los archivos analizados por la aplicación y colocados en Copia de seguridad. Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`. De forma predeterminada, la opción de guardar archivos en Copia de seguridad está desactivada (`SAVEQB=0`).

   Ejemplo

   ```
   msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

msiexec /i. Recuperando la aplicación

Al recuperarse, la aplicación comprueba y restaura la integridad de todos los módulos de la aplicación dañados y las claves de registro del sistema creadas como parte del proceso de instalación de la aplicación.

Kaspersky Endpoint Security se puede recuperar desde la línea de comandos en una de las siguientes formas:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
- En modo silencioso. Tras iniciar la recuperación en el modo silencioso, su participación en el proceso de recuperación ya no se requiere.

Si el instalador de Kaspersky Endpoint Security se está ejecutando en modo de recuperación y la aplicación no necesita recuperación, el instalador no realiza cambios.

Si el instalador de Kaspersky Endpoint Security se está ejecutando en modo de recuperación y la aplicación no está instalada, el instalador inicia el proceso de instalación.

Para recuperar la aplicación en modo silencioso:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:
   - Si el proceso de recuperación no está protegido con contraseña:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` es el id. único de la aplicación. Puede utilizar el siguiente comando para descubrir el GUID de la aplicación en la Base de conocimientos de soporte técnico:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Si el proceso de recuperación está protegido con contraseña:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Ejemplo

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Comandos AVP

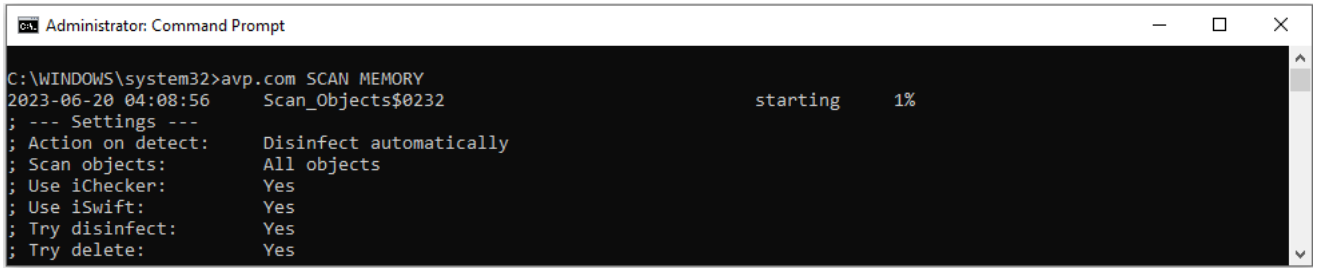
Para administrar Kaspersky Endpoint Security a través de la línea de comandos:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

   Puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% durante la instalación de la aplicación.
3. Utilice la siguiente plantilla para ejecutar el comando:

```
avp.com <command> [options]
```

Kaspersky Endpoint Security ejecutará el comando especificado (consulte la siguiente imagen).



Administración de la aplicación desde la línea de comandos

SCAN. Análisis antimalware

Ejecución de la tarea *Análisis antimalware*.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Cobertura del análisis	
`<files to scan>`	Lista de archivos y carpetas, separados con espacios. Las rutas largas deben estar entre comillas. Las rutas cortas (en formato de MS-DOS) no necesitan las comillas. Por ejemplo: • `"C:\Program Files (x86)\Example Folder"` (ruta larga). • `C:\PROGRA~2\EXAMPL~1` (ruta corta).

`/ALL`	Ejecutar la tarea *Análisis antimalware*. Kaspersky Endpoint Security analiza los siguientes objetos: • Memoria del núcleo • Objetos cargados en el inicio del sistema operativo • Sectores de arranque • Copia de seguridad del sistema operativo • Todas las unidades de disco duro y unidades extraíbles En Kaspersky Endpoint Security para Windows 12.12, el correo electrónico está excluido de la cobertura del análisis de la aplicación. El análisis de los mensajes de correo electrónico entrantes y salientes lo realiza el componente Protección frente a amenazas en el correo. Si está utilizando una versión anterior del complemento de administración, la aplicación excluye el correo electrónico del alcance del análisis, incluso si la directiva lo incluye.
`/MEMORY`	Analizar la memoria del núcleo
`/STARTUP`	Analizar los objetos que se cargan cuando se inicia el sistema operativo
`/REMDRIVES`	Analizar las unidades extraíbles.
`/FIXDRIVES`	Analizar los discos duros.
`/NETDRIVES`	Analizar las unidades de red.
`/QUARANTINE`	Analizar los archivos del depósito de copias de seguridad de Kaspersky Endpoint Security.
`/@:<file list.lst>`	Analizar los archivos y las carpetas indicados en una lista. Cada archivo de la lista debe estar en una fila diferente. Las rutas largas deben estar entre comillas. Las rutas cortas (en formato de MS-DOS) no necesitan las comillas. Por ejemplo: • `"C:\Program Files (x86)\Example Folder"` (ruta larga). • `C:\PROGRA~2\EXAMPL~1` (ruta corta).

Acción al detectar una amenaza	
`/i0`	**Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.
`/i1`	**Desinfectar; informar si falla la desinfección**. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección falla, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.
`/i2`	**Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo. Esta acción está seleccionada de forma predeterminada.
`/i3`	**Eliminar si falla la desinfección**. También eliminar los archivos compuestos (por ejemplo, los archivos de almacenamiento) cuando un archivo infectado no se pueda desinfectar o eliminar.
`/i4`	**Eliminar**. También eliminar los archivos compuestos (por ejemplo, los archivos de almacenamiento) cuando un archivo infectado no se pueda eliminar.

Tipos de archivos	
`/fe`	**Archivos analizados por extensión**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. El formato de archivo se determina en función de su extensión.
`/fi`	**Archivos analizados por formato**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.
`/fa`	**Todos los archivos**. Si se activa este parámetro, la aplicación comprueba todos los archivos sin excepción (todos los formatos y las extensiones). Esta es la configuración predeterminada.

Exclusiones del análisis	
`-e:a`	No analizar archivos RAR, ARJ, ZIP, CAB, LHA, JAR ni ICE.
`-e:<file mask>`	No analizar los archivos que coincidan con la máscara de archivos especificada. Por ejemplo: • La máscara `*.exe` comprende las rutas a todos los archivos de extensión exe. • La máscara `example*` comprende las rutas a todos los archivos de nombre EXAMPLE.
`-e:<seconds>`	No analizar los archivos que demoren más en analizarse que el límite de tiempo indicado (expresado en segundos).
`-es:<megabytes>`	No analizar los archivos que superen el límite de tamaño indicado (expresado en megabytes).

Guardar eventos en un modo de archivo de informe (solo para los perfiles de análisis, actualización y reversión)	
`/R:<report file>`	Guardar solo los eventos críticos en el archivo del informe.
`/RA:<report file>`	Guardar todos los eventos en el archivo del informe.

Tecnologías de análisis	
`/iChecker=on|off`	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).
`/iSwift=on|off`	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

Configuración avanzada	
`/C:<file with scan settings>`	Archivo con la configuración de la tarea de *Análisis antimalware*. Deberá crear este archivo manualmente y guardarlo en formato TXT. Puede incluir lo siguiente: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Ejemplo

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Actualización de las bases de datos y módulos de la aplicación

Ejecución de la tarea *Actualización de las bases de datos y módulos de la aplicación*.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

Sintaxis del comando

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Configuración de la tarea de actualización	
`local`	Inicio de la tarea de *Actualización de las bases de datos y módulos de la aplicación* que se creó automáticamente después de instalar la aplicación. Puede cambiar la configuración de la tarea de *Actualización de las bases de datos y módulos de la aplicación* en la interfaz de la aplicación local o en la consola de Kaspersky Security Center. Si esta opción no está configurada, Kaspersky Endpoint Security inicia la tarea de *Actualización de las bases de datos y módulos de la aplicación* con la configuración predeterminada o con la configuración especificada en el comando. Puede establecer la configuración de la tarea *Actualización de las bases de datos y módulos de la aplicación* de la siguiente manera: • `UPDATE` inicia la tarea *Actualización de las bases de datos y módulos de la aplicación* con la configuración predeterminada: el origen de actualizaciones son los servidores de actualización de Kaspersky, la cuenta es Sistema y otras opciones de configuración predeterminadas. • `UPDATE local` inicia la tarea *Actualización de las bases de datos y módulos de la aplicación* que se creó automáticamente después de la instalación (tarea predefinida). • `UPDATE <update settings>` inicia la tarea *Actualización de las bases de datos y módulos de la aplicación* con una configuración definida manualmente (ver a continuación).

Origen de actualizaciones	
`"<update source>"`	Dirección de un servidor HTTP/FTP o de una carpeta compartida con el paquete de actualización. No es posible especificar más de un origen. Si no se especifica el origen de actualizaciones, Kaspersky Endpoint Security utiliza la fuente predeterminada: los servidores de actualización de Kaspersky.

Guardar eventos en un modo de archivo de informe (solo para los perfiles de análisis, actualización y reversión)	
`/R:<report file>`	Guardar solo los eventos críticos en el archivo del informe.
`/RA:<report file>`	Guardar todos los eventos en el archivo del informe.

Configuración avanzada	
`/C:<file with update settings>`	Archivo con la configuración de la tarea de *Actualización de las bases de datos y módulos de la aplicación*. Deberá crear este archivo manualmente y guardarlo en formato TXT. Puede incluir lo siguiente: `["<update source>"] [/R[A]:<report file>]`.

Ejemplo

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Reversión de la última actualización

Revertir la última actualización de las bases de datos antivirus. Permite recuperar una versión anterior de las bases de datos y de los módulos de la aplicación; esto puede ser necesario, por ejemplo, cuando las bases de datos más recientes contienen una firma inválida que hace que Kaspersky Endpoint Security bloquee una aplicación segura.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

Sintaxis del comando

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Guardar eventos en un modo de archivo de informe (solo para los perfiles de análisis, actualización y reversión)	
`/R:<report file>`	Guardar solo los eventos críticos en el archivo del informe.
`/RA:<report file>`	Guardar todos los eventos en el archivo del informe.

Ejemplo

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Rastreo

Los archivos de seguimiento se almacenan en el equipo siempre que la aplicación esté en uso y se eliminan permanentemente cuando se quita la aplicación. Los archivos de seguimiento —exceptuados los del Agente de autenticación— se almacenan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. De manera predeterminada, la función está deshabilitada.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Nivel de seguimiento	
`<tracing level>`	Nivel de detalle del seguimiento. Valores disponibles: • `100` (crítico). Solo mensajes sobre errores graves. • `200` (alto). Mensajes sobre todos los errores, incluidos los errores graves. • `300` (diagnóstico). Mensajes sobre todos los errores, además de las advertencias. • `400` (importante). Todos los mensajes de error y de advertencia, así como otra información adicional. • `500` (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado). • `600` (bajo). Todos los mensajes.

Configuración avanzada	
`all`	Ejecutar un comando con los parámetros `file` y `mem`.
`file`	Guardar un archivo de seguimiento (sin límite de tamaño).
`rot`	Guardar los datos de seguimiento en un número de conjuntos de archivos de tamaño limitado. Cuando se alcance el tamaño máximo, los archivos más antiguos se sobrescribirán.
`mem`	Guardar datos de seguimiento en archivos de volcado.

Ejemplo

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Iniciar un perfil

Iniciar un perfil (por ejemplo, iniciar una actualización de las bases de datos o activar un componente de protección).

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com START <profile> [/R[A]:<report file>]
```

Perfil	
`<profile>`	Nombre de perfil. Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Puede ver la lista de perfiles disponibles ejecutando el comando `HELP START`.

Guardar eventos en un modo de archivo de informe (solo para los perfiles de análisis, actualización y reversión)	
`/R:<report file>`	Guardar solo los eventos críticos en el archivo del informe.
`/RA:<report file>`	Guardar todos los eventos en el archivo del informe.

Ejemplo

```
avp.com START Scan_Objects
```

STOP. Detener un perfil

Detener la ejecución del perfil (por ejemplo, detener un análisis de unidades extraíbles o desactivar un componente de protección).

Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe contar con los permisos **Desactivar componentes de protección** y **Desactivar componentes de control**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Perfil	
`<profile>`	Nombre de perfil. Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Puede ver la lista de perfiles disponibles ejecutando el comando `HELP STOP`.

Autenticación	
`/login=<user name> /password=<password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

STATUS. Estado del perfil

Mostrar información del estado de los perfiles de la aplicación (por ejemplo, `running` o `completed`). Puede ver la lista de perfiles disponibles mediante el comando `HELP STATUS`.

Kaspersky Endpoint Security también muestra el estado de los perfiles de servicio. Puede que necesite esta información si se comunica con el Soporte técnico de Kaspersky.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com STATUS [<profile>]
```

Si introduce el comando sin un perfil, Kaspersky Endpoint Security muestra el estado de todos los perfiles de la aplicación.

STATISTICS. Estadísticas sobre el funcionamiento de los perfiles

Mostrar estadísticas sobre alguno de los perfiles de la aplicación (por ejemplo, la duración de un análisis o la cantidad de amenazas detectadas). Puede ver la lista de perfiles disponibles mediante el comando `HELP STATISTICS`.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com STATISTICS <profile>
```

RESTORE. Restauración de archivos de Copia de seguridad

Restaurar un archivo almacenado en Copia de seguridad a su carpeta original. Si en la ruta especificada ya existe un archivo con el mismo nombre, la aplicación pedirá confirmación para reemplazarlo. El archivo restaurado se guarda con su nombre original.

> Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Restaurar desde copia de seguridad**.

Copias de seguridad almacena copias de seguridad de los archivos que se modificaron o eliminaron durante la desinfección. Una *copia de seguridad* es una copia del archivo creada antes de que el archivo se desinfectara o se eliminara. Las copias de seguridad de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. El usuario cuya cuenta se usó para instalar la Kaspersky Endpoint Security tiene derechos de acceso limitado a esta carpeta.

> Kaspersky Endpoint Security no ofrece la posibilidad de configurar permisos de acceso de usuario a copias de seguridad de los archivos.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Configuración avanzada	
`/REPLACE`	Si el archivo ya existe, sobrescribirlo.
`<file name>`	Nombre del archivo que se va a restaurar.

Autenticación	
`/login=<user name> /password=<password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Exportar ajustes de la aplicación

Exportar ajustes de configuración de Kaspersky Endpoint Security a un archivo. Si el comando contiene solo el nombre del archivo al que desea exportar la configuración, la aplicación emplaza el archivo de la siguiente manera:

- Si la ruta a avp.com se añade a la variable del sistema %PATH%, la aplicación sitúa el archivo en la carpeta `C:\Windows\SysWOW64`.
- Si ejecuta el comando desde la carpeta de instalación de la aplicación, la exportación fallará porque la autoprotección de la aplicación bloquea la creación de un nuevo archivo en la carpeta de la aplicación. Para exportar la configuración de la aplicación a un archivo, introduzca la ruta del archivo.

Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Exportar configuración**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Perfil	
`<profile>`	Nombre de perfil. Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Puede ver la lista de perfiles disponibles ejecutando el comando `HELP EXPORT`.

Archivo para la exportación	
`<file name>`	Nombre del archivo en el que se guardarán los ajustes de configuración exportados. También puede introducir la ruta del archivo. Los ajustes de Kaspersky Endpoint Security pueden exportarse a un archivo de configuración DAT o CFG, a un archivo de texto TXT o a un documento XML.

Autenticación	
`/login=<user name> /password= <password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importar configuración de la aplicación

Importación de la configuración de Kaspersky Endpoint Security desde un archivo creado con el comando `EXPORT`.

Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Configurar parámetros de la aplicación**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Archivo para importar	
`<file name>`	Nombre del archivo de configuración que se importará. Los ajustes de configuración de Kaspersky Endpoint Security pueden importarse desde un archivo de configuración DAT o CFG, un archivo de texto TXT o un documento XML.

Autenticación	
`/login=<user name> /password= <password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Aplicar un archivo clave.

Activar Kaspersky Endpoint Security con un archivo clave. Si la aplicación ya está activada, la clave se añade como clave de reserva.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

Sintaxis del comando

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Archivo clave	
`<file name>`	Nombre del archivo clave.

Autenticación	
`/login=<user name> /password= <password>`	Credenciales de una cuenta de usuario. Estos datos solo se necesitan si la protección con contraseña está activada.

Ejemplo

```
avp.com ADDKEY file.key
```

LICENSE. Administración de licencias

Gestionar las claves de licencia de Kaspersky Endpoint Security o con las claves de Kaspersky Endpoint Security, EDR Optimum o EDR Expert (complemento de Kaspersky Endpoint Detection and Response).

Para ejecutar este comando y eliminar una clave de licencia, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Eliminar clave**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

Sintaxis del comando

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Operación	
`/ADD <file name>`	Activar Kaspersky Endpoint Security con un archivo clave. Si la aplicación ya está activada, la clave se añade como clave de reserva.
`/ADD <activation code>`	Activar Kaspersky Endpoint Security con un código de activación. Si la aplicación ya está activada, la clave se añade como clave de reserva.
`/REFRESH`	Actualice el estado de la licencia de Kaspersky Endpoint Security. De este modo, la aplicación recibe información actualizada sobre el estado de la licencia de los servidores de activación de Kaspersky.
`/REFRESH <license ID>`	Actualizar el estado de las licencias mediante el ID de licencia. Con este comando, puede actualizar el estado del complemento de EDR, el complemento de MDR, el complemento de KUMA u otras licencias. Puede obtener el ID de licencia desde el certificado de licencia. De este modo, la aplicación recibe información actualizada sobre el estado de la licencia de los servidores de activación de Kaspersky.
`/CHECK`	Obtener información de la licencia Kaspersky Endpoint Security muestra información sobre todas las claves de licencia añadidas, incluidas las claves de reserva, el complemento EDR, el complemento MDR, las claves del complemento KUMA y otras claves. Kaspersky Endpoint Security muestra la siguiente información de licencia: • nombre de la licencia; • identificador de la licencia; • dirección del Servidor de protección (SVM) al que está conectada la máquina virtual en la que está instalada la aplicación en modo Light Agent; • tipo de licencia: de prueba, comercial, beta, suscripción; • fecha y hora de activación de la aplicación; • fecha y hora de vencimiento de la licencia; • número de días antes hasta el vencimiento de la licencia;
`/CHECK <license ID>`	Obtener información de licencia por ID. Puede utilizar este comando para obtener información sobre la licencia. Puede obtener el ID de licencia desde el certificado de licencia.
`/DEL /login=<user name> /password= <password>`	Elimine la clave de licencia de la aplicación. La clave de licencia de reserva también se quitará.
`/DEL <license ID> /login=<user name> /password=<password>`	Eliminar la clave con el ID de licencia. Con este comando, puede eliminar una clave del complemento de EDR, el complemento de MDR, el complemento de KUMA u otras licencias. Puede obtener el ID de licencia desde el certificado de licencia.

Autenticación	
`/login=<user name> /password= <password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Ejemplo

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Compra de una licencia

Abrir el sitio web de Kaspersky para comprar o renovar una licencia.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

PBATESTRESET. Restablecer los resultados de la comprobación de disco antes de cifrar el disco

Restablecer los resultados de la comprobación de compatibilidad para el Cifrado de disco completo (FDE), incluidas las tecnologías Cifrado de disco de Kaspersky y Cifrado de unidad BitLocker.

Antes de aplicar el cifrado de disco completo, la aplicación realiza una serie de pruebas para verificar si el equipo puede cifrarse. Si el equipo no es compatible con el Cifrado de disco completo (FDE), Kaspersky Endpoint Security deja constancia de la incompatibilidad. Si se intenta realizar una nueva operación de cifrado, la aplicación omite la verificación y simplemente advierte que el cifrado no puede aplicarse. Esto significa que, ante un cambio en la configuración de hardware del equipo, los resultados de la verificación deben descartarse, y se debe volver a comprobar si el disco duro del equipo es compatible con las tecnologías Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

EXIT. Salir de la aplicación

Salir de Kaspersky Endpoint Security. La aplicación se descargará de la RAM del equipo.

Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Salir de la aplicación**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Desactivar una directiva

Desactivar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse.

> Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Desactivar la directiva de Kaspersky Security Center**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Activar una directiva

Activar una directiva de Kaspersky Security Center en el equipo. Los parámetros de la aplicación tomarán los valores que indique la directiva.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

DISABLE. Desactivar la protección

Desactivar el componente Protección frente a amenazas en archivos si la licencia de Kaspersky Endpoint Security ha caducado. No podrá ejecutar este comando si la aplicación no se ha activado en el equipo o la licencia aún es válida.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

SPYWARE. Detección de spyware

Administrar la detección de spyware. De manera predeterminada, la detección de spyware está activada.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com SPYWARE on|off
```

KSN. Cambiar entre KSN/KPSN

Selección de una solución de Kaspersky para determinar la reputación de archivos o sitios web. Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura para trabajar con las bases de datos de reputación de Kaspersky:

- *Kaspersky Security Network (KSN).* Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky y, a su vez, envían a Kaspersky información sobre los objetos que se detectan en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos.

- *Kaspersky Private Security Network (KPSN)* es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos. KPSN se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:

  - porque las estaciones de trabajo locales no tienen acceso a Internet;

  - porque, por motivos legales o debido a las directivas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

Sintaxis del comando

```
avp.com KSN /global | /private <file name>
```

Archivo de configuración de Kaspersky Security Network	
`<file name>`	Nombre del archivo de configuración que contiene la configuración de Kaspersky Private Security Network. Este archivo tiene la extensión PKCS7 o PEM.

Ejemplo

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Ejemplo

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Desactivar la protección de conexión del servidor.

Ejecutar la tarea *Protección de la conexión al servidor de administración*, que elimina la contraseña de la conexión del equipo al servidor de administración. De esta forma, la tarea desactiva la protección de la conexión del servidor de administración.

Para ejecutar este comando, es necesario que la protección con contraseña esté activada.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Contraseña	
`/password=<password>`	La contraseña de la cuenta de usuario KLAdmin o la contraseña de la tarea *Protección de la conexión al servidor de administración*. Si no se especifica el parámetro, Kaspersky Endpoint Security le pide que introduzca una contraseña en la siguiente línea.

Comandos KESCLI

Los comandos KESCLI le permiten recibir información sobre el estado de la protección del equipo con el componente OPSWAT y realizar tareas estándar, como *Análisis antimalware* y *Actualización de las bases de datos y módulos de la aplicación*.

Puede consultar la lista de comandos KESCLI mediante el comando `kescli --help` o el comando abreviado `kescli -h`.

Para administrar Kaspersky Endpoint Security a través de la línea de comandos:

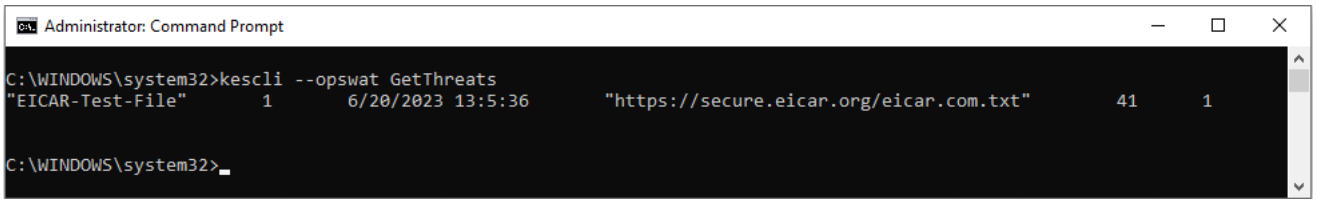
1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

   Puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% durante la instalación de la aplicación.

3. Utilice la siguiente plantilla para ejecutar el comando:

```
kescli <comando> [opciones]
```

Kaspersky Endpoint Security ejecutará el comando especificado (consulte la siguiente imagen).



Administración de la aplicación desde la línea de comandos

Scan. Análisis antimalware

Ejecución de la tarea *Análisis antimalware* (Análisis completo).

Para ejecutar la tarea, el administrador debe Permitir el uso de tareas locales en la directiva.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Puede verificar el estado de finalización de la tarea de *Análisis antimalware* con el comando `GetScanState` y consultar la fecha y la hora en la que se completó por última vez con el comando `GetLastScanTime`.

Cobertura del análisis	
`<scan scope>`	Lista de archivos y carpetas, separados con `;` (punto y coma). Por ejemplo, `"C:\Program Files (x86)\Example Folder"`.

Acción al detectar una amenaza	
`0`	**Informar**. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.
`1`	**Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo. Esta acción está seleccionada de forma predeterminada.

Ejemplo

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Estado de finalización del análisis

Mostrar información sobre el estado de finalización de la tarea *Análisis antimalware* (*Análisis completo*):

- `1`: el análisis está en proceso.
- `0`: no se está ejecutando el análisis.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetScanState
```

GetLastScanTime. Especificación del tiempo para completar el análisis

Mostrar información sobre la fecha y hora de la última instancia en la que se completó la tarea *Análisis antimalware* (*Análisis completo*).

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetLastScanTime
```

GetThreats. Obtención de datos sobre amenazas detectadas

Mostrar una lista de amenazas detectadas (*Informe de amenazas*). En este informe, encontrará información sobre amenazas y la actividad de virus durante los últimos 30 días previos a la creación del informe.

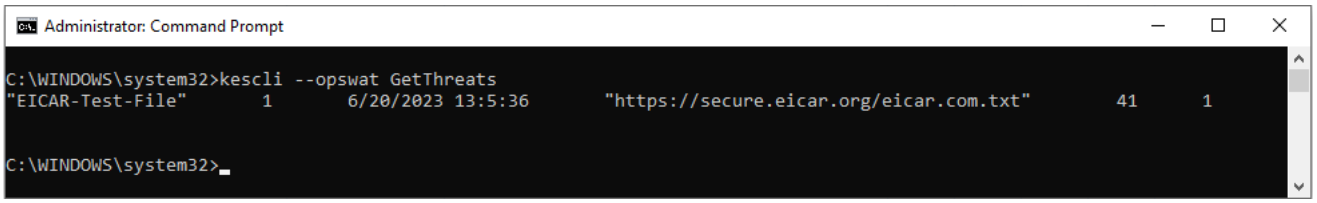
Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetThreats
```

Al ejecutar este comando, Kaspersky Endpoint Security enviará una respuesta con el siguiente formato:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



Administración de la aplicación desde la línea de comandos

Tipo de objeto	
0	Desconocido (Unknown).
1	Virus (Virware).
2	Programas troyanos (Trojware).
3	Programas maliciosos (Malware).
4	Programas de anuncios (Adware).
5	Programas de marcado automático (Pornware).
6	Aplicaciones que puede utilizar un ciberdelincuente para hacerle daño al equipo o los datos del usuario (Riskware).
7	Objetos comprimidos cuyo método de compresión puede usarse para proteger código malicioso (Packed).
20	Objetos desconocidos (Xfiles).
21	Aplicaciones conocidas (Software).
22	Archivos ocultos (Hidden).
23	Aplicaciones que solicitan atención (Pupware).
24	Comportamiento extraño (Anomaly).
30	Sin determinar (Undetect).
40	Banners de anuncios (Banner).
50	Ataque de red (Attack).
51	Acceso a registros (Registry).
52	Actividad sospechosa (Suspicion).
60	Vulnerabilidades (Vulnerability).
70	Phishing (Phishing).
80	Archivo adjunto no deseado en correos electrónicos (Attachment).
90	Software malicioso detectado por Kaspersky Security Network (Urgent).
100	Enlace desconocido (Suspic URL).
110	Otro software malicioso (Behavioral).

Acción al detectar una amenaza	
0	Desconocido (unknown).
1	Se resolvió la amenaza (ok).
2	Se infectó el objeto infectado y no se lo desinfectó (infected).
5	No se desinfectó el objeto en carpeta comprimida (archive).
9	Se desinfectó el objeto (disinfected).
10	No se desinfectó el objeto (not disinfected).

11	Se eliminó el objeto (`deleted`).
13	Se creó una copia de seguridad del objeto (`backupped`).
15	Se movió el objeto a Copia de seguridad (`quarantined`).
23	Se eliminó el objeto al reiniciar el equipo (`delete on reboot`).
25	Se desinfectó el objeto al reiniciar el equipo (`disinfect on reboot`).
29	Se movió el objeto a Copia de seguridad por el usuario (`added by user`).
30	Se añadió el objeto a las exclusiones (`added to exclude`).
31	Se movió el objeto a Copia de seguridad al reiniciar el equipo (`quarantine on reboot`).
36	Falso positivo (`false alarm`).
38	Se finalizó el proceso (`terminated`).
40	No se detectó el objeto (`not found`).
41	No se ha podido resolver la amenaza (`untreatable`).
42	Se restauró el objeto (`rolled back`).
43	Se creó el objeto a partir de la actividad de amenazas (`produced by threat`).
44	Se restauró el objeto al reiniciar el equipo (`roll back on reboot`).
0xffffffff	No se procesó el objeto (`discarded`).

Nivel de peligro de la amenaza	
`0`	Desconocido
`1`	Máximo
`2`	Análisis medio
`4`	Mínimo
`8`	Información (menor que *mínimo*)

UpdateDefinitions. Actualización de las bases de datos y módulos de la aplicación

Ejecución de la tarea *Actualización de las bases de datos y módulos de la aplicación*. Kaspersky Endpoint Security emplea una fuente predeterminada: los servidores de actualización de Kaspersky.

Para ejecutar la tarea, el administrador debe Permitir el uso de tareas locales en la directiva.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Este comando no se puede ejecutar si la aplicación está instalada en Modo de Light Agent.

Sintaxis del comando

```
kescli --opswat UpdateDefinitions
```

Puede consultar la fecha y hora de lanzamiento de las bases de datos de antivirus actuales con el comando `GetDefinitionsetState`.

GetDefinitionState. Determinar la fecha y hora de la última actualización de las bases de datos

Mostrar información sobre la fecha y hora de la última actualización de las bases de datos antivirus en uso.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetDefinitionState
```

EnableRTP. Activación de la protección

Activar los componentes de protección de Kaspersky Endpoint Security en el equipo: Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red y Prevención de intrusiones en el host.

> Para habilitar los componentes de protección, el administrador debe asegurarse de que la configuración de la directiva relevante se pueda modificar (los atributos están abiertos).

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat EnableRTP
```

Como resultado, los componentes de protección están habilitados incluso si ha prohibido la modificación de la configuración de la aplicación con Protección con contraseña.

Puede verificar el estado de funcionamiento del componente Protección frente a amenazas en archivos con el comando `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Estado de la Protección frente a amenazas en archivos

Mostrar información sobre el estado del componente Protección frente a amenazas en archivos:

- `1`: el componente está activado.
- `0`: el componente está desactivado.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Estado de cifrado del disco

Mostrar información sobre el estado de cifrado del disco:

- `1` significa que el disco está protegido por tecnología de cifrado de discos Kaspersky o BitLocker.
- `0` significa que el disco no está cifrado.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetEncryptionState
```

Version. Identificación de la versión de la aplicación

Mostrar la versión de Kaspersky Endpoint Security para Windows.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --Version
```

También puede emplear el comando abreviado `-v`.

Comandos de administración de Detection and Response

Puede utilizar la línea de comandos para administrar la funcionalidad integrada de las soluciones de Detection and Response (por ejemplo, Kaspersky Sandbox o Kaspersky Endpoint Detection and Response Optimum). Puede administrar las soluciones de Detection and Response si la administración mediante la consola de Kaspersky Security Center no es posible. Para ver la lista de comandos de administración disponibles, utilice el comando `HELP`. Para conocer la sintaxis de un comando específico, escriba `HELP <command>`.

Para administrar las funciones integradas de las soluciones de Detection and Response mediante la línea de comando, haga lo siguiente:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Utilice la siguiente plantilla para ejecutar el comando:

```
avp.com <command> [options]
```

Kaspersky Endpoint Security ejecutará el comando especificado.

SANDBOX. Administrar Sandbox

Comandos para administrar el componente Sandbox:

- Active o desactive el componente Sandbox.

  Los componentes Sandbox proporcionan interacción con la solución Kaspersky Sandbox y el componente KATA Sandbox, que es parte de Kaspersky Anti Targeted Attack Platform.

- Configure el componente Sandbox:

  - Conecte el equipo a los servidores de Sandbox.

    Los servidores utilizan imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows para ejecutar objetos que se deben analizar. Puede introducir una dirección IP (IPv4 o IPv6) o un nombre de dominio completo. Para obtener detalles sobre la implementación de imágenes virtuales y la configuración de los servidores de Sandbox, consulte la Ayuda de Kaspersky Sandbox y la Ayuda de Kaspersky Anti Targeted Attack Platform.

  - Configure el tiempo de espera de la conexión para el servidor.

    Tiempo de espera de conexión para el servidor de Sandbox (para Kaspersky Sandbox) o el servidor de Central Node (para KATA). Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de espera de conexión del servidor si su velocidad de conexión es baja o si la conexión es inestable. El tiempo de espera recomendado para las solicitudes es de 0,5 segundos o menos.

  - Configure una conexión confiable entre el equipo y los servidores.

    Para configurar una conexión de confianza con el servidor de Sandbox (para Kaspersky Sandbox) o el servidor de Central Node (para KATA), debe preparar un certificado TLS. A continuación, debe añadir el certificado al equipo mediante el uso de una directiva. También debe añadir el certificado al servidor de Sandbox (para Kaspersky Sandbox) o al servidor de Central Node (para KATA).

  - Configuración del modo de integración.

Debe seleccionar una solución de la que Sandbox forme parte, es decir, Kaspersky Sandbox o KATA Sandbox. *Kaspersky Sandbox* es una solución independiente de Detection and Response de Kaspersky. *KATA Sandbox* es un componente de la solución Kaspersky Anti Targeted Attack Platform. Cuando se integra con KATA Sandbox, el componente puede funcionar en los siguientes modos:

- **Manual**. El usuario envía manualmente el archivo para su análisis desde el menú contextual (**Enviar a Sandbox**).
- **Automático**. La aplicación detecta objetos automáticamente y los envía a Sandbox para su análisis.
- **Combinado**.

- Muestra la configuración actual del componente.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Operación	
`stop`	Desactive el componente Sandbox.
`start`	Active el componente Sandbox.

`set`	Configure el componente Sandbox. Los parámetros que puede configurar son los siguientes:
	• Añada servidores Sandbox (`--servers`)
	• Añada un certificado TLS (`--pinned-certificate`)
	• Añadir un contenedor de cifrado (`--client-certificate`)
	• Especifique una contraseña para el contenedor criptográfico (`--client-certificate-password`);
	• Configure el tiempo de espera de la conexión del servidor (`--timeout`)
	• Seleccione un modo de integración (`--mode`):
	  • `KSB`: integración con Kaspersky Sandbox;
	  • `KATAManual`: integración manual con KATA Sandbox;
	  • `KATAAuto`: integración automática con KATA Sandbox;
	  • `KATAFull`: integración combinada con KATA Sandbox.

`show`	Muestra la configuración actual del componente. Obtiene la siguiente respuesta:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autenticación	
`/login=<user name> /password=<password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION. Administración de la prevención de ejecución

Desactivar el componente de prevención de ejecución o mostrar la configuración actual del componente, incluida la lista de reglas de prevención de ejecución.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com prevention disable
```

```
avp.com prevention /show
```

Cuando ejecute el comando `prevention /show`, obtendrá la siguiente respuesta:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Valores de retorno de comando:

- `-1` significa que el comando no es compatible con la versión de la aplicación que está instalada en el equipo.
- `0` significa que el comando se ejecutó correctamente.
- `1` significa que no se pasó un argumento obligatorio al comando.
- `2` significa que ocurrió un error general.

- 4 significa que hubo un error de sintaxis.
- 9: operación incorrecta (por ejemplo, un intento de desactivar el componente cuando ya está desactivado).

ISOLATION. Administrar el aislamiento de red

Desactivar Aislamiento de red en el equipo o mostrar la configuración actual del componente. La configuración del componente también incluye una lista de conexiones de red añadidas a exclusiones.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Como resultado de ejecutar el comando `stat`, recibe la siguiente respuesta: `Network isolation on|off`.

RESTORE. Restauración de archivos de la cuarentena

Restaurar un archivo almacenado en Cuarentena a su carpeta de origen. *Cuarentena* es un almacenamiento local especial en el equipo. El usuario puede poner en cuarentena archivos que considere peligrosos para el equipo. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la Cuarentena solo cuando se integra con soluciones de Kaspersky Detection and Response. En otros casos, Kaspersky Endpoint Security coloca el archivo relevante en Copia de seguridad. Para obtener información sobre cómo administrar la cuarentena como parte de las soluciones, consulte la Ayuda de Kaspersky Sandbox, la Ayuda de Kaspersky Endpoint Detection and Response Optimum, la Ayuda de Kaspersky Endpoint Detection and Response Expert, la Ayuda de Kaspersky Anti Targeted Attack Platform y la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises).

Para ejecutar este comando, es necesario que la protección con contraseña esté activada. El usuario debe tener el permiso **Restaurar desde copia de seguridad**.

El objeto se pone en cuarentena en la cuenta del sistema (SYSTEM).

Restaurar archivos de la Cuarentena implica las siguientes consideraciones especiales:

- Si la carpeta de destino se ha eliminado o el usuario no tiene derechos de acceso a esa carpeta, la aplicación sitúa el archivo en la carpeta `%DataRoot%\QB\Restored`. Luego, debe mover el archivo manualmente a la carpeta de destino.
- La aplicación trata el nombre del archivo que se está restaurando como sensible a mayúsculas y minúsculas. Si no respeta las mayúsculas y minúsculas al introducir el nombre del archivo, la aplicación no lo restaura.

- Si la carpeta de destino ya tiene un archivo con el mismo nombre, la aplicación cancela la restauración del archivo.
- Si está utilizando la solución KATA (EDR), la aplicación guarda una copia del archivo en Cuarentena después de restaurar el archivo. Puede vaciar manualmente la Cuarentena. Para las soluciones EDR Optimum y EDR Expert, la aplicación elimina el archivo después de la restauración.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Configuración avanzada	
`/REPLACE`	Si el archivo ya existe, sobrescribirlo.
`<file name>`	Nombre del archivo que se va a restaurar.

Autenticación	
`/login=<user name> /password=<password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Valores de retorno de comando:

- `-1` significa que el comando no es compatible con la versión de la aplicación que está instalada en el equipo.
- `0` significa que el comando se ejecutó correctamente.
- `1` significa que no se pasó un argumento obligatorio al comando.
- `2` significa que ocurrió un error general.
- `4` significa que hubo un error de sintaxis.

IOCSCAN. Analizar en busca de indicadores de compromiso (IOC)

Ejecución de la tarea *Análisis de IOC*. Un *Indicador de compromiso (IOC)* es un conjunto de datos sobre un objeto o actividad que indica el acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. La tarea de *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta a la amenaza.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

El análisis de IOC se interrumpe después de 128 coincidencias con los indicadores de compromiso descritos en los archivos de IOC. Esto es necesario para limitar la cantidad de entradas del informe de la tarea Análisis de IOC, y facilitar así el análisis y la protección del informe de desbordamiento debido a los indicadores de compromiso formulados de manera imprecisa que pueden generar una gran cantidad de coincidencias.

Sintaxis del comando

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

Archivos IOC	
`<full path to the IOC file>`	Ruta completa al archivo de IOC que desea utilizar para el análisis. Puede especificar varios archivos IOC separados por espacios. La ruta completa al archivo de IOC se debe introducir sin el argumento `/path`. Por ejemplo, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Ruta a la carpeta con archivos IOC que desea usar para el análisis. Los *archivos IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos IOC deben cumplir con el estándar OpenIOC. Por ejemplo, `C:\Users\Admin\Desktop\IOC`

Tipo de datos para análisis de IOC	
`/process=on|off`	Analice los datos del proceso al realizar el análisis de IOC (término ProcessItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los procesos que se ejecutan en el equipo al realizar el análisis. Si el archivo de IOC contiene términos de IOC del documento de IOC ProcessItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del proceso solo si el documento de IOC ProcessItem se describe en el archivo de IOC que se proporciona para el análisis.
`/hint=<full path to the executable file of the process|full path to the file>`	Analice los datos del archivo al realizar el análisis de IOC (términos ProcessItem y FileItem). Puede seleccionar el archivo de una de las siguientes formas: • `<full path to the executable file of the process>` – término ProcessItem; • `<full path to the file>` – término FileItem.
`/registry=on|off`	Analice los datos del registro de Windows al realizar un análisis de IOC (término RegistryItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza el registro de Windows. Si el archivo de IOC contiene términos del documento de IOC RegistryItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza el registro de Windows solo si el documento de IOC de RegistryItem se describe en el archivo de IOC que se proporciona para el análisis. Para el tipo de datos RegistryItem, Kaspersky Endpoint Security analiza un grupo de claves de registro.
`/dnsentry=on|off`	Analice los datos sobre los registros en la caché de DNS local al realizar el análisis de IOC (término DnsEntryItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza la caché de DNS local. Si el archivo de IOC contiene términos del documento de IOC DnsEntryItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza la caché de DNS local solo si el documento de IOC DnsEntryItem se describe en el archivo de IOC que se proporciona para el análisis.

`/arpentry=on|off`	Analice los datos sobre los registros en la tabla ARP al realizar el análisis de IOC (término ArpEntryItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza la tabla ARP. Si el archivo de IOC contiene términos del documento de IOC ArpEntryItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza la tabla ARP solo si el documento de IOC de ArpEntryItem se describe en el archivo de IOC que se proporciona para el análisis.
`/ports=on|off`	Analice los datos sobre los puertos abiertos para escuchar al realizar el análisis de IOC (término PortItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza la tabla de conexiones activas en el dispositivo. Si el archivo de IOC contiene términos del documento de IOC PortItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza la tabla de conexiones activas solo si el documento de IOC PortItem se describe en el archivo de IOC que se proporciona para el análisis.
`/services=on|off`	Analice los datos sobre los servicios instalados en el dispositivo al realizar el análisis de IOC (término ServiceItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los datos sobre los servicios instalados en el dispositivo. Si el archivo de IOC contiene términos del documento de IOC ServiceItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del servicio solo si el documento de IOC de ServiceItem se describe en el archivo de IOC que se proporciona para el análisis.
`/system=on|off`	Analice los datos del entorno al realizar el análisis de IOC (término SystemInfoItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los datos del entorno. Si el archivo de IOC contiene términos del documento de IOC SystemInfoItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del entorno solo si el documento de IOC SystemInfoItem se describe en el archivo de IOC que se proporciona para el análisis.
`/users=on|off`	Analice los datos sobre los usuarios al realizar el análisis de IOC (término UserItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los datos sobre los usuarios creados en el sistema. Si el archivo de IOC contiene términos del documento de IOC UserItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos sobre los usuarios creados en el sistema solo si el documento de IOC de UserItem se describe en el archivo de IOC que se proporciona para el análisis.
`/volumes=on|off`	Analice datos sobre volúmenes al realizar el análisis de IOC (término VolumeItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los datos sobre los volúmenes del dispositivo. Si el archivo de IOC contiene términos del documento de IOC VolumeItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del volumen solo si el documento de IOC de VolumeItem se describe en el archivo de IOC que se proporciona para el análisis.
`/eventlog=on|off`	Analice los datos sobre los registros en el registro de eventos de Windows al realizar el análisis de IOC (término EventLogItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los registros del registro de eventos de Windows. Si el archivo de IOC contiene términos del documento de IOC EventLogItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza el registro de eventos de Windows si el documento de IOC EventLogItem se describe en el archivo de IOC que se proporciona para el análisis. Para el término de IOC EventLogItem\source, use el valor **Nombre del proveedor** del esquema XML del evento.

`/datetime=<event publication date>`	Tenga en cuenta la fecha en la que se publicó el evento en el registro de eventos de Windows al determinar la cobertura de análisis de IOC para el documento de IOC correspondiente. Al realizar un análisis de IOC, Kaspersky Endpoint Security analiza las entradas del registro de eventos de Windows publicadas durante el período desde la fecha y hora especificadas hasta el momento en que se ejecuta la tarea. Kaspersky Endpoint Security permite especificar la fecha de publicación del evento como valor del argumento. El análisis se realiza solo para los eventos publicados en el registro de eventos de Windows después de la fecha especificada y antes de que se ejecute el análisis. Si no se especifica el argumento, Kaspersky Endpoint Security analiza los eventos con cualquier fecha de publicación. La configuración `TaskSettings::BaseSettings::EventLogItem::datetime` no se puede editar. La configuración se utiliza solo si el documento de IOC EventLogItem se describe en el archivo de IOC proporcionado para el análisis.
`/channel=<list of channels>`	Lista de nombres de canales (registros) para los que desea realizar un análisis de IOC. Si se especifica el argumento, Kaspersky Endpoint Security analiza los registros publicados en los registros especificados. El documento de IOC debe tener descrito el término EventLogItem. El nombre del registro se especifica como una cadena de acuerdo con el nombre del registro (canal) especificado en las propiedades del registro (el parámetro de Full Name) o en las propiedades del evento (el parámetro `<Channel></Channel>` en el esquema xml del evento). Puede especificar varios canales separados por espacios. Si no se especifica el argumento, Kaspersky Endpoint Security analiza los registros en busca de canales `Application`, `System`, `Security`.
`/files=on|off`	Analice los datos del archivo al realizar el análisis de IOC (término FileItem). Si el valor del argumento es `off`, Kaspersky Endpoint Security no analiza los datos del archivo. Si el archivo de IOC contiene términos del documento de IOC FileItem, estos se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del archivo solo si el documento de IOC de FileItem se describe en el archivo de IOC que se proporciona para el análisis.
`/drives=<all|system|critical|custom>`	Establezca la cobertura de análisis de IOC al analizar los datos para el documento de IOC de FileItem. Puede establecer los siguientes valores para la cobertura del análisis: • `<all>` para todas las coberturas de archivo disponibles. • `<system>` para archivos en carpetas donde está instalado el sistema operativo. • `<critical>` para archivos temporales en carpetas de usuario y del sistema. • `<custom>` para archivos en alcances definidos por el usuario (`/scope=<list of folders to scan>`). Si no se especifica el argumento, el análisis se realiza para áreas críticas.
`/excludes=<list of exclusions>`	Establezca la cobertura de la exclusión al analizar los datos del documento de IOC de FileItem. Puede especificar varias rutas separadas por espacios.
`/scope=<list of folders to scan>`	Alcance del análisis de IOC definido por el usuario al analizar los datos para el documento de IOC de FileItem (`/drives=custom`). Puede especificar varias rutas separadas por espacios.
`/retro /<number of days>`	*Análisis de IOC retrospectivo* es un modo de la tarea *Análisis de IOC* en la que Kaspersky Endpoint Security analiza en busca de indicadores de compromiso utilizando datos durante un período de tiempo determinado. Este modo está diseñado para buscar indicadores de compromiso mediante la telemetría del equipo protegido, como la actividad de la red, los procesos, los archivos y otra telemetría. Puede establecer un período de tiempo de 1 a 14 días. De forma predeterminada, la aplicación analiza en busca de indicadores de compromiso durante un día.
`/network=on|off`	Análisis de datos de red (la duración de NetworkItem).
`/url=on|off`	Análisis de datos en registros del navegador (la duración de UrlHistoryItem). El análisis de IOC retrospectivo analiza los registros de los siguientes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versión 79 o posterior).
`/email`	Análisis de objetos de correo (la duración de EmailItem).
`/route`	Análisis de tablas de enrutamiento y reenvío (la duración de RouteEntryItem).

Valores de retorno de comando:

- `-1` significa que el comando no es compatible con la versión de la aplicación que está instalada en el equipo.
- `0` significa que el comando se ejecutó correctamente.

- 1 significa que no se pasó un argumento obligatorio al comando.
- 2 significa que ocurrió un error general.
- 4 significa que hubo un error de sintaxis.

Si el comando se ejecutó correctamente (valor devuelto `0`) y se detectaron indicadores de compromiso en el camino, Kaspersky Endpoint Security envía la siguiente información del resultado de la tarea a la línea de comandos:

`Uuid`	Id. del archivo de IOC desde el encabezado de la estructura del archivo de IOC (la etiqueta `<ioc id="">`)
`Name`	Descripción del archivo de IOC desde el encabezado de la estructura del archivo de IOC (la etiqueta `<description></description>`)
`Matched Indicator Items`	Lista de id. de todos los indicadores coincidentes.
`Matched objects`	Datos para cada documento de IOC para el que hubo una coincidencia.

MDRLICENSE. Activación MDR

Añadir el archivo de configuración BLOB para activar Managed Detection and Response. El archivo BLOB contiene el ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra dentro del archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener información detallada sobre un archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

Se requieren privilegios de administrador para realizar operaciones con un archivo BLOB. La configuración de Managed Detection and Response en la directiva también debe estar disponible para su edición ( ).

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Operación	
`/ADD <file name>`	Aplique el archivo de configuración BLOB para la integración con Kaspersky Managed Detection and Response (formato de archivo P7). Puede aplicar solo un archivo BLOB. Si ya se añadió un archivo BLOB al equipo, se reemplazará el archivo.
`/DEL`	Elimina el archivo de configuración BLOB.

Autenticación	
`/login=<user name> /password= <password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Ejemplo

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integración de EDR (KATA)

Comandos para administrar el componente Endpoint Detection and Response (KATA):

- Activar o desactivar el componente EDR (KATA).

  El componente EDR (KATA) proporciona interoperabilidad con la solución Kaspersky Anti Targeted Attack Platform.

- Configurar la conexión a los servidores de Kaspersky Anti Targeted Attack Platform.

- Muestra la configuración actual del componente.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Operación	
`stop`	Desactive el componente EDR (KATA).
`start`	Active el componente EDR (KATA).
`set`	Configure el componente EDR (KATA). Los parámetros que puede configurar son los siguientes: • Añadir servidores de Central Node (`servers=<server address>:<port>`) • Añada un certificado TLS (`server-certificate=<path to the TLS certificate>`) • Configure el tiempo de espera de la conexión del servidor de Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Establezca el período de sincronización con el servidor de Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Muestra la configuración actual del componente.

EDRExpertOnPrem. Integración de EDR Expert (on-premises)

Comandos para administrar el agente integrado y configurar la integración de Kaspersky Endpoint Detection and Response Expert (on-premises):

- Habilitar o deshabilitar el agente integrado de EDR Expert (on-premises).
- Configurar los parámetros de conexión de los servidores de EDR Expert (on-premises).
- Mostrar la configuración actual del agente integrado.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Operación	Descripción
`stop`	Desactive el agente integrado de EDR Expert (on-premises).
`start`	Habilite el agente integrado de EDR Expert (on-premises).

`set`	Configure el agente integrado de EDR Expert (on-premises).
	Puede configurar los siguientes ajustes de conexión para los *servidores de respuesta*:
	• `servers=<server address>:<port>`. Dirección del servidor de respuesta (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Utilice un contenedor criptográfico para la autenticación mutua. Un *contenedor criptográfico* es un archivo PFX que contiene un certificado y una clave privada en formato PKCS#12. Para habilitar este tipo de autenticación, debe crear un contenedor criptográfico en una autoridad de certificación externa.
	• `timeout=<server connection timeout (s)>`. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente.
	• `sync-period=<server synchronization period (min)>`. Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security recibe tareas de respuesta ante amenazas y envía los resultados de la tarea.
	Puede configurar los siguientes ajustes de conexión para los *servidores de recopilación de telemetría*:
	• `telemetry-servers=<server address:port>`. Dirección del servidor de recopilación de telemetría (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. Utilice un contenedor criptográfico para la autenticación mutua. Un *contenedor criptográfico* es un archivo PFX que contiene un certificado y una clave privada en formato PKCS#12. Para habilitar este tipo de autenticación, debe crear un contenedor criptográfico en una autoridad de certificación externa.
	• `telemetry-timeout=<server connection timeout (s)>`. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente.
	• `events-send-period=<seconds>`. Retraso máximo al enviar eventos. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.
	• `events-limit=<0|1>`. Limite el número de solicitudes. Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos.
	• `events-per-hour=<number of events>`. Número máximo de eventos por hora. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60.000 eventos por hora.
	• `max-packet-length=<number of packets>`. Longitud máxima del paquete. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos.
	• `telemetry-only-tagged-events=<0|1>`. Envío de telemetría solo con IOA. *Indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que puede indicar un ataque dirigido. La aplicación compara el comportamiento en curso en el sistema con estas reglas y registra los eventos que son indicativos de un ataque dirigido. La aplicación utiliza la tecnología de *análisis de transmisión*, que permite el seguimiento en tiempo real de dichos eventos.
	Puede configurar los siguientes ajustes generales:
	• `mode=EDRKATA | EDRExpertOnPrem`. Cambio entre soluciones:
	  • `EDRKATA`. Endpoint Detection and Response Expert (versión 7.1 o anterior).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (versión 8.0 o posterior). Valor predeterminado.
	• `login=<user name> password=<password>`. Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

`show`	Muestra la configuración actual del componente.

KUMA. Integración de KUMA

Comandos para administrar el agente de KUMA integrado:

- Activar o desactivar la integración con KUMA.

  El agente de KUMA integrado proporciona interoperabilidad con la solución Kaspersky Unified Monitoring and Analysis Platform.

- Configuración de la conexión a los servidores de Kaspersky Unified Monitoring and Analysis Platform.

- Muestra la configuración actual del componente.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Operación	
`stop`	Desactivar la integración de KUMA.
`start`	Activar la integración de KUMA.
`set`	Configurar el agente de KUMA integrado. Los parámetros que puede configurar son los siguientes: • Añadir servidores de KUMA (`/servers=<protocol>://<server address>:<port>`) La aplicación admite los siguientes protocolos de conexión al servidor: `tcp`, `udp`, `http`, `https`. • Añada un certificado TLS (`/server-certificate=<path to the TLS certificate>`) • Configure el tiempo de espera de la conexión del servidor (`/timeout=<KUMA server connection timeout (s)>`) • Añadir un contenedor de cifrado (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Configure el retardo de transmisión del evento (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Muestra la configuración actual del componente.

Autenticación	
`/login=<user name> /password=<password>`	Credenciales de cuenta de usuario con los permisos de protección con contraseña requeridos.

Ejemplo

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. Ejecución de Análisis de YARA

Ejecución de la tarea *Ejecutar Análisis de YARA*. La aplicación analiza archivos y objetos en busca de indicadores de ataques dirigidos a la infraestructura de TI corporativa utilizando bases de datos de reglas YARA. Las *reglas YARA* son descripciones de firmas de ataques dirigidos e intrusiones en la infraestructura de TI corporativa que Kaspersky Endpoint Security utiliza para analizar objetos.

Para ejecutar un análisis de YARA, debe preparar archivos YARA que describan las reglas. Al crear archivos YARA, tenga en cuenta los siguientes requisitos:

- Kaspersky Endpoint Security admite archivos YARA con las extensiones .YARA y .YAR, que siguen el estándar abierto YARA 4.2.3 para describir indicadores de compromiso.
- Solo se pueden especificar archivos con reglas YARA para la tarea. La tarea *Ejecutar análisis de YARA* no admite otros tipos de reglas.
- Si ha agregado archivos YARA que Kaspersky Endpoint Security no admite, o si las reglas contienen errores de sintaxis, la tarea se anula con el mensaje de error correspondiente.
- Los identificadores de todos los archivos YARA utilizados en una sola tarea deben ser únicos. Si hay archivos de YARA con el mismo identificador, esto puede afectar los resultados de la ejecución de la tarea.
- Un análisis de YARA se interrumpe después de 128 coincidencias con los indicadores descritos en las reglas de YARA. Esto es necesario para limitar la cantidad de entradas del informe de análisis de YARA, y facilitar así el análisis y la protección del informe de desbordamiento debido a las reglas de YARA formuladas de manera imprecisa que pueden generar una gran cantidad de coincidencias.

Kaspersky recomienda crear una regla por archivo YARA. Esto hace que los resultados del análisis sean más legibles.

Un análisis de puede llevar una cantidad de tiempo considerable. Dependiendo del tamaño de la unidad, la configuración de la tarea y la cantidad de objetos en el disco, un análisis de YARA puede durar desde varios minutos hasta varias horas. La aplicación no muestra un indicador de progreso. No es posible detener ni cancelar un análisis de YARA. Se recomienda esperar hasta que los resultados de un análisis de YARA estén disponibles.

Sintaxis del comando

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

Archivos YARA	
`<full path to the YARA file>`	Ruta completa al archivo de YARA que desea utilizar para el análisis. Puede especificar rutas a varios archivos YARA separados por espacios. Argumento requerido si el valor `/path=<path to the folder with YARA files>` no se especifica. Ejemplo: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Ruta completa a una carpeta con archivos YARA que desea usar para el análisis. Argumento requerido si el valor `<full path to the YARA file>` no se especifica. Ejemplo: `/path=C:\Users\Admin\Desktop\YARA`

Configuración avanzada	
`/fastScan=<on|off>`	Análisis de YARA rápido Para cada objeto, la aplicación registra una aparición del indicador detectado. La aplicación también oculta duplicados de indicadores detectados en el registro. El análisis de YARA rápido permite analizar archivos grandes a mayor velocidad. Si no se especifica esta configuración, la aplicación realiza un análisis de YARA estándar. En este modo, la aplicación registra duplicados de indicadores detectados.
`/maxRules=<maximum number of scan rules>`	Límite del número de reglas únicas que, al alcanzarse, hace que la aplicación detenga el análisis YARA. Si no se especifica el valor de este parámetro o si se especifica `0`, la aplicación realiza el análisis de YARA sin limitaciones.
`/timeOut=<stop scan after the specified time in seconds>`	Cuánto tiempo puede tardar un análisis de YARA, en segundos. Cuando este tiempo se agota, la aplicación detiene el análisis de YARA. Si no se especifica el valor de este parámetro o si se especifica `0`, la aplicación realiza el análisis de YARA sin limitaciones.
`/recursive=<on|off>`	Este argumento inicia un análisis recursivo de subcarpetas dentro del análisis personalizado `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Este argumento inicia un análisis de YARA de archivos en la lista de carpetas especificada. Puede especificar varios valores separados por espacios. Kaspersky Endpoint Security admite los caracteres `*` y `?` al introducir una máscara de ruta de carpeta. Si este parámetro no se especifica, la aplicación realiza un análisis de YARA de todos los discos locales, excepto los recursos de red compartidos, las unidades en la nube y los medios extraíbles.
`/scanMemory=<on|off>`	Analizar la memoria de todos los procesos en ejecución.
`/scanProcess=<process name>`	Analizar la memoria solo para procesos especificados. Especifique rutas completas separadas por espacios a archivos ejecutables de procesos. También puede usar los caracteres `*` y `?` para introducir una máscara.
`/maxSize=<file size in bytes>`	Limitar el tamaño de archivo para el análisis de YARA. La aplicación omite archivos más grandes.
`/includes=<list of objects to be scanned>>`	Edición de la cobertura del análisis. Puede especificar varios valores separados por espacios. Estos son los valores disponibles: • Nombre del archivo • Extensión del archivo La cobertura del análisis se debe especificar con el parámetro `/scanFolders`. Ejemplo: `/scanFolders C:\*.* /includes=*.exe *.dll`: la aplicación analiza todos los archivos con las extensiones EXE y DLL en el disco C.
`/excludes=<list of objects to be scanned>`	Excluir archivos del análisis de YARA. Puede especificar varios valores separados por espacios. Estos son los valores disponibles: • Ruta del archivo • Máscara de la ruta del archivo Las exclusiones se deben especificar con el parámetro `/scanFolders`. Ejemplo: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml`: la aplicación omite el archivo readme.txt, todos los archivos de la carpeta C:\trusted y todos los archivos con la extensión .XML en la carpeta raíz en el disco C.
`/scanAutoruns=<on|off>`	Análisis de YARA de objetos de punto de ejecución automática.
`/excludeAutoruns=<list of autorun point areas to skip>`	Excluir objetos de punto de ejecución automática del alcance de análisis. Especifique rutas completas separadas por espacios a archivos ejecutables de procesos. También puede usar los caracteres `*` y `?` para introducir una máscara.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Si especifica una ruta a una carpeta, la aplicación guarda los resultados del análisis en la ruta especificada en un archivo llamado yara_<nombre del equipo>_<hora de finalización del análisis>.txt. Si especifica una ruta a un archivo TXT específico, la aplicación guarda los resultados del análisis en ese archivo. Por ejemplo, `/logFolder=C:\test` o `/logFolder=C:\test\abc.txt`. Los resultados del análisis se envían a la línea de comandos independientemente de si se especifica la opción `/logFolder`.

Valores de retorno de comando:

- `-1` significa que el comando no es compatible con la versión de la aplicación que está instalada en el equipo.
- `0` significa que el comando se ejecutó correctamente.
- `1` significa que no se pasó un argumento obligatorio al comando.
- `2` significa que ocurrió un error general.
- `4` significa que hubo un error de sintaxis.
- `5` significa que no se han encontrado uno o más archivos con las reglas YARA especificadas en el parámetro.

Si el comando se ejecutó correctamente (valor devuelto `0`) y se detectaron indicadores de compromiso en el camino, Kaspersky Endpoint Security envía la siguiente información del resultado de la tarea a la línea de comandos:

`Started at <time>` `Finished at <time>`	Hora de inicio y hora de finalización de un análisis.
`Host name: <computer name>`	El nombre del equipo en el que se detectó el objeto.
`Result: <error>`	Código del error que se produjo al ejecutar la tarea. Si no hay errores, la aplicación genera `0x00000000`.
`Comment: <comment text>`	Descripción del error que se produjo al ejecutar la tarea. Por ejemplo, `Operation timeout`.
`Object Name:` o `Process:` (al analizar la memoria del proceso)	El nombre del objeto o proceso sobre el que se activó la regla YARA.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hashes del objeto sobre el que se activó la regla YARA.
`Rule Name`	El nombre de la regla YARA activada.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadatos especificados en la regla YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Se han encontrado coincidencias dentro del objeto que cumplen las condiciones de la regla YARA:
	• Desplazamiento en la memoria de proceso o el archivo donde se detectó una coincidencia (`Offset`).
	• El nombre de la cadena coincidente en la regla YARA (`String name`).
	• La cadena coincidente en la memoria de proceso o en el archivo (`String data`).

FILTROS DE TELEMETRÍA. Filtrado de eventos que se enviarán a KUMA

De forma predeterminada, el envío de eventos al servidor KUMA está desactivado. Para asegurarse de que KUMA funcione correctamente, debe habilitar el envío de telemetría. Puede seleccionar el origen de un evento desde los registros estándar: *Application*, *Security* o *System*. Para mejorar el rendimiento y optimizar la transmisión de datos al servidor KUMA, puede agregar o excluir manualmente eventos individuales de la telemetría. Por ejemplo, puede excluir eventos de Sysmon.

Puede exportar la lista de exclusiones a un archivo JSON desde la línea de comandos.

Si el comando contiene solo el nombre del archivo al que desea exportar la configuración, la aplicación emplaza el archivo de la siguiente manera:

- Si la ruta a avp.com se añade a la variable del sistema %PATH%, la aplicación sitúa el archivo en la carpeta `C:\Windows\SysWOW64`.
- Si ejecuta el comando desde la carpeta de instalación de la aplicación, la exportación fallará porque la autoprotección de la aplicación bloquea la creación de un nuevo archivo en la carpeta de la aplicación. Para exportar la configuración de la aplicación a un archivo, introduzca la ruta del archivo.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Operación	
`export`	Exportación de filtros de eventos para enviar a KUMA.
`import`	Importación de filtros de eventos para enviar a KUMA. Si ya existen reglas de filtrado de eventos en el equipo, Kaspersky Endpoint Security las reemplaza al importar.

Archivo para exportar o importar	
`<file name>`	Nombre del archivo con filtros de eventos que se enviarán a KUMA. También puede introducir la ruta del archivo. Puede exportar filtros a un archivo JSON para enviarlos a KUMA.

Comandos de administración de Light Agent

Puede administrar la aplicación en el modo Light Agent para proteger entornos virtuales en la línea de comandos. Puede administrar la aplicación en modo Light Agent si la administración mediante la consola de Kaspersky Security Center no es posible. Para ver la lista de comandos de administración disponibles, utilice el comando `HELP`. Para conocer la sintaxis de un comando específico, escriba `HELP <command>`.

Para administrar la aplicación en modo Light Agent desde la línea de comandos:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Utilice la siguiente plantilla para ejecutar el comando:

   ```
   avp.com <command> [options]
   ```

   Kaspersky Endpoint Security ejecutará el comando especificado.

La aplicación instalada en modo Light Agent admite casi todos los comandos AVP de la aplicación instalada en modo Estándar. En el modo Light Agent, las tareas de actualización de la base de datos antivirus y las tareas de administración de claves de licencia son limitadas.

KSVLAINFO. Determinación del modo Light Agent

Determinación del modo Light Agent.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com KSVLAINFO
```

El comando envía la siguiente información a la consola:

- Modo Light Agent para proteger entornos virtuales: activado o desactivado.

  Si el modo Light Agent está activado, la aplicación se utiliza como parte de la solución de Kaspersky Security for Virtualization Light Agent .

- Modo de protección de VDI: activado o desactivado.

  El modo de protección VDI ayuda a optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. Si el modo de protección VDI está activado, las actualizaciones que requieren reiniciar la máquina virtual protegida no se instalan en las máquinas virtuales no persistentes. Al recibir actualizaciones que requieren un reinicio, el Light Agent instalado en una máquina virtual no persistente envía un mensaje a Kaspersky Security Center informándole que la plantilla de la máquina virtual protegida debe actualizarse.

- Tipo de máquina virtual protegida: persistente o no persistente.

- Rol de la máquina virtual protegida en la infraestructura virtual: servidor o estación de trabajo.

- Identificador: UUID.

VIISINFO. Estado de la conexión del Light Agent al servidor de integración

Ver información sobre la conexión del Agente Light al servidor de integración.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com VIISINFO
```

El comando envía la siguiente información a la consola:

- Dirección y puerto del servidor de integración al que está conectado el Light Agent.
- Estado de conexión del servidor de integración.
- Fecha y hora de la última conexión del Light Agent al servidor de integración.

SVMINFO. Estado de la conexión del Light Agent al Servidor de protección

Visualización de información sobre la conexión del Agente Light al Servidor de protección.

Para ejecutar el comando, vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security. También puede añadir la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

Sintaxis del comando

```
avp.com SVMINFO
```

El comando envía la siguiente información a la consola:

- Dirección de la SVM a la que está conectado el Light Agent y la ubicación de la SVM en la infraestructura virtual relativa al Light Agent: local o no local.
- Método de detección de SVM que utiliza el Light Agent: mediante un servidor de integración o usando una lista personalizada de direcciones de SVM.
- Lista de direcciones de SVM si se selecciona la lista de direcciones de SVM como método de detección de SVM.
- Etiqueta para conectar el Light Agent a la SVM.
- Algoritmo de selección de SVM: estándar o ampliado. Si se está utilizando el algoritmo de selección de SVM ampliado, también se muestra el tipo de ruta de SVM en la infraestructura virtual.
- Estado de protección de la conexión entre el Light Agent y el Servidor de protección.

Códigos de error

Al utilizar la aplicación a través de la línea de comandos, pueden ocurrir errores. En tales casos, Kaspersky Endpoint Security muestra un mensaje de error, como `Error: Cannot start task 'EntAppControl'`. Del mismo modo, Kaspersky Endpoint Security puede mostrar un código como `error=8947906D` (consulte la siguiente tabla).

Código de error	Descripción
09479001	La clave ya está en uso
0947901D	La licencia ha caducado. Las actualizaciones de las bases de datos ya no están disponibles
89479002	No se encuentra la clave
89479003	No se encuentra la firma digital o está dañada
89479004	La información está dañada
89479005	El archivo de clave está dañado
89479006	La licencia ha caducado
89479007	Archivo de clave no especificado
89479008	Archivo de clave no válido
89479009	Error al guardar los datos
8947900A	Error al leer los datos
8947900B	Error de E/S
8947900C	No se encuentran las bases de datos
8947900E	La biblioteca de licencia no se ha cargado
8947900F	Las bases de datos se han dañado o se han actualizado manualmente
89479010	Las bases de datos están dañadas
89479011	No se puede utilizar un archivo de clave no válido para añadir una clave de reserva
89479012	Error del sistema
89479013	La lista de claves rechazadas está dañada
89479014	La firma del archivo no coincide con la firma digital de Kaspersky
89479015	No se puede utilizar una clave para una licencia de evaluación como clave para una licencia comercial
89479016	Se requiere la licencia de pruebas beta para utilizar la versión beta de la aplicación
89479017	El archivo de clave no es compatible con esta aplicación. Kaspersky Endpoint Security para Windows no puede activarse con un archivo de clave para otra aplicación. Compruebe la aplicación que ha instalado
89479018	Clave de licencia bloqueada por Kaspersky
89479019	La aplicación ya se ha utilizado bajo una licencia de evaluación. No se puede añadir otra vez una clave para la licencia de evaluación
8947901A	El archivo de clave está dañado
8947901B	No se encuentra la firma digital, está dañada o no corresponde a la firma digital de Kaspersky
8947901C	No se puede añadir una clave si la licencia no comercial correspondiente ha caducado
8947901E	La fecha en la que se creó o utilizó el archivo de clave no es válida. Compruebe la fecha del sistema
8947901F	No se puede añadir una clave para la licencia de evaluación: otra clave para la licencia de evaluación ya está activa
89479020	La lista de claves rechazadas está dañada o no se encuentra
89479021	La descripción de actualización no se encuentra o está dañada
89479022	La clave no es adecuada para esta aplicación
89479023	No se puede utilizar un archivo de clave no válido para añadir una clave de reserva
89479025	Error al enviar la solicitud del servidor de activación. Posibles motivos: error en la conexión a Internet o problemas temporales en el servidor de activación. Intente activar la aplicación más tarde (en 1 o 2 horas) con el código de activación. Si vuelve a ocurrir este error, póngase en contacto con su proveedor de Internet
89479026	La solicitud contiene un código de activación incorrecto
89479027	No se puede obtener el estado de respuesta

Código de error	Descripción
89479028	Se ha producido un error al guardar el archivo temporal
89479029	Se ha introducido un código de activación incorrecto o se ha establecido en el equipo una fecha del sistema no válida. Compruebe la fecha del sistema en el equipo
8947902A	La clave no es compatible con esta aplicación o la licencia ha caducado
8947902B	Error al recibir un archivo de clave. Se ha introducido un código de activación incorrecto
8947902C	El servidor de activación devolvió el error 400
8947902D	El servidor de activación devolvió el error 401
8947902E	El servidor de activación devolvió el error 403
8947902F	El recurso necesario no está disponible en el servidor de activación. El servidor de activación devolvió el error 404. Compruebe la configuración de la conexión a Internet
89479030	El servidor de activación devolvió el error 405
89479031	El servidor de activación devolvió el error 406
89479032	Se requiere autenticación del proxy. Compruebe la configuración de red
89479033	Se ha agotado el tiempo de espera de la solicitud
89479034	El servidor de activación devolvió el error 409
89479035	El recurso necesario no está disponible en el servidor de activación. El servidor de activación devolvió el error 410. Compruebe la configuración de la conexión a Internet
89479036	El servidor de activación devolvió el error 411
89479037	El servidor de activación devolvió el error 412
89479038	El servidor de activación devolvió el error 413
89479039	El servidor de activación devolvió el error 414
8947903A	El servidor de activación devolvió el error 415
8947903C	Error interno del servidor
8947903D	Funcionalidad no compatible
8947903E	La respuesta de la puerta de vínculo no es válida. Compruebe la configuración de red
8947903F	El recurso no está disponible temporalmente
89479040	Se ha agotado el tiempo de espera de la puerta de vínculo. Compruebe la configuración de la red
89479041	El protocolo no es compatible con el servidor
89479043	Error HTTP desconocido
89479044	ID de recursos no válido
89479046	URL no válida
89479047	Carpeta de destino no válida
89479048	Error de asignación de memoria
89479049	Se ha producido un error al convertir los parámetros a cadena ANSI (URL, carpeta o agente)
8947904A	Se ha producido un error al crear un proceso de trabajo
8947904B	El proceso de trabajo ya se está ejecutando
8947904C	El proceso de trabajo no se está ejecutando
8947904D	No se encontró el archivo de clave en el servidor de activación
8947904E	La clave está bloqueada
8947904F	Error interno del Servidor de activación
89479050	No hay suficientes datos en la solicitud de activación

Código de error	Descripción
89479053	La licencia que se corresponde con la clave añadida ha caducado
89479054	Se ha establecido una fecha del sistema no válida en el equipo. Compruebe el valor de la fecha del sistema
89479055	La licencia de evaluación ha caducado
89479056	El período de activación de la aplicación ha caducado
89479057	Se ha superado el límite de activaciones de aplicaciones para el código especificado
89479058	Procedimiento de activación terminado con error de sistema
89479059	No se puede utilizar una clave para una licencia de evaluación como clave para una licencia comercial
8947905C	Se requiere un código de activación
89479062	No se puede conectar con el servidor de activación
89479064	El servidor de activación no está disponible. Compruebe la configuración de la conexión a Internet y vuelva a intentar la activación
89479065	La licencia ha caducado
89479066	No se puede remplazar la clave activa con una clave caducada
89479067	No se puede añadir una clave de reserva si la licencia correspondiente caduca antes que la licencia actual
89479068	No se encuentra la clave de suscripción actualizada
8947906A	Código de activación no válido
8947906B	La clave ya está activa
8947906C	Los tipos de licencia que corresponden a las claves activa y de reserva no coinciden
8947906D	Componente no compatible con la licencia
8947906E	No se puede añadir la clave de suscripción como clave de reserva
89479213	Error genérico de la capa de transporte
89479214	No se pudo conectar con el servidor de activación
89479215	Formato de dirección web no válido
89479216	Error al convertir la dirección del servidor proxy
89479217	Error al convertir la dirección del servidor. Compruebe la configuración de su conexión a Internet
89479218	Error al intentar conectar con el servidor
89479219	Acceso denegado remotamente
8947921A	Se ha agotado el tiempo de espera de la operación
8947921B	Error al enviar la solicitud HTTP
8947921C	Error de conexión SSL
8947921D	Operación interrumpida debido a una devolución de llamada
8947921E	Demasiadas redirecciones
8947921F	Error en la comprobación del destinatario
89479220	Respuesta vacía del servidor
89479221	Error al enviar datos
89479222	Error al recibir datos
89479223	Problema relacionado con el certificado SSL
89479224	Problema relacionado con el cifrado SSL
89479225	Problema relacionado con el centro de certificación SSL
89479226	Contenidos del paquete de red no válidos

Código de error	Descripción
89479227	Acceso denegado a la cuenta
89479228	Archivo del certificado SSL no válido
89479229	No se puede cerrar la conexión SSL
8947922A	Error recurrente
8947922B	Archivo no válido con certificados revocados
8947922C	Error en la solicitud del certificado SSL
89479401	Error desconocido del servidor
89479402	Error interno del servidor
89479403	No hay ninguna clave disponible para el código de activación introducido
89479404	Clave activa bloqueada
89479405	Faltan parámetros obligatorios de la solicitud de activación
89479406	Número de cliente o contraseña no válidos
89479407	Código de activación no válido
89479408	El código de activación no es compatible con esta aplicación. Kaspersky Endpoint Security para Windows no puede activarse con un código de activación para otra aplicación. Compruebe la aplicación que ha instalado
89479409	Se requiere un código de activación
8947940B	Período de activación terminado
8947940C	Se ha superado el número de activaciones con este código
8947940D	Formato no válido de la ID de solicitud
8947940E	El código de activación ya está en uso
8947940F	Error al renovar el código de activación
89479410	Código de activación no válido para esta región
89479411	Este código de activación no se puede emplear para la localización de la aplicación
89479412	El código de activación es para la nueva versión de la aplicación. Necesita un código de activación diferente para activar la versión instalada de la aplicación
89479413	El servidor de activación devolvió el error 643
89479414	El servidor de activación devolvió el error 644
89479415	El servidor de activación devolvió el error 645
89479416	El servidor de activación devolvió el error 646
89479417	Se requiere la versión 1.0 del servidor de activación
89479418	Formato de código de activación incorrecto
89479419	La hora del equipo no está sincronizada con la hora del servidor de activación
8947941A	Versión incorrecta de la aplicación
8947941B	La suscripción ha caducado
8947941C	Se ha superado el número de activaciones
8947941D	Firma del vale no válida
8947941E	Se necesitan datos adicionales
8947941F	Error en la verificación de los datos
89479420	Suscripción inactiva
89479421	El servidor de activación se encuentra en mantenimiento

Código de error	Descripción
89479501	Error inesperado
89479502	Se ha transferido un parámetro no válido. Por ejemplo, una lista vacía de direcciones de servidor de activación
89479503	Código de activación no válido (hash no válido)
89479504	ID de usuario no válido
89479505	Contraseña de usuario no válida
89479506	Respuesta no válida del servidor de activación
89479507	Se ha interrumpido la solicitud de activación
89479509	El servidor de activación devolvió una lista de reenvío vacía

Apéndice. Perfiles de la aplicación

Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Los perfiles permiten administrar la aplicación desde la línea de comandos. Puede usarlos para ejecutar los comandos `START`, `STOP`, `STATUS`, `STATISTICS` y `EXPORT`. Con los perfiles, puede configurar parámetros de la aplicación (por ejemplo, `STOP DeviceControl`) o ejecutar tareas (por ejemplo, `START Scan_My_Computer`).

Estos son los perfiles disponibles:

- `AdaptiveAnomaliesControl` – Control de anomalías adaptativo
- `AMSI`: Protección AMSI.
- `AntiCryptor`
- `BehaviorDetection`: Detección de comportamiento.
- `DeviceControl` – Control de dispositivos
- `EntAppControl` – Control de aplicaciones
- `File_Monitoring` o `FM` – Protección contra archivos peligrosos
- `Firewall` o `FW` – Firewall
- `HIPS`: Prevención de intrusiones en el host.
- `IDS` – Protección frente a amenazas en la red
- `IntegrityCheck` – Comprobación de integridad
- `LogInspector` – Inspección de registros
- `Mail_Monitoring` o `EM` – Protección frente a amenazas en el correo
- `Rollback` - Actualizar reversión (el perfil no se puede aplicar si la aplicación está instalada en Modo de Light Agent)
- `Scan_ContextScan` – Análisis desde el menú contextual

- `Scan_IdleScan` – Análisis en segundo plano
- `Scan_Memory` – Memoria del kernel
- `Scan_My_Computer` – Análisis completo
- `Scan_Objects` – Análisis personalizado
- `Scan_Qscan` – Análisis de los objetos que se cargan durante el inicio del sistema operativo
- `Scan_Removable_Drive` – Análisis de unidades extraíbles
- `Scan_Startup` o `STARTUP` – Análisis de áreas críticas
- `Updater` - Actualización (el perfil no se puede aplicar si la aplicación está instalada en Modo de Light Agent)
- `Web_Monitoring` o `WM` – Protección frente a amenazas web
- `WebControl` – Control web

Kaspersky Endpoint Security también es compatible con los perfiles de servicio. Puede necesitar este tipo de perfil si en alguna oportunidad se comunica con el Soporte técnico de Kaspersky.

Administrar la aplicación a través de la API REST

Kaspersky Endpoint Security le permite configurar la aplicación, ejecutar un análisis, actualizar las bases de datos antivirus y realizar otras tareas utilizando soluciones de terceros. Kaspersky Endpoint Security proporciona una API para este fin. La API REST de Kaspersky Endpoint Security funciona a través de HTTP y consta de un conjunto de métodos de solicitud y respuesta. En otras palabras, puede administrar Kaspersky Endpoint Security a través de una solución de terceros, en lugar de mediante la interfaz de la aplicación local o la Consola de administración de Kaspersky Security Center.

Para comenzar a usar la API REST, debe instalar Kaspersky Endpoint Security con compatibilidad con la API REST. El cliente REST y Kaspersky Endpoint Security tienen que estar instalados en el mismo equipo.

Para garantizar una interacción segura entre Kaspersky Endpoint Security y el cliente REST:

- Configure la protección del cliente de REST contra el acceso no autorizado según las recomendaciones del desarrollador del cliente de REST. Configure la protección de la carpeta del cliente de REST contra la escritura con la ayuda de la Lista de Control de Acceso Discrecional - DACL.
- Para ejecutar el cliente de REST, utilice una cuenta aparte con derechos de administrador. Deniegue el acceso interactivo al sistema para esta cuenta.

La aplicación se administra a través de la API REST en http://127.0.0.1 o http://localhost. No se puede administrar Kaspersky Endpoint Security de forma remota a través de la API REST.

ABRIR LA DOCUMENTACIÓN DE LA API REST

Instalar la aplicación con la API REST

Para administrar la aplicación a través de la API REST, debe instalar Kaspersky Endpoint Security con compatibilidad con la API REST. Si administra Kaspersky Endpoint Security a través de la API REST, no puede administrar la aplicación utilizando Kaspersky Security Center.

Preparativos para la instalación de la aplicación con soporte de API REST

La interacción segura de Kaspersky Endpoint Security con el cliente REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga útil de cada solicitud.

Para crear un certificado, puede utilizar, por ejemplo, OpenSSL.

Ejemplo:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Utilice el algoritmo de cifrado RSA con una longitud de clave de 2048 bits o más.

Como resultado, obtendrá un certificado `cert.pem` y una clave privada `key.pem`.

Instalar la aplicación con soporte de API REST

Para instalar Kaspersky Endpoint Security con compatibilidad con la API REST:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta que contiene el paquete de distribución para Kaspersky Endpoint Security versión 11.2.0 o posterior.
3. Instale Kaspersky Endpoint Security con la siguiente configuración:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Nombre de usuario que se utilizará para administrar la aplicación a través de la API REST. Introduzca el nombre de usuario con el formato `<DOMAIN>\<UserName>` (por ejemplo, `RESTAPI_User=COMPANY\Administrator`). Puede administrar la aplicación a través de la API REST solo desde esta cuenta. Solo puede seleccionar un usuario para que funcione con la API REST.
   - `RESTAPI_Port=<port>`

     Puerto utilizado para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782. Asegúrese de que el puerto esté libre. Parámetro opcional.
   - `RESTAPI_Certificate=<path to certificate>`

     Certificado para identificar solicitudes (por ejemplo, `RESTAPI_Certificate=C:\cert.pem`).

     Puede instalar el certificado después de instalar la aplicación o actualizar el certificado después de que caduque.

     Cómo instalar un certificado para la identificación de solicitudes de API REST

     1. Desactivar Autoprotección de Kaspersky Endpoint Security

        El mecanismo de Autoprotección impide la modificación o eliminación de los archivos de aplicaciones que se encuentran en el disco duro, de los procesos en la memoria y de las entradas en el registro del sistema.

     2. Vaya a la clave de registro que contiene la configuración de la API REST:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`

     3. Introduzca la ruta al certificado, por ejemplo, `Certificate = C:\Folder\cert.pem`.

     4. Activar Autoprotección de Kaspersky Endpoint Security.

     5. Reiniciar la aplicación.
   - `AdminKitConnector=1`

     Administración de aplicaciones mediante sistemas de administración. La administración está permitida de forma predeterminada.

También puede usar el archivo setup.ini para definir la configuración para que funcione con la API REST.

Ejemplo:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

Como resultado, podrá administrar la aplicación a través de la API REST. Para verificar su funcionamiento, abra la documentación de la API REST utilizando una solicitud GET.

Ejemplo:
```
GET http://localhost:6782/kes/v1/api-docs
```

Si ha instalado la aplicación con soporte para la API REST, Kaspersky Endpoint Security crea automáticamente una regla de permiso en la configuración de Control web para acceder a los recursos web (*Regla de servicio para la API REST*). Esta regla es necesaria para permitir que el cliente REST acceda a Kaspersky Endpoint Security en todo momento. Por ejemplo, si ha restringido el acceso de los usuarios a los recursos web, esto no afectará a la administración de la aplicación a través de la API REST. Recomendamos que no se elimine la regla ni se cambie la configuración de *Regla de servicio para la API REST*. Si eliminó la regla, Kaspersky Endpoint Security la restaurará después de que reinicie la aplicación.

Funcionamiento con la API

No se puede restringir el acceso a la aplicación a través de la API REST utilizando la protección con contraseña. Por ejemplo, no se puede impedir que un usuario desactive la protección a través de la API REST. Puede configurar la protección con contraseña a través de la API REST y restringir el acceso de los usuarios a la aplicación a través de la interfaz local.

Para administrar la aplicación a través de la API REST, debe ejecutar el cliente REST con la cuenta que especificó al instalar la aplicación con compatibilidad con la API REST. Solo puede seleccionar un usuario para que funcione con la API REST.

ABRIR LA DOCUMENTACIÓN DE LA API REST

Para administrar la aplicación a través de la API REST se tienen que realizar los pasos siguientes:

1. Obtenga los valores actuales de la configuración de la aplicación. Para hacerlo, envíe una solicitud GET.

   Ejemplo:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. La aplicación enviará una respuesta con la estructura y los valores de la configuración. Kaspersky Endpoint Security admite los formatos XML y JSON.

   Ejemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Edite la configuración de la aplicación. Utilice la estructura de configuración recibida en respuesta a la solicitud GET.

   Ejemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Guarde la configuración de la aplicación (la carga útil) en un JSON (payload.json).

5. Firme el JSON en formato PKCS7.

   Ejemplo:

   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   Como resultado, obtiene un archivo firmado con la carga útil de la solicitud (`signed_payload.pem`).

6. Edite la configuración de la aplicación. Para hacerlo, envíe una solicitud POST y adjunte el archivo firmado con la carga útil de la solicitud (`signed_payload.pem`).

La aplicación implementa la configuración nueva y envía una respuesta que contiene los resultados de la configuración de la aplicación (la respuesta puede estar vacía). Puede verificar que la configuración se actualice mediante una solicitud GET.

Fuentes de información de la aplicación

Esta sección contiene las fuentes de información sobre la aplicación.

Puede seleccionar la fuente de información más práctica dependiendo de la importancia y urgencia del problema.

Página de Kaspersky Endpoint Security en el sitio web de Kaspersky

En la página de Kaspersky Endpoint Security, puede ver información general sobre la aplicación, sus funciones y sus características.

La página de Kaspersky Endpoint Security contiene un enlace a la tienda en línea. En ella puede comprar o renovar la aplicación.

Página de Kaspersky Endpoint Security en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico.

En la página de Kaspersky Endpoint Security de la Base de conocimientos, puede leer artículos que proporcionan información útil, recomendaciones y respuestas a preguntas frecuentes sobre cómo comprar, instalar y usar la aplicación.

Los artículos de la Base de conocimientos pueden responder a preguntas relacionadas no solo con Kaspersky Endpoint Security, sino también con otras aplicaciones de Kaspersky. Los artículos de la Base de conocimientos también pueden contener noticias de soporte técnico.

Discusión sobre aplicaciones de Kaspersky en el Foro

Si su pregunta no requiere una respuesta urgente, puede comentarla con los expertos de Kaspersky y otros usuarios en nuestro Foro.

En el Foro, puede ver temas existentes, publicar sus propios comentarios y crear nuevos temas de debate.

Cómo ponerse en contacto con el Soporte técnico

Si no es posible encontrar una solución al problema en la documentación o en otras fuentes de información acerca de Kaspersky Endpoint Security, le recomendamos que se ponga en contacto con el Soporte técnico. El Soporte técnico responderá a sus preguntas sobre la instalación y uso de Kaspersky Endpoint Security.

Kaspersky ofrece soporte para Kaspersky Endpoint Security durante su ciclo de vida (consulte la página del ciclo de vida de la aplicación). Antes de ponerse en contacto con el Soporte técnico, lea las reglas de soporte.

Puede ponerse en contacto con Soporte técnico de una de las siguientes formas:

- Visitando el sitio web de soporte técnico
- Enviando una solicitud al Soporte técnico de Kaspersky a través del portal CompanyAccount de Kaspersky

Después de informar a los especialistas de Soporte técnico de Kaspersky acerca del problema, puede que le pidan que cree un *archivo de seguimiento*. El archivo de seguimiento permite supervisar paso a paso el proceso de ejecución de comandos de aplicación y determinar la etapa de funcionamiento de la aplicación en la que se produce el error.

Los especialistas de Soporte técnico pueden solicitar también información adicional sobre el sistema operativo, los procesos en ejecución del equipo e informes detallados sobre el funcionamiento de los componentes de aplicación.

Mientras el diagnóstico está en ejecución, los expertos del Soporte técnico pueden pedir que cambie la configuración de la aplicación por:

- Activar una función que permitirá recibir información de diagnóstico extendida.
- Configure componentes individuales de la aplicación cambiando configuraciones especiales a las que no se puede acceder a través de la interfaz de usuario estándar.
- Cambiar opciones relativas al almacenamiento de la información de diagnóstico.
- Configurar la interceptación y el registro del tráfico de red.

Los expertos del Soporte técnico le darán toda la información que necesitará para realizar estas operaciones (descripción de la secuencia de pasos, parámetros que se deben modificar, archivos de configuración, secuencias de comandos, funcionalidad adicional de la línea de comandos, módulos de depuración, utilidades con fines especiales, etc.). También le informarán del alcance de los datos utilizados con fines de depuración. La información de diagnóstico extendida se guarda en el equipo del usuario. Los datos no se transmiten automáticamente a Kaspersky.

Las operaciones que se describen anteriormente solo se deben realizar bajo la supervisión de los especialistas de Soporte técnico siguiendo sus instrucciones. Cambiar la configuración de la aplicación por su cuenta de forma no descrita en la Ayuda en línea o en las recomendaciones del Servicio técnico puede provocar ralentizaciones y caídas del sistema operativo, reducir el nivel de protección de su equipo y dañar la disponibilidad e integridad de la información que se procesa.

Contenido y almacenamiento de archivos de seguimiento

Usted es personalmente responsable de la seguridad de los datos que se almacenan en su equipo y, especialmente, de supervisar y restringir el acceso a los datos hasta que se envíen a Kaspersky.

Los archivos de seguimiento se almacenan en el equipo siempre que la aplicación esté en uso y se eliminan permanentemente cuando se quita la aplicación.

Los archivos de seguimiento —exceptuados los del Agente de autenticación— se almacenan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

El nombre de los archivos de rastreo tiene el siguiente formato: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Puede ver los datos almacenados en los archivos de seguimiento.

Todos los archivos de seguimiento contienen los datos comunes siguientes:

- Hora del evento
- Número del subproceso de ejecución

  El archivo de seguimiento del Agente de autenticación no contiene esta información.

- Componente de la aplicación que causó el evento
- Nivel de gravedad de eventos (evento informativo, advertencia, evento crítico, error)
- Una descripción del evento que implica la ejecución del comando por un componente de la aplicación y el resultado de la ejecución de este comando.

Contenidos de los archivos de seguimiento SRV.log, GUI.log y ALL.log

Los archivos de seguimiento `SRV.log`, `GUI.log` y `ALL.log` pueden almacenar la siguiente información además de los datos generales:

- Datos personales, incluido el apellido, el nombre y el segundo nombre, si se incluyen estos datos en la ruta a los archivos en un equipo local.
- Datos sobre el hardware instalado en el equipo (como datos de firmware de BIOS/UEFI). Estos datos se escriben en archivos de seguimiento cuando se realiza el Cifrado de disco de Kaspersky.
- El nombre de usuario y la contraseña si se transmitieron abiertamente. Estos datos se pueden registrar en archivos de seguimiento durante el análisis del tráfico de Internet.
- El nombre de usuario y la contraseña si se incluyen en encabezados HTTP.

- El nombre de la cuenta de Microsoft Windows si se incluye el nombre de la cuenta en un nombre de archivo.
- Su dirección de correo electrónico o una dirección web que contenga el nombre y la contraseña de su cuenta si se incluyen en el nombre del objeto detectado.
- Los sitios web que visita y a los que se le redirige desde estos. Estos datos se escriben en archivos de seguimiento cuando la aplicación analiza sitios web.
- Dirección del servidor proxy, nombre del equipo, puerto, dirección IP y nombre de usuario usado para iniciar sesión en el servidor proxy. Estos datos se escriben en los archivos de seguimiento si la aplicación utiliza a un servidor proxy.
- Direcciones IP remotas con las que el equipo establece conexiones.
- Asunto del mensaje, ID, nombre y dirección del remitente de la página web del remitente del mensaje en una red social. Estos datos se escriben en archivos de seguimiento si el componente Control web está activado.
- Datos de tráfico de red. Estos datos se escriben en archivos de seguimiento si los componentes de supervisión están activados (como Control web).
- Datos recibidos de los servidores de Kaspersky (como la versión de las bases de datos antivirus).
- Estados de los componentes de Kaspersky Endpoint Security y sus datos de funcionamiento.
- Datos sobre la actividad del usuario en la aplicación.
- Eventos del sistema operativo.

Contenido de los archivos de seguimiento HST.log, BL.log, Dumpwriter.log, WD.log y AVPCon.dll.log

Además de datos generales, el archivo de seguimiento `HST.log` contiene información sobre la ejecución de una tarea de la actualización de la base de datos y del módulo de aplicación.

Además de datos generales, el archivo de seguimiento `BL.log` contiene información sobre los eventos que ocurren durante el funcionamiento de la aplicación, así como los datos requeridos para solucionar problemas de errores de aplicación. Este archivo se crea si se inicia la aplicación con el parámetro -bl de avp.exe.

Además de datos generales, el archivo de seguimiento `Dumpwriter.log` contiene información de servicio requerida para solucionar errores que se producen cuando se escribe el archivo de volcado de la aplicación.

Además de datos generales, el archivo de seguimiento `WD.log` contiene información sobre los eventos que se producen durante el funcionamiento del servicio avpsus, incluidos eventos de actualización del módulo de aplicación.

Además de datos generales, el archivo de seguimiento `AVPCon.dll.log` contiene información sobre los eventos que se producen durante el funcionamiento del módulo de conectividad de Kaspersky Security Center.

Contenido de los archivos de seguimiento del rendimiento

El nombre de los archivos de seguimiento del rendimiento sigue este formato: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Además de los datos generales, los archivos de seguimiento del rendimiento contienen información sobre la carga del procesador, sobre los procesos en ejecución y sobre el tiempo de carga del sistema operativo y las aplicaciones.

Contenido de los archivos de seguimiento del componente de protección AMSI

Además de datos generales, el archivo de seguimiento `AMSI.log` contiene información sobre los resultados de los análisis realizados por solicitud de aplicaciones de terceros.

Contenido de archivos de seguimiento del componente Protección frente a amenazas en el correo

Además de datos generales, el archivo de seguimiento `mcou.OUTLOOK.EXE.log` puede contener partes de mensajes de correo electrónico, entre ellas direcciones de correo electrónico.

Contenido de archivos de seguimiento del componente Analizar desde el menú contextual

Además de datos generales, el archivo de seguimiento `shellex.dll.log` contiene información sobre la ejecución de la tarea de análisis y los datos requeridos para depurar la aplicación.

Contenido de los archivos de seguimiento del complemento web de la aplicación

Los archivos de seguimiento del complemento web de la aplicación se almacenan en el equipo en el que se ha instalado Kaspersky Security Center Web Console, dentro de la carpeta `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

El nombre de los archivos de seguimiento del complemento web de la aplicación sigue este formato: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Web Console comienza a guardar información en cuanto concluye su instalación. Los archivos de seguimiento se eliminan cuando Web Console se desinstala.

Además de los datos generales, los archivos de seguimiento del complemento web contienen la siguiente información:

- Contraseña del usuario KLAdmin para desbloquear la interfaz de Kaspersky Endpoint Security (Protección con contraseña).
- Contraseña temporal para desbloquear la interfaz de Kaspersky Endpoint Security (Protección con contraseña).
- Nombre de usuario y contraseña para el servidor de correo SMTP (Notificaciones por correo electrónico).
- Nombre de usuario y contraseña para el servidor proxy (Servidor proxy).
- Nombre de usuario y contraseña para la tarea *Cambiar componentes de la aplicación*.
- Credenciales de cuentas y rutas especificadas en las propiedades de las directivas y de las tareas de Kaspersky Endpoint Security.

Contenidos del archivo de seguimiento del Agente de autenticación

El archivo de seguimiento del Agente de autenticación se almacena en la carpeta System Volume Information y tiene el siguiente nombre: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Además de datos generales, el archivo de seguimiento del Agente de autenticación contiene información sobre el funcionamiento del Agente de autenticación y las acciones que el usuario lleva a cabo con el Agente de autenticación.

Rastreo del funcionamiento de aplicaciones

El *rastreo de la aplicación* es un registro detallado de las acciones que realiza la aplicación y de los mensajes acerca de los eventos que se producen durante el funcionamiento de la aplicación. Durante el proceso de rastreo, la aplicación crea un conjunto de archivos con datos sobre el funcionamiento de diferentes componentes de la aplicación (por ejemplo, SRV.log, WD.log y otros).

> La función de rastreo de la aplicación solo debe utilizarse bajo la supervisión del Soporte técnico de Kaspersky.

Para crear un archivo de seguimiento de la aplicación:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Herramientas de soporte**.
3. Utilice el interruptor **Activar el seguimiento de aplicaciones** para activar o desactivar el rastreo del funcionamiento de la aplicación.

4. En la lista desplegable **Rastreo**, seleccione un modo de seguimiento de la aplicación:

   - **Con limitación de tamaño**. Guardar los datos de seguimiento en un número de conjuntos de archivos de tamaño limitado. Cuando se alcance el tamaño máximo, los archivos más antiguos se sobrescribirán. Si se selecciona este modo, puede definir el número máximo de conjuntos de archivos por rotación y el tamaño máximo para cada conjunto de archivos.

     De forma predeterminada, la aplicación guarda cinco conjuntos de archivos de rastreo. El tamaño máximo de cada conjunto de archivos es 3072 MB. De esta forma, necesita 15 GB de espacio libre en disco para guardar los archivos de rastreo.

   - **Sin limitaciones**. Guardar un archivo de seguimiento (sin límite de tamaño).

5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento:

   - **Normal** significa que el archivo de seguimiento guarda mensajes sobre todos los errores, advertencias e información sobre el funcionamiento normal de la aplicación (predeterminado).

   - **Detallado** significa que el archivo de seguimiento guarda toda la información sobre el funcionamiento de la aplicación.

   Hay niveles de seguimiento adicionales disponibles si administra la configuración de seguimiento de la aplicación en la línea de comandos. Se le aconseja que aclare el nivel de seguimiento necesario con un especialista del Soporte técnico. Si no dispone de asistencia por parte del Soporte técnico, establezca el nivel de seguimiento en **Normal**.

   > Si el seguimiento de la aplicación se activó en la línea de comandos y se estableció un nivel de seguimiento diferente a **Normal** o **Detallado**, la lista desplegable **Nivel** se establece en **Normal**.

6. Para detener el proceso de seguimiento, regrese a la ventana **Herramientas de soporte** y desactive el seguimiento.

> También puede crear archivos de seguimiento al instalar la aplicación desde la línea de comandos, incluso al utilizar el archivo setup.ini.

Como resultado, se crean archivos de rastreo del funcionamiento de la aplicación en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Cuando los archivos de seguimiento rotados están creados, envíelos al Soporte técnico de Kaspersky.

Kaspersky Endpoint Security elimina los archivos de seguimiento de manera automática cuando se elimina la aplicación. También puede eliminar los archivos de forma manual. Para hacerlo, debe desactivar el rastreo y detener la aplicación.

Rastreo del rendimiento de aplicaciones

Kaspersky Endpoint Security le permite obtener información sobre los problemas que puedan ocurrir en el funcionamiento del equipo al utilizar la aplicación. Por ejemplo, si observa demoras al cargar el sistema operativo tras instalar la aplicación, puede recibir información al respecto. Para brindar esta información, Kaspersky Endpoint Security crea archivos de seguimiento del rendimiento. Realizar un *rastreo del rendimiento* se refiere a registrar las acciones que la aplicación realiza con el fin de diagnosticar los problemas de rendimiento de Kaspersky Endpoint Security. Para obtener la información, Kaspersky Endpoint Security utiliza el servicio de Seguimiento de eventos para Windows (ETW). Diagnosticar los problemas de Kaspersky Endpoint Security y determinar sus causas es tarea del Soporte técnico de Kaspersky.

La función de rastreo de la aplicación solo debe utilizarse bajo la supervisión del Soporte técnico de Kaspersky.

Para crear un archivo de seguimiento del rendimiento:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Herramientas de soporte**.
3. Utilice el interruptor **Activar el seguimiento de rendimiento** para activar o desactivar el seguimiento del rendimiento de las aplicaciones.
4. En la lista desplegable **Rastreo**, seleccione un modo de seguimiento de la aplicación:
   - **Con limitación de tamaño**. Guardar los datos de seguimiento en un número limitado de archivos, que no podrán superar un tamaño máximo. Cuando se alcance el tamaño máximo, los archivos más antiguos se sobrescribirán. Si se selecciona este modo, puede definir el tamaño máximo para cada archivo.
   - **Sin limitaciones**. Guardar un archivo de seguimiento (sin límite de tamaño).
5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento:
   - **Ligero**. Kaspersky Endpoint Security analizará los procesos más importantes del sistema operativo relacionados con el rendimiento.
   - **Detallado**. Kaspersky Endpoint Security analizará todos los procesos del sistema operativo relacionados con el rendimiento.
6. En la lista desplegable **Tipo de rastreo**, seleccione el tipo de rastreo:
   - **Información básica**. Kaspersky Endpoint Security analizará los procesos mientras el sistema operativo esté en funcionamiento. Utilice este tipo de seguimiento para problemas que continúen después de que el sistema operativo se haya cargado (por ejemplo, si tiene problemas para acceder a Internet a través del navegador).
   - **Al reiniciar**. Kaspersky Endpoint Security analizará los procesos únicamente mientras el sistema operativo se esté cargando. Una vez que el sistema operativo se haya cargado, Kaspersky Endpoint Security detendrá el proceso de seguimiento. Utilice este tipo de seguimiento si su problema está vinculado a alguna demora durante la carga del sistema operativo.

7. Reinicie el equipo e intente reproducir el problema.

8. Para detener el proceso de seguimiento, vuelva a la ventana Herramientas de soporte y desactive el seguimiento.

Como resultado, se crea un archivo de seguimiento del rendimiento en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Envíe ese archivo al Soporte técnico de Kaspersky.

Escritura de volcado

Un archivo de volcado contiene toda información sobre la memoria de trabajo de los procesos de la Kaspersky Endpoint Security en el momento en que se crea el archivo de volcado.

> Los archivos de volcado guardados pueden contener datos confidenciales. Para controlar el acceso a los datos, debe garantizar de forma independiente la seguridad de los archivos de volcado.

Los archivos de volcado se almacenan en el equipo siempre que la aplicación esté en uso y se eliminan permanentemente cuando se elimina la aplicación. Los archivos de volcado se almacenan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

Cómo activar la escritura de volcado en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.

2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de la aplicación**.

4. En el bloque **Información de depuración**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, use la casilla de verificación **Activar escritura de volcado** para activar o desactivar la escritura de volcado de la aplicación.

6. Guarde los cambios.

Cómo activar la escritura de volcado en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.

2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.

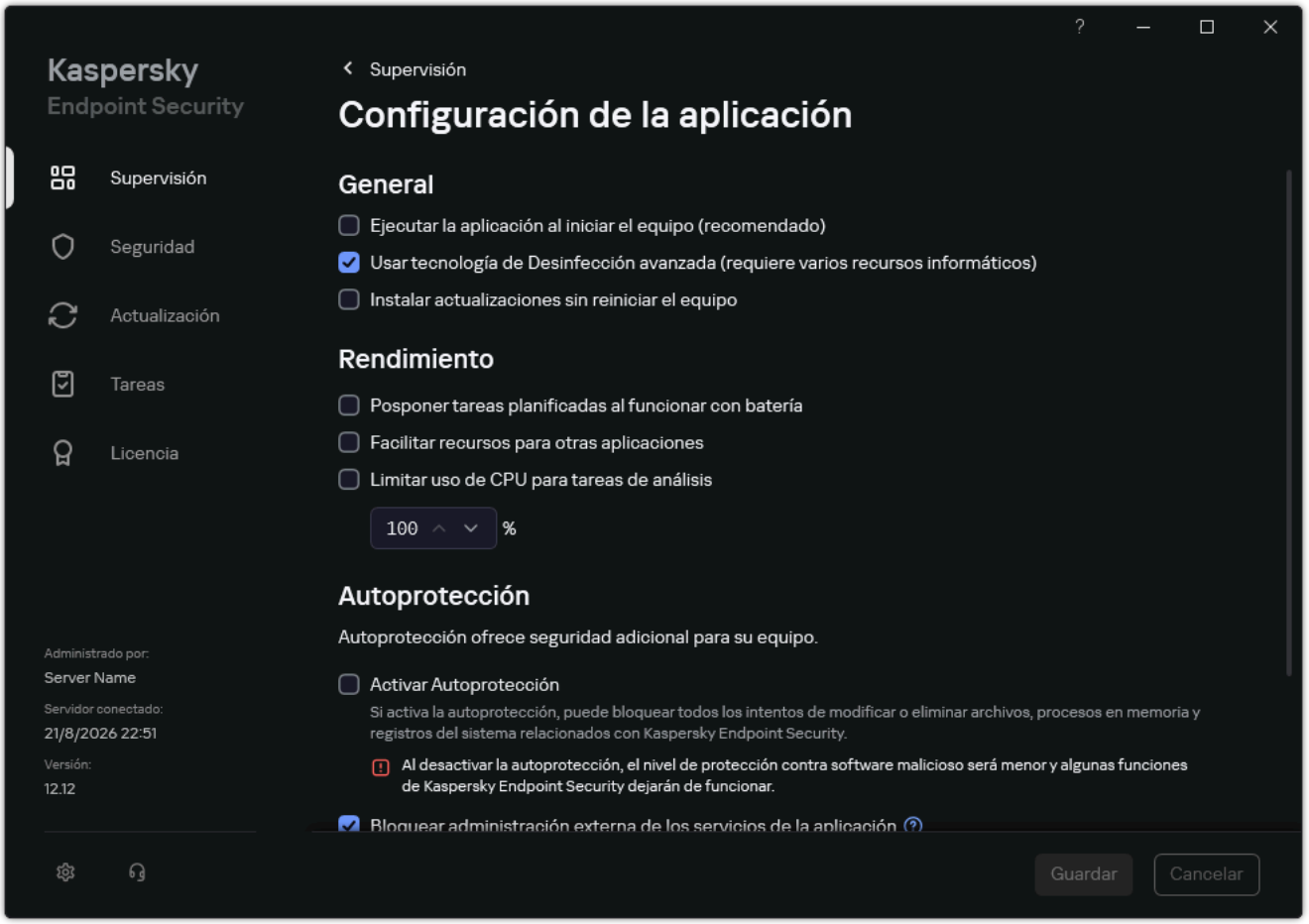
4. Vaya a **Configuración general** → **Soporte técnico**.

5. En el bloque **Información de depuración**, use la casilla de verificación **Escritura de volcado ACTIVADA** para activar o desactivar la escritura de volcado de la aplicación.

6. Guarde los cambios.

Cómo activar la escritura de volcado en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. En el bloque **Información de depuración**, use la casilla de verificación **Activar escritura de volcado** para activar o desactivar la escritura de volcado de la aplicación.
4. Guarde los cambios.

Protección de archivos de volcado y archivos de seguimiento

Los archivos de volcado y los archivos de rastreo contienen información sobre el sistema operativo y también pueden contener datos de usuario. Para evitar el acceso no autorizado a dichos datos, puede activar la protección de los archivos de volcado y rastreo.

Si se activa la protección de los archivos de volcado y rastreo, los usuarios siguientes pueden acceder a dichos archivos:

- El administrador del sistema y el administrador local pueden acceder a los archivos de volcado, así como el usuario que activó la escritura de los archivos de volcado y rastreo.
- Únicamente el administrador del sistema y el administrador del equipo local pueden acceder a los archivos de rastreo.

Cómo activar la protección de archivos de volcado y archivos de rastreo en la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general → Configuración de la aplicación**.
4. En el bloque **Información de depuración**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, use la casilla de verificación **Activar la protección de los archivos de volcado y de rastreo** para activar o desactivar la protección de archivos.
6. Guarde los cambios.

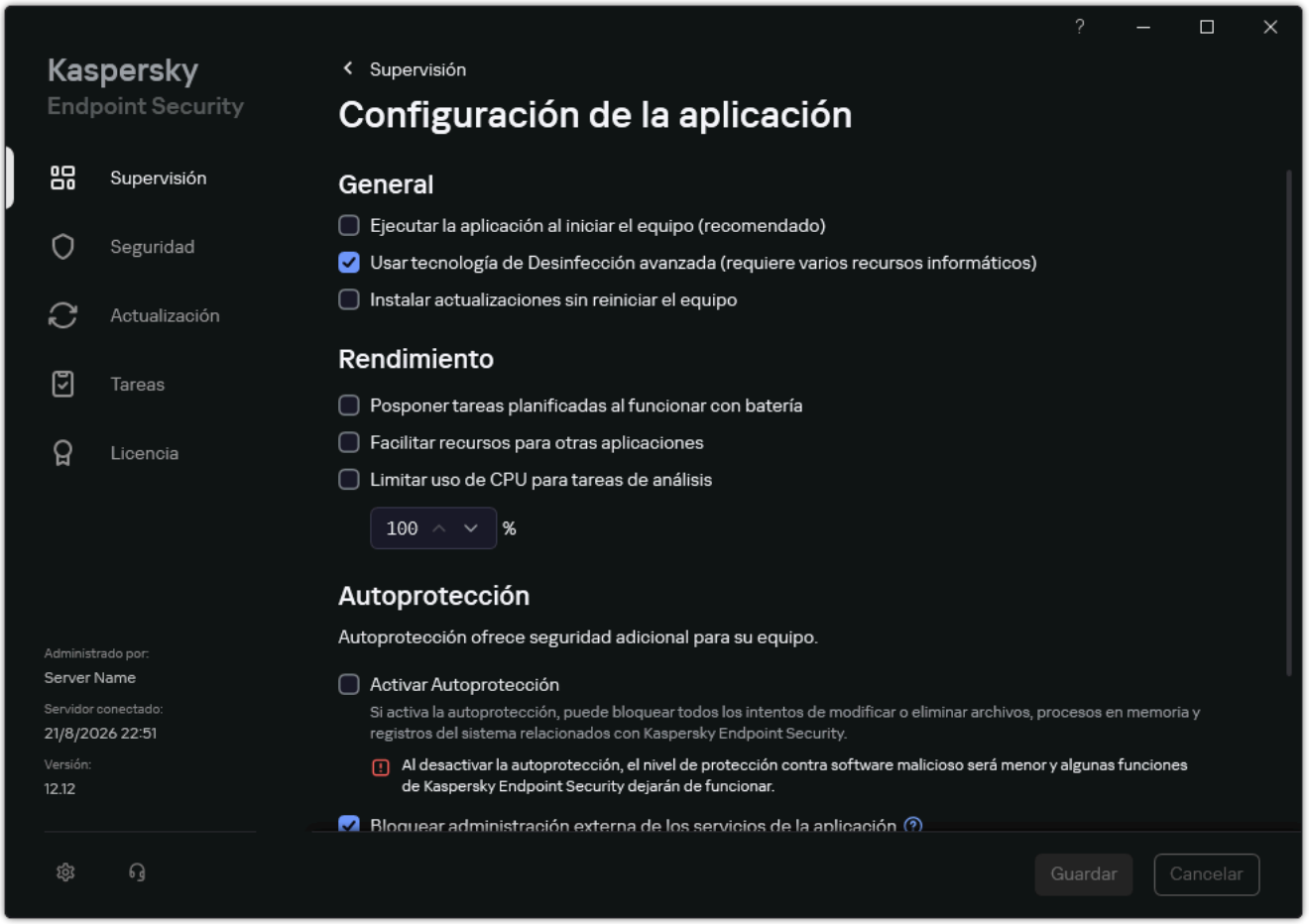
Cómo activar la protección de archivos de volcado y archivos de rastreo en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general → Soporte técnico**.
5. En el bloque de **Información de depuración**, utilice la casilla de verificación **Protección de volcado y archivos de rastreo ACTIVADA** para activar o desactivar la protección de archivos.
6. Guarde los cambios.

Cómo activar la protección de archivos de volcado y archivos de rastreo en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.



Configuración de Kaspersky Endpoint Security para Windows

3. En el bloque de **Información de depuración**, utilice la casilla de verificación **Activar la protección de los archivos de volcado y de rastreo** para activar o desactivar la protección de archivos.
4. Guarde los cambios.

Los archivos de volcado y rastreo que se escribieron mientras la protección estaba activa permanecen protegidos incluso después de que esta función se desactive.

Obtención de datos del sistema operativo (Obtener información del sistema de Kaspersky)

Después de instalar la aplicación Kaspersky Endpoint Security, es posible que el sistema operativo o una aplicación no funcionen correctamente. Existe un conflicto entre la aplicación y el software o los controladores de los componentes del equipo.

Para identificar la causa del problema, el Soporte Técnico de Kaspersky requiere un informe de la utilidad Obtener información del sistema de Kaspersky (en adelante, GSI). Para obtener información detallada sobre el uso de la utilidad, consulte la Base de conocimientos de Kaspersky.

Limitaciones y advertencias

Kaspersky Endpoint Security presenta ciertas limitaciones que no suponen ningún impedimento para el funcionamiento de la aplicación.

Instalación de la aplicación

- Para más información sobre la compatibilidad con los sistemas operativos Microsoft Windows 10, Microsoft Windows Server 2016 y Microsoft Windows Server 2019, visite la Base de conocimientos del Soporte técnico.
- Para más información sobre la compatibilidad con Microsoft Windows 11 y Microsoft Windows Server 2022, visite la Base de conocimientos del Soporte técnico.
- Después de instalarse en un equipo infectado, la aplicación no informa al usuario sobre la necesidad de ejecutar un análisis del equipo. Puede experimentar problemas para activar la aplicación. Para resolver estos problemas, inicie un Análisis de áreas críticas.
- Si se utilizan caracteres que no son ASCII (por ejemplo, letras rusas) en los archivos setup.ini y setup.reg, se recomienda editar el archivo con notepad.exe y guardar el archivo en codificación UTF-16LE. No se admiten otras codificaciones.
- La aplicación no admite el uso de caracteres que no sean ASCII al especificar la ruta de instalación de la aplicación en la configuración del paquete de instalación.
- Cuando la configuración de la aplicación se importa desde un archivo CFG, no se aplica el valor de la configuración que define la participación en Kaspersky Security Network. Después de importar la configuración, lea el texto de la Declaración de Kaspersky Security Network y confirme su consentimiento para participar en Kaspersky Security Network. Puede leer el texto de la Declaración en la interfaz de la aplicación o en el archivo ksn_*.txt ubicado en la carpeta que contiene el kit de distribución de la aplicación.
- Si desea eliminar y volver a instalar el cifrado (FLE o FDE) o el componente de Control de dispositivos, debe reiniciar el sistema antes de la reinstalación.
- Cuando utilice el sistema operativo Microsoft Windows 10, debe reiniciar el sistema después de eliminar el componente Cifrado de archivos (FLE).
- Cuando se eliminen componentes de la aplicación por separado (por ejemplo, mediante la tarea *Cambiar componentes de la aplicación*), es posible que deba reiniciar el equipo.
- En las propiedades de la tarea *Cambiar componentes de la aplicación*, al cambiar el modo de instalación (**Modo independiente** / **Modo combinado**), no se admite la sincronización del conjunto de componentes entre modos. La aplicación sincroniza el conjunto de componentes entre modos después de que vuelva a abrir las propiedades de la tarea.
- La instalación de la aplicación puede terminar con un error que indica que *una aplicación sin nombre o que no se puede leer está instalada en el equipo*. Esto significa que las aplicaciones incompatibles o fragmentos de ellas permanecen en su equipo. Para eliminar artefactos de aplicaciones incompatibles, envíe una solicitud con una descripción detallada de la situación al Soporte técnico de Kaspersky a través de CompanyAccount de Kaspersky.
- Si ha cancelado la eliminación de Kaspersky Endpoint Security, inicie la recuperación de la aplicación después de reiniciar el equipo.

- La aplicación requiere Microsoft .NET Framework 4.0 o posterior. Microsoft .NET Framework 4.6.1 tiene vulnerabilidades. Si está utilizando Microsoft .NET Framework 4.6.1, debe instalar actualizaciones de seguridad. Para obtener detalles sobre las actualizaciones de seguridad de Microsoft .NET Framework, consulte el Sitio web de soporte técnico de Microsoft.

- Si la aplicación no se instaló correctamente con el componente Kaspersky Endpoint Agent seleccionado en un sistema operativo de servidor y aparece la ventana *Error del coordinador de Windows Installer*, consulte las instrucciones en el sitio web de soporte de Microsoft.

- Si la aplicación se instaló localmente en modo no interactivo, use el archivo setup.ini proporcionado para reemplazar los componentes instalados.

- Después de instalar Kaspersky Endpoint Security para Windows en algunas configuraciones de Windows 7, Windows Defender continúa funcionando. Se le recomienda que desactive Windows Defender manualmente para evitar un rendimiento degradado del sistema.

- Al instalar Kaspersky Endpoint Security para Windows en un servidor con las aplicaciones Kaspersky Security para Windows Server (KSWS) y Windows Defender instaladas, debe reiniciar el sistema. Es necesario reiniciar el sistema aunque se haya activado la instalación de la aplicación sin reinicio del sistema. Windows Defender for Windows Server se incluye la lista de software incompatible con Kaspersky Endpoint Security para Windows. Antes de instalar la aplicación, el instalador elimina Windows Defender for Windows Server. La eliminación de software no compatible hace necesario reiniciar el sistema.

- Antes de instalar Kaspersky Endpoint Security para Windows (KES) en un servidor con Kaspersky Security para Windows Server (KSWS) instalado, debe desactivar la protección con contraseña de KSWS. Después de migrar de KSWS a KES, active la protección con contraseña en la configuración de la aplicación.

- Para instalar la aplicación en equipos con Windows 7 o Windows Server 2008 R2 con software Veeam Backup & Replication instalado, quizá necesites reiniciar el equipo y volver a ejecutar la instalación.

- La migración de Kaspersky Small Office Security (KSOS) a Kaspersky Endpoint Security (KES) con la Protección con contraseña activada está disponible desde KSOS compilación 21.16.*.*. Para migrar versiones de KSOS anteriores, debe desactivar Protección con contraseña o eliminar KSOS manualmente. La migración de KSOS a KES con Protección con contraseña desactivada se realiza correctamente.

- No puede instalar Kaspersky Endpoint Security en una unidad extraíble de arranque. Al realizar la instalación, Kaspersky Endpoint Security muestra un mensaje de error: *Ha seleccionado una carpeta o unidad no válida. La aplicación se debe instalar en una unidad de disco duro local*. Si logra instalar la aplicación en una unidad extraíble con herramientas de terceros, esto puede hacer que el sistema operativo falle (BSOD) durante el proceso de arranque. Esto significa que Kaspersky Endpoint Security no es compatible con Windows To Go y soluciones similares. Para analizar un equipo desde una unidad extraíble, puede utilizar la aplicación gratuita Kaspersky Rescue Disk.

- La instalación de Kaspersky Endpoint Security con componentes de red en un servidor de terminal con sesiones RDP multiusuario implica algunas consideraciones especiales. Los sistemas operativos obligan a finalizar todas las sesiones de usuario después de que finalice la sesión de administrador. Para conectarse al servidor de terminal, debe reiniciar el servidor o iniciar sesión en el sistema localmente. Tal comportamiento está dictado por peculiaridades de cómo funciona el sistema operativo Windows.

- Si los complementos web de Kaspersky Endpoint Security para Windows (compilación 12.11.0.2004) y Kaspersky Endpoint Security para Linux (compilación 12.4.0.1354) están instalados en Kaspersky Security Center 16.0 o 16.1, actualizar el complemento web de Kaspersky Endpoint Security para Windows a la compilación 12.11.0.6004 puede provocar fallos en las políticas de Kaspersky Endpoint Security para Linux.

  Posible solución: vaya a la ventana **Configuración → Complementos web** y elimine el complemento web de Kaspersky Endpoint Security para Windows, el complemento web de Kaspersky Endpoint Security para Linux y Unified Protection and Management Plug-in de la lista. A continuación, instale primero el complemento web de Kaspersky Endpoint Security para Linux, seguido del complemento web de Kaspersky Endpoint Security para Windows.

- En la Consola web, la lista de componentes se muestra incorrectamente en las propiedades del paquete de instalación de Kaspersky Endpoint Security 12.11 para Windows. El componente independiente Anti-Cryptor no está disponible en esta versión de la aplicación. La función de protección de carpetas compartidas contra el cifrado externo se incluye en el componente Detección de comportamiento. En Kaspersky Endpoint Security 12.12 para Windows, esta función es un componente aparte. Al mismo tiempo, en la Consola de administración (MMC), la lista de componentes se muestra correctamente.

- Al usar la versión 7.0 o posterior del complemento web, la lista de componentes seleccionados de forma predeterminada para la instalación se muestra incorrectamente en las propiedades del paquete de instalación de Kaspersky Endpoint Security 14.1 y versiones anteriores. Si no se modifica esta lista al crear el paquete de instalación, la aplicación se instalará con el conjunto predeterminado de componentes especificado para la versión correspondiente de la aplicación.

Actualización de la aplicación

- A partir de la versión 11.0.0 de la aplicación, puede instalar el complemento MMC de Kaspersky Endpoint Security para Windows sobre la versión anterior del complemento. Para regresar a una versión anterior del complemento, elimine el complemento actual e instale una versión anterior.

- Al actualizar Kaspersky Endpoint Security 11.0.0 o 11.0.1 para Windows, la configuración de la programación de las tareas locales de las tareas *Actualización de las bases de datos y módulos de la aplicación*, *Análisis de áreas críticas*, *Análisis personalizado* y *Comprobación de integridad de la aplicación* no se guarda.

- En equipos que ejecutan Windows 10 versión 1903 y 1909, las actualizaciones de Kaspersky Endpoint Security 10 para Windows Service Pack 2 Maintenance Release 3 (compilación 10.3.3.275), Service Pack 2 Maintenance Release 4 (compilación 10.3.3.304), 11.0.0 y 11.0.1 con el componente Cifrado de archivos (FLE) instalado pueden terminar con un error. Esto se debe a que el cifrado de archivos no es compatible con estas versiones de Kaspersky Endpoint Security para Windows en Windows 10 versión 1903 y 1909. Antes de instalar esta actualización, se recomienda eliminar el componente de cifrado de archivos.

- La aplicación requiere Microsoft .NET Framework 4.0 o posterior. Microsoft .NET Framework 4.6.1 tiene vulnerabilidades. Si está utilizando Microsoft .NET Framework 4.6.1, debe instalar actualizaciones de seguridad. Para obtener detalles sobre las actualizaciones de seguridad de Microsoft .NET Framework, consulte el Sitio web de soporte técnico de Microsoft.

- Al actualizar Kaspersky Endpoint Security, la aplicación desactiva el uso de KSN hasta que se acepta la Declaración de Kaspersky Security Network. Además, el estado del equipo se puede cambiar a *Crítico* en Kaspersky Security Center; se recibe el evento *Servidores de KSN no disponibles*. Si utiliza Kaspersky Managed Detection and Response, recibirá eventos sobre violaciones del funcionamiento de la solución. El uso de KSN es necesario para el funcionamiento de Kaspersky Managed Detection and Response. Kaspersky Endpoint Security activa el uso de KSN tras la aplicación de la directiva mediante la cual el administrador acepta las condiciones de uso de KSN. Una vez que se ha aceptado la Declaración de Kaspersky Security Network, Kaspersky Endpoint Security reanuda su funcionamiento.

- Tras actualizar Kaspersky Endpoint Security a la versión 11.10.0 o posterior sin reiniciar, el equipo tendrá dos aplicaciones Kaspersky Endpoint Security instaladas. No elimine manualmente la versión anterior de la aplicación. La versión anterior se eliminará automáticamente al reiniciar el equipo.

- Después de actualizar Kaspersky Endpoint Security en un equipo que ejecute Microsoft Windows 11, el menú contextual del archivo puede mostrar elementos para las versiones anteriores y nuevas de la aplicación. Reinicie su equipo dos veces para garantizar el correcto funcionamiento del menú contextual del archivo.

- Si la autoprotección de la aplicación está desactivada y todos los adaptadores de red están detenidos, los componentes de red de la aplicación no funcionarán entre el final de la actualización de la aplicación y el reinicio del equipo. Los componentes de red de la aplicación incluyen Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red, Firewall, Prevención de intrusiones en el host y Control Web. Reinicie el equipo para que la aplicación funcione correctamente.

- El componente Prevención de ataques de BadUSB no funciona entre el final de la actualización de la aplicación y el reinicio del equipo. Reinicie el equipo para que la aplicación funcione correctamente.

- La aplicación no se puede actualizar si no se ha completado el proceso de actualización anterior. Reinicie el equipo para que la aplicación funcione correctamente.

- Una vez que la aplicación se actualiza desde versiones anteriores a Kaspersky Endpoint Security 11 para Windows, se debe reiniciar el equipo.

- Si administra Kaspersky Endpoint Security mediante Kaspersky Security Center Cloud Console, no se permite la actualización de la aplicación localmente. Al actualizar la aplicación localmente, no es posible aceptar el Contrato de procesamiento de datos para Kaspersky Security Center Cloud Console.

Soporte para arquitectura Arm

- No se admite la instalación de Kaspersky Endpoint Security en modo de Light Agent en máquinas virtuales basadas en Arm.

- Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.

- El cifrado de archivos no es compatible con equipos basados en Arm.

- El cifrado de unidades extraíbles no se admite en equipos basados en Arm.

- En equipos que ejecutan Windows 11 para Arm64, EDR Agent no es compatible con Bitdefender Endpoint Security Tools.

- La función de protección de la señal de audio y la de protección del acceso a la cámara web no son compatibles con equipos basados en Arm.

- En equipos basados en Arm, la extensión Protección frente a amenazas en el correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64.

- Kaspersky Endpoint Security no envía a Kaspersky Sandbox objetos destinados a la arquitectura Arm.

- Control de impresión no es compatible con equipos basados en Arm.

- En los equipos basados en Arm, la tarea *Análisis de IOC* tarea admite archivos de correo electrónico solo de los siguientes clientes de correo: versiones de 32 y 64 bits de Outlook 2016 y Outlook 2021, 2024 y 365 para Arm64.

- En los equipos que ejecutan Windows 11 para Arm64, es posible que la autenticación basada en tokens no esté disponible porque el sistema operativo no puede detectar un certificado válido en el token. Este comportamiento se debe a la forma en que el sistema operativo interactúa con el software del token. Por ejemplo, es posible que el sistema operativo no disponga de los controladores necesarios para que el token funcione. En este caso, Kaspersky Endpoint Security tampoco admite la autenticación basada en tokens (Protección con contraseña). Puede utilizar otros métodos de autenticación, como las credenciales de usuario.

Soporte para plataformas de servidores

- En servidores con *deduplicación de datos* habilitada, debe añadir el archivo fsdmhost.exe a la lista de aplicaciones de confianza. Esto ayuda a optimizar el rendimiento de la aplicación y evitar una carga excesiva en la CPU.

- El sistema de archivos ReFS es compatible con limitaciones:

  - Kaspersky Endpoint Security puede procesar incorrectamente los eventos de desinfección de amenazas. Por ejemplo, si la aplicación ha eliminado un archivo malicioso, el informe puede tener una entrada de Objeto no procesado. Al mismo tiempo, Kaspersky Endpoint Security desinfecta las amenazas de acuerdo con la configuración de la aplicación. Kaspersky Endpoint Security también puede crear un duplicado del evento *El objeto se desinfectará al reiniciar* para el mismo objeto.

  - Protección frente a amenazas en archivos puede omitir algunas amenazas. Al mismo tiempo, Análisis antimalware funciona correctamente.

  - Después de iniciar la tarea *Análisis antimalware*, las exclusiones añadidas con iChecker se restablecen al reiniciar el servidor.

  - La tecnología iSwift no es compatible. Kaspersky Endpoint Security no considera las exclusiones de análisis añadidas mediante la tecnología iSwift.

  - Kaspersky Endpoint Security no detecta los archivos eicar.com y susp-eicar.com si el archivo meicar.exe ya existía en el equipo antes de instalar Kaspersky Endpoint Security.

  - Kaspersky Endpoint Security puede mostrar incorrectamente notificaciones de desinfección de amenazas. Por ejemplo, la aplicación puede mostrar una notificación de amenaza para una amenaza previamente desinfectada.

- Las tecnologías Cifrado de archivos (FLE) y Cifrado de disco de Kaspersky (FDE) no son compatibles con las plataformas de servidor. Al mismo tiempo, Kaspersky Endpoint Security puede procesar incorrectamente los eventos de cifrado de datos.

- En los sistemas operativos de servidor, no se muestra ninguna advertencia sobre la necesidad de una desinfección avanzada.

- Se ha excluido la compatibilidad con Microsoft Windows Server 2008. No se admite la instalación de la aplicación en un equipo que ejecute el sistema operativo Microsoft Windows Server 2008.

- Tener Kaspersky Endpoint Security instalado en un servidor con Microsoft Data Protection Manager (DPM) desplegado puede provocar un error funcionamiento de DPM. Está relacionado con las limitaciones de funcionamiento de DPM. Para eliminar errores de funcionamiento, debe añadir unidades del servidor local a exclusiones para el componente Protección frente a amenazas en archivos y las tareas de *Análisis antimalware*.

- El modo Server Core se admite con limitaciones:

  - La interfaz gráfica de usuario local no está disponible, incluidas las notificaciones, las notificaciones emergentes y otros controles de la interfaz. La aplicación no puede mostrar ventanas de mensajes, incluidas las siguientes ventanas:

    - Solicitud de confirmación de la versión de la aplicación y la actualización del módulo;

    - Solicitud de reinicio del equipo;

- Solicitud de credenciales de autenticación del servidor proxy;
- Preguntar para acceder a un dispositivo (Control de Dispositivos).

- Los siguientes componentes no están disponibles: Protección contra amenazas web, Protección contra amenazas de correo, Control web, Prevención de ataques BadUSB.
- Anti-Bridging no está disponible.
- Solo puede aceptar la Declaración de Kaspersky Security Network en la directiva de la aplicación en la consola de Kaspersky Security Center.
- El cifrado de unidad BitLocker solo está disponible con un módulo de plataforma segura (TPM). No se puede usar un PIN/contraseña para el cifrado porque la aplicación no puede mostrar la ventana de solicitud de contraseña para la autenticación previa al inicio. Si el sistema operativo tiene activado el modo de compatibilidad con los Estándares federales de procesamiento de la información (FIPS), instale una unidad extraíble para guardar la clave de cifrado antes de comenzar a cifrar la unidad.

Soporte para plataformas virtuales

- No se admite el Cifrado de disco completo (FDE) en máquinas virtuales Hyper-V.
- No se admite el Cifrado de disco completo (FDE) en las plataformas virtuales Citrix.
- Los sistemas operativos Windows 10 Enterprise multi-session y Windows 11 Enterprise multi-session se admiten con las siguientes limitaciones:
  - Kaspersky Endpoint Security desinfecta las amenazas activas sin avisar al usuario, al igual que cuando se desinfectan las amenazas activas en los servidores. Como el sistema operativo sigue funcionando en modo multisesión, otros usuarios activos pueden perder sus datos si la amenaza no se resuelve inmediatamente.
  - Cifrado de disco completo (FDE) no es compatible.
  - Administrar BitLocker no es compatible.
  - Usar Kaspersky Endpoint Security con unidades extraíbles no es compatible. La infraestructura Microsoft Azure define a las unidades extraíbles como unidades de red.
- No se admite la instalación y el uso del Cifrado de archivos (FLE) en plataformas virtuales Citrix.
- Para admitir la compatibilidad de Kaspersky Endpoint Security para Windows con Citrix PVS, realice la instalación con la opción **Garantizar la compatibilidad con Citrix PVS** activada. Esta opción se puede activar en el Asistente de configuración o mediante el parámetro de línea de comando `/pCITRIXCOMPATIBILITY=1`. En caso de instalación remota, el archivo KUD debe editarse añadiendo el siguiente parámetro: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Antes de iniciar la clonación, debe desactivar la Autoprotección para clonar máquinas virtuales que usan vDisk.

- Al preparar una máquina de plantilla para la imagen maestra de Citrix XenDesktop con Kaspersky Endpoint Security para Windows y el Agente de red de Kaspersky Security Center preinstalados, añada los siguientes tipos de exclusiones al archivo de configuración:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Para obtener detalles sobre Citrix XenDesktop, visite el Sitio web de soporte de Citrix.

- En algunos casos, es posible que un intento de desconectar de forma segura una unidad extraíble no tenga éxito en una máquina virtual implementada en un hipervisor VMware ESXi. Intente desconectar de forma segura el dispositivo una vez más.

- Kaspersky Endpoint Security es compatible con el hipervisor VMware ESXi con las siguientes limitaciones:

  - Kaspersky Endpoint Security puede ser incompatible con los controladores de Guest Introspection (vnetWFP.sys, vnetFLT.sys y otros). Para resolver la incompatibilidad, actualice los controladores a la última versión o desinstálelos.

  - En algunos casos, un intento de eliminar de forma segura un disco extraíble en una máquina virtual puede no tener éxito. Intente desconectar de forma segura el dispositivo una vez más.

- La instalación de Kaspersky Endpoint Security en máquinas virtuales con el agente de Citrix VDA puede finalizar con un error de compatibilidad. Esto sucede porque Citrix Provisioning Services tiene una compatibilidad limitada con las soluciones antivirus. Para conocer las prácticas recomendadas de uso de soluciones antivirus con Citrix Provisioning Services, consulte el sitio web de soporte de Citrix.

- Kaspersky Endpoint Security omite el análisis de una unidad extraíble si la unidad está conectada a una máquina virtual en el hipervisor Citrix (la tarea *Análisis de unidades extraíbles*). En dichos dispositivos, el sistema operativo detecta la unidad extraíble conectada como una unidad de red. En estos casos, puede utilizar la tarea *Análisis personalizado*. El comportamiento de la aplicación en modo estándar y en modo de Light Agent es el mismo.

- Si Kaspersky Endpoint Security está instalado en una máquina virtual de una infraestructura que utiliza la tecnología Citrix App Layering, los archivos que la aplicación detecte como infectados y que tengan el estado *El objeto se eliminará al reiniciar* no se eliminarán automáticamente cuando se reinicie la máquina virtual.

  Para eliminar dichos archivos, debe montar el archivo VHDX que contiene User Layer en el ordenador del administrador de Citrix App Layering y ejecutar un análisis de malware en el disco montado.

- Antes de crear una instantánea de Golden Image de una máquina virtual con Kaspersky Endpoint Security instalado, se recomienda apagar la máquina virtual y crear una instantánea «en frío». Si crea una instantánea mientras la máquina virtual está en ejecución (una instantánea "en caliente"), no se garantiza el correcto funcionamiento de la aplicación.

Compatibilidad con Kaspersky Security Center

- En Kaspersky Security Center Web Console versión 14.1 y anteriores, los nombres de las áreas funcionales de los componentes Inspección de registros y Monitor de integridad de archivos no aparecen correctamente en la sección de configuración de permisos de acceso del usuario de las propiedades del Servidor de administración.

- Tras reparar la aplicación, la protección de la conexión del equipo al Servidor de administración se desactiva. Tras reparar la aplicación, vuelva a ejecutar la tarea *Protección de la conexión al servidor de administración*.

- En la Consola de administración de Kaspersky Security Center, la ventana **Seleccione a un usuario o grupo de usuarios** muestra solo los primeros 50 000 usuarios de la lista de usuarios de Kaspersky Security Center . Consulte la Ayuda de Kaspersky Security Center para más detalles.

- Al buscar dispositivos administrados en la Consola de administración de Kaspersky Security Center, la pestaña **Componentes de la aplicación** puede mostrar simultáneamente varias variantes del nombre del mismo componente de la aplicación, incluidos los nombres correspondientes a versiones anteriores de Kaspersky Endpoint Security. Los nombres de algunos componentes también pueden estar duplicados.

  Para buscar por componente, simplemente debe seleccionar una de las variantes que aparecen. Para obtener más información sobre la detección de dispositivos, consulte la Ayuda de Kaspersky Security Center.

- En Kaspersky Security Center Web Console 15.1 Update 2 con el complemento web de Kaspersky Endpoint Security para Windows versión 12.11 o posterior y el complemento Unified Protection and Management instalado, las condiciones de activación de perfiles de la directiva no funcionan. Kaspersky Security Center no añade a la consola los nuevos dispositivos que cumplen las condiciones de activación del perfil.

Administración de licencias

- Si aparece el mensaje *Error al recibir datos* del sistema, verifique que el equipo en el que está realizando la activación tenga acceso a la red o establezca la configuración de activación a través del servidor proxy de activación de Kaspersky Security Center.

- En la interfaz de la aplicación, la fecha de caducidad de la licencia se muestra en la hora local del equipo.

- La instalación de la aplicación con un archivo llave incrustado en un equipo que tiene acceso a Internet inestable puede resultar en la visualización temporal de eventos que indiquen que la aplicación no está activada o que la licencia no permite el funcionamiento del componente. Esto se debe al hecho de que, durante el proceso de instalación, la aplicación activa primero la licencia de prueba integrada. Requiere acceso a Internet.

- Durante el período de evaluación, la instalación de cualquier actualización o parche de la aplicación en un equipo que tiene un acceso a Internet inestable puede resultar en la visualización temporal de eventos que indiquen que la aplicación no está activada. Esto se debe al hecho de que, durante el proceso de actualización, la aplicación activa primero la licencia de prueba integrada. Requiere acceso a Internet.

- Si la licencia de prueba se activó automáticamente durante la instalación de la aplicación y luego la aplicación se eliminó sin guardar la información de la licencia, la aplicación no se activará automáticamente con la licencia de prueba cuando se reinstale. En este caso, active manualmente la aplicación.

- Si está usando Kaspersky Security Center versión 11 y Kaspersky Endpoint Security versión 14.2, es posible que los informes de rendimiento de componentes no funcionen correctamente. Si instaló componentes de Kaspersky Endpoint Security que no están incluidos en su licencia, el Agente de red puede enviar errores de estado de componentes al registro de eventos de Windows. Para evitar errores, elimine los componentes que no están incluidos en su licencia.

Protección frente a amenazas en el correo

- Al analizar el correo electrónico con la extensión de Protección frente a amenazas en el correo para Microsoft Outlook, recomendamos utilizar el modo caché de Exchange Server (Use Cached Exchange Mode).

- Kaspersky Endpoint Security no es compatible con la versión de 64 bits del cliente de correo electrónico Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de 64 bits de Microsoft Outlook (archivos PST y OST) si hay una versión de 64 bits de Microsoft Outook instalada en el equipo, aunque el correo esté incluido en la cobertura del análisis.

- Kaspersky Endpoint Security no es compatible con el nuevo cliente de correo de Microsoft Outlook.

- Si ha desactivado la desinfección de las amenazas detectadas por Protección frente a amenazas en el correo y recibe un correo electrónico infectado en su buzón de Outlook, Protección frente a amenazas web puede bloquear la comunicación con el servidor Exchange a través de MAPI. A continuación, Protección frente a amenazas web genera un evento de detección de amenazas y lo envía a Kaspersky Security Center. Para restablecer la conexión entre el equipo y el servidor Exchange, debe eliminar manualmente el correo electrónico infectado del buzón de Outlook.

  Al actualizar la versión de la aplicación sin reiniciar el equipo, el nivel de protección de Protección frente a amenazas en el correo se reduce temporalmente (durante un máximo de un minuto). Si recibe un correo electrónico infectado en su buzón de Outlook mientras se actualiza la aplicación, Protección frente a amenazas web también bloqueará la conexión con el servidor Exchange a través de MAPI. Para restablecer la conexión, elimine el correo electrónico infectado del buzón de Outlook.

Motor de reparación

- La aplicación solo puede restaurar archivos en dispositivos que utilizan los sistemas de archivos NTFS o FAT32.
- La aplicación restaura archivos de hasta 100 MB de tamaño.
- La aplicación puede restaurar archivos de las siguientes extensiones: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Los archivos almacenados en unidades de red o en discos CD o DVD regrabables no pueden restaurarse.
- Los archivos cifrados con el sistema de cifrado de archivos EFS no pueden restaurarse. Para más información sobre el funcionamiento de EFS, visite el sitio web de Microsoft.
- La aplicación no controla los cambios que se realizan en los archivos a través de procesos que funcionan en el nivel del núcleo del sistema operativo.

Firewall

- Si una regla de paquete de red o una regla de red de la aplicación especifica nombres DNS, Kaspersky Endpoint Security puede enviar solicitudes al servidor DNS para determinar las direcciones IP de estos recursos. El firewall utiliza direcciones IP para supervisar la actividad de la red. Por lo tanto, la aplicación resuelve los nombres DNS en direcciones IP. Se recomienda usar nombres DNS en reglas solo para equipos LAN o servicios internos.
- Para especificar una regla para todas las direcciones IPv6, añada el rango de direcciones ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. El firewall no admite la máscara ::/0.
- La filtración de paquetes o conexiones por dirección local, interfaz física y período de vida del paquete (TTL) se admite en los siguientes casos:
  - Por dirección local para paquetes salientes o conexiones en reglas de la aplicación para TCP y UDP y reglas de paquetes.
  - Por dirección local para paquetes o conexiones entrantes (excepto UDP) en reglas de bloques de aplicaciones y reglas de paquetes.
  - Por período de vida del paquete (TTL) en reglas de paquetes en bloque para paquetes entrantes o salientes.
  - Por interfaz de red para paquetes entrantes y salientes o conexiones en reglas de paquetes.

- Si ha configurado un adaptador de red o un período de vida (TTL) de paquetes en una regla para paquetes permitidos, la prioridad de esta regla es inferior a la de una regla de aplicaciones bloqueadas. En otras palabras, si se ha bloqueado la actividad de red de una aplicación (por ejemplo, si la aplicación está en el grupo de confianza *Restricción máxima*) no puede permitir actividad de red en la aplicación con una regla de paquetes con esta configuración. En el resto de los casos, la prioridad de una regla de paquetes es superior a una regla de red de la aplicación.

- Al importar reglas de paquetes de Firewall, Kaspersky Endpoint Security puede modificar los nombres de las reglas. La aplicación determina reglas con conjuntos idénticos de parámetros generales: protocolo, dirección, puertos remotos y locales, período de vida del paquete (TTL). Si este conjunto de parámetros generales es idéntico para varias reglas, la aplicación asigna el mismo nombre a estas reglas o añade una etiqueta de parámetro al nombre. De esta manera, Kaspersky Endpoint Security importa todas las reglas de paquetes, pero el nombre de las reglas que tienen configuraciones generales idénticas se puede modificar.

- Si ha activado la notificación de eventos de la aplicación en una reglas de la red, al mover la aplicación a un grupo de confianza diferente, no se aplicarán las restricciones de este grupo de confianza. Por lo tanto, si la aplicación está en el grupo de confianza, no tendrá restricciones de red. Luego activó la notificación de eventos para esta aplicación y la movió al grupo de confianza *No fiable*. El Firewall no aplicará las restricciones de red para esta aplicación. Le recomendamos que primero mueva la aplicación al grupo de confianza apropiado y luego active la notificación de eventos. Si este método no es adecuado, puede configurar manualmente las restricciones para la aplicación en la configuración de las reglas de la red. La restricción se aplica solo a la interfaz local de la aplicación. Mover la aplicación entre grupos de confianza en la directiva funciona correctamente.

- Los componentes de Firewall y Prevención de intrusiones tienen configuración común: derechos de la aplicación y recursos protegidos. Si cambia esta configuración para el Firewall, Kaspersky Endpoint Security aplica automáticamente la nueva configuración a la Prevención de intrusiones. Si, por ejemplo, ha permitido cambios en la configuración general de la directiva de Firewall (el candado está abierto), la configuración de Prevención de intrusiones también se podrá editar.

- Cuando se activa una regla de paquete de red en Kaspersky Endpoint Security 11.6.0 o versiones anteriores, la columna **Nombre de aplicación** en el informe del Firewall siempre muestra el valor *Kaspersky Endpoint Security*. Asimismo, el Firewall bloqueará la conexión al nivel del paquete para todas las aplicaciones. Este comportamiento se ha modificado para Kaspersky Endpoint Security 11.7.0 o versiones posteriores. Se añadió la columna **Tipo de regla** al informe del Firewall. Cuando se activa una regla de paquete de red, el valor en la columna **Nombre de aplicación** permanece vacío.

- Si ha prohibido toda la actividad de red mediante el firewall, el componente Protección frente a amenazas en la red puede detectar un ataque del tipo Análisis de puertos. Esto puede suceder porque la aplicación inicia la Protección frente a amenazas en la red antes que el Firewall para detectar actividad sospechosa en la red.

Prevención de ataques de BadUSB

- Kaspersky Endpoint Security restablece el límite de tiempo para el bloqueo del dispositivo USB cuando el equipo está bloqueado (por ejemplo, cuando se cumple el límite de tiempo para el bloqueo de pantalla). Es decir, si introduce un código de autorización erróneo para el dispositivo USB muchas veces y la aplicación bloquea el dispositivo USB, Kaspersky Endpoint Security le permite repetir el intento de autorización después de desbloquear el equipo. En este caso, Kaspersky Endpoint Security no bloquea el dispositivo USB durante el tiempo especificado en la configuración del componente Prevención de ataques de BadUSB.

- Kaspersky Endpoint Security restablece el límite de tiempo de bloqueo del dispositivo USB cuando la protección del equipo está pausada. Es decir, si introduce un código de autorización erróneo para el dispositivo USB muchas veces y la aplicación bloquea el dispositivo USB, Kaspersky Endpoint Security le permite repetir el intento de autorización después de reanudar la protección del equipo. En este caso, Kaspersky Endpoint Security no bloquea el dispositivo USB durante el tiempo especificado en la configuración del componente Prevención de ataques de BadUSB.

Kaspersky Security Network

- Kaspersky Endpoint Security no admite HTTPS cuando se conecta a KSN Proxy (casilla de verificación **Usar HTTPS** activada en la configuración de conexión de KSN Proxy) si la dirección del servidor incluye letras no latinas (símbolos no ASCII).

- En Kaspersky Security Center, cuando se pasa de utilizar Kaspersky Security Network global a utilizar Kaspersky Security Network (KSPN) privada, o viceversa, la opción de participar en Kaspersky Security Network está desactivada en la directiva del producto. Después del cambio, lea atentamente el texto de la Declaración de Kaspersky Security Network y confirme su consentimiento para participar en KSN. Puede leer el texto de la Declaración en la interfaz de la aplicación o al editar la directiva del producto.

- A partir de Kaspersky Endpoint Security 12.9 para Windows, al cambiar de KPSN a KSN global, debe volver a confirmar su acuerdo con la Declaración de Kaspersky Security Network. Para hacer esto, debe habilitar el uso de Kaspersky Security Network en las propiedades de la directiva o en la interfaz de la aplicación y confirmar su acuerdo con la Declaración de Kaspersky Security Network. Si ya ha utilizado el KSN global, primero debe desactivar el Uso de KSN, luego volver a activarlo y confirmar su aceptación de la Declaración de Kaspersky Security Network. Si no está de acuerdo con la Declaración de Kaspersky Security Network, la aplicación no podrá acceder a los datos de Kaspersky Security Network.

- Kaspersky Endpoint Security no envía archivos de texto (como archivos TXT, CSV, LOG y DOCX sin macros) a Kaspersky Security Network para su análisis. La aplicación envía a analizar archivos que pueden suponer una amenaza para KSN. Estos archivos incluyen archivos ejecutables o archivos que pueden contener código ejecutable (como macros en archivos DOCX). Otros componentes de la aplicación son responsables de analizar archivos de texto. También puede comprobar manualmente la reputación de un archivo de texto desde el menú contextual del archivo. Si un archivo de texto tiene una reputación *No fiable (Kaspersky Security Network)*, la aplicación ignora la acción definida para las amenazas detectadas.

Control de aplicaciones

- Al trabajar con las reglas de Control de aplicaciones, no se recomienda añadir más de 100 000 condiciones de inclusión y exclusión en total para aplicaciones en diferentes categorías, siempre que Kaspersky Endpoint Security se esté ejecutando en un equipo que cumpla con los requisitos mínimos de hardware y funciona con Microsoft Windows 10.

- Solo se admiten archivos en formato ZIP cuando se trabaja con reglas de Control de aplicaciones en Kaspersky Security Center Web Console. No se admiten archivos en otros formatos, como RAR o 7z. No existe tal restricción si trabaja con reglas de Control de aplicaciones en la Consola de administración (MMC).

- Cuando se trabaja con reglas de Control de aplicaciones en Kaspersky Security Center Web Console, el tamaño máximo admitido de un archivo cargado es 104 MB. No existe tal restricción si trabaja con reglas de Control de aplicaciones en la Consola de administración (MMC).

- Cuando se trabaja en Microsoft Windows 10 en modo de lista de aplicaciones rechazadas, las reglas de bloqueo pueden aplicarse incorrectamente, lo que podría causar el bloqueo de aplicaciones que no están especificadas en las reglas.

- Si ha añadido nuevas *reglas de control de aplicaciones predefinidas* al actualizar Kaspersky Endpoint Security, no puede aplicar estas reglas a versiones anteriores de la aplicación.

- Cuando el componente Control de aplicaciones bloquea las aplicaciones web progresivas (PWA), appManifest.xml se indica como la aplicación bloqueada en el informe.

- Al añadir la aplicación estándar Bloc de notas a una regla de Control de aplicaciones para Windows 11, no se recomienda especificar la ruta a la aplicación. En equipos que ejecutan Windows 11, el sistema operativo utiliza Metro Notepad, ubicado en la carpeta `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. En versiones anteriores del sistema operativo, Bloc de notas se encuentra en las siguientes carpetas:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Al añadir Bloc de notas a una regla de Control de aplicaciones, puede especificar el nombre de la aplicación y el hash del archivo desde las propiedades de la aplicación en ejecución, por ejemplo.

- Al migrar la directiva de KSWS al perfil de directiva de KES, el Asistente de conversión por lotes de directivas y tareas (Asistente de migración) cambia el nombre de las categorías de aplicaciones si los nombres de las categorías contienen caracteres prohibidos: `'` `*` `<` `>` `?` `\` `:` `|`. El Asistente de migración reemplaza estos caracteres con caracteres `_`. Por ejemplo, el nombre de la categoría de aplicación `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` se cambia a `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Control de dispositivos

- Kaspersky Endpoint Security puede registrar eventos de conexión y desconexión de dispositivos externos. Los servicios de Windows utilizan la cuenta de usuario del sistema para conectar o desconectar dispositivos. Esto hace que sea imposible saber qué usuario está conectando o desconectando el dispositivo. Kaspersky Endpoint Security especifica la cuenta de usuario SYSTEM en el evento.

- El acceso a los dispositivos de impresión que se añadieron a la lista de confianza es bloqueado por las reglas de bloqueo de dispositivos y bus.

- Para los dispositivos MTP, se admite el control de las operaciones de lectura, escritura y conexión si está utilizando los controladores integrados de Microsoft del sistema operativo. Si un usuario instala un controlador personalizado para trabajar con un dispositivo (por ejemplo, como parte de iTunes o Android Debug Bridge), es posible que el control de las operaciones de lectura y escritura no funcione.

- Cuando se trabaja con dispositivos MTP, las reglas de acceso se cambian después de volver a conectar el dispositivo.

- El componente Control de dispositivos registra eventos relacionados con los dispositivos supervisados, como la conexión y desconexión de un dispositivo, la lectura de un archivo de un dispositivo, la escritura de un archivo en un dispositivo y otros eventos. Kaspersky Endpoint Security registra eventos de desconexión solo para los siguientes tipos de dispositivos: Dispositivos portátiles (MTP), Unidades extraíbles, Disquetes y Unidades de CD/DVD. Para otros tipos de dispositivos, la aplicación no registra eventos de desconexión. La aplicación registra la operación de conexión de un dispositivo a un equipo en todos los tipos de dispositivos.

- Si está añadiendo un dispositivo a la lista de confianza según una máscara de modelo y usa caracteres que están incluidos en la ID pero no en el nombre del modelo, estos dispositivos no se añaden. En una estación de trabajo, estos dispositivos se añadirán a la lista de confianza según una máscara de identificación.

- Cuando la aplicación se actualiza sin reiniciar el equipo, el Control de dispositivos no aplica reglas de acceso a los dispositivos que se vuelven a conectar. Sin embargo, si el dispositivo estaba conectado antes de la actualización, el Control de dispositivos aplica las reglas correctamente. Reinicie el equipo para que la aplicación funcione correctamente con los dispositivos que se vuelven a conectar.

- En equipos con Kaspersky Endpoint Security versión 12.0 instalada, el modo de acceso a impresoras **Permitir y no registrar** para el tipo de dispositivo **Impresoras de red** se denomina **Depende del bus de conexión** si se aplica la directiva de Kaspersky Endpoint Security versión 12.1 en el equipo. En estos modos la aplicación realiza las mismas acciones. En Kaspersky Endpoint Security versión 12.1, el modo de acceso para las impresoras de red tiene el nombre correcto **Permitir y no registrar**.

- A partir de Kaspersky Endpoint Security 12.0 para Windows, la aplicación permite configurar reglas de impresión para impresoras (control de impresión). Después de instalar la aplicación con control de impresión o actualizar la aplicación a una versión con control de impresión, debe reiniciar el equipo. Hasta que el equipo se reinicia, Kaspersky Endpoint Security no aplica reglas de impresión y solo puede controlar el acceso a las impresoras. Si reiniciar el equipo afecta negativamente los flujos de trabajo en su organización, puede reiniciar solo el servicio spoolsv (Cola de impresión). Control de impresión no es compatible con equipos basados en Arm.

- A partir de la versión Kaspersky Endpoint Security 12.0 para Windows, se ha añadido la compatibilidad con el protocolo WPA3 para dispositivos de tipo **wifi**. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en un equipo, el protocolo WPA2 se selecciona en equipos con Kaspersky Endpoint Security versión 11.11.0 y anteriores; WPA2/WPA3 se selecciona con las versiones 12.0 a 12.1; WPA3 se selecciona con las versiones 12.2 y posteriores.

- Los dispositivos Apple se consideran dispositivos portátiles (MTP) y dispositivos de iTunes. El sistema operativo puede identificar de forma incorrecta la conexión del dispositivo Apple y no determinar dicho dispositivo Apple como dispositivo portátil (MTP). Por tanto, el dispositivo Apple no estará disponible en el administrador de archivos, pero sí se podrá acceder a él en la aplicación iTunes. Como resultado, Kaspersky Endpoint Security controlará el acceso al dispositivo Apple solo en la aplicación iTunes. Para acceder al dispositivo Apple como dispositivo portátil (MTP), debe ir al Administrador de dispositivos y eliminar el controlador USB del dispositivo móvil de Apple de la lista de controladores USB. Tras reiniciar el equipo, el sistema operativo identificará el dispositivo Apple como dispositivo portátil (MTP) y el dispositivo de iTunes. Kaspersky Endpoint Security controlará el acceso al dispositivo tanto en la aplicación iTunes como en el administrador de archivos.

- En Kaspersky Endpoint Security 12.3 para Windows, la configuración de acceso es diferente para el tipo de dispositivo **Bluetooth**. Si especificaste el valor **Depende del bus de conexión** en la versión anterior de la aplicación, después de actualizar la aplicación a la versión 12.3, el valor configurado cambia a **Permitir y no registrar**. Esto no altera el comportamiento del dispositivo.

- Control de dispositivos admite dispositivos con Bluetooth solo a través de la pila Bluetooth de Microsoft Windows. Control de dispositivos puede funcionar incorrectamente con pilas Bluetooth de terceros.

- Si el dispositivo Bluetooth oculta o falsifica su clase de dispositivo (COD), Control de Dispositivo puede funcionar incorrectamente.

- En equipos con Windows 7 o Windows 8 con determinados controladores de llave Bluetooth Realtek, quizá no sea posible permitir únicamente la conexión de dispositivos Bluetooth como dispositivos de entrada (clase HID). Es decir, si prohíbe el acceso a dispositivos Bluetooth en la configuración de la aplicación y añade dispositivos de entrada a las exclusiones, Control de dispositivos puede impedir el acceso a todos los dispositivos Bluetooth.

Control Web

- Los formatos OGV y WEBM no son compatibles.

- El protocolo RTMP no es compatible.

- Control web solo admite WSL1. La aplicación no controla el tráfico WSL2.

Control de anomalías adaptativo

- Se recomienda crear exclusiones automáticamente según el evento. Al añadir manualmente una exclusión, añada el carácter * al comienzo de la ruta al especificar el objeto de destino.
- El **Informe de reglas de Control de anomalías adaptativo activado** no se puede generar si la muestra incluye al menos un evento cuyo nombre contiene más de 260 caracteres.
- No se admite la adición de exclusiones del repositorio Activación de reglas del Control de anomalías adaptativo si las propiedades de un objeto o proceso tienen un valor que supera los 256 caracteres (por ejemplo, una ruta a un objeto objetivo). Puede añadir una exclusión manualmente en la configuración de directivas. También puede añadir una exclusión en el informe sobre las reglas del Control de anomalías adaptativo.
- Kaspersky Security Center 15.1 no puede generar un informe **Informe de estado de reglas de Control de anomalías adaptativo** detallado para una regla específica.
- Las reglas de Control de anomalías adaptativo solo están disponibles en el idioma en el que se instaló el complemento web. Si cambia el idioma de la interfaz, Web Console muestra una lista de reglas vacía. Para acceder a las reglas, vuelva a seleccionar el idioma en el que se instaló el complemento web.

Cifrado de unidad (FDE)

- Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.
- El cifrado de unidad de BitLocker no es compatible con equipos que ejecutan Windows Home.
- Con el Cifrado de unidad BitLocker, el usuario puede cambiar manualmente la contraseña de autenticación mediante la API de Windows. En estos casos, BitLocker ignora los requisitos de contraseña establecidos en la directiva de Kaspersky Endpoint Security. En otras palabras, el usuario puede establecer cualquier contraseña.
- Después de instalar la aplicación, debe reiniciar el sistema operativo para que el cifrado del disco duro funcione correctamente.
- El agente de autenticación no admite jeroglíficos ni los caracteres especiales | y \.
- Para obtener un rendimiento óptimo del equipo después del cifrado, es necesario que el procesador sea compatible con el conjunto de instrucciones AES-NI (Intel Advanced Encryption Standard New Instructions). Si el procesador no es compatible con las AES-NI, es posible que se disminuya el rendimiento del equipo.
- Cuando hay procesos que intentan acceder a dispositivos encriptados antes de que la aplicación les haya otorgado acceso a dichos dispositivos, la aplicación muestra una advertencia que indica que dichos procesos deben terminarse. Si los procesos no se pueden terminar, vuelva a conectar los dispositivos cifrados.
- Las ID únicas de los discos duros se muestran en las estadísticas de cifrado del dispositivo en formato invertido.
- No se recomienda formatear los dispositivos mientras se cifran.
- Cuando se conectan simultáneamente varias unidades extraíble a un equipo, la directiva de cifrado se puede aplicar a una sola unidad extraíble. Cuando se vuelven a conectar los dispositivos extraíbles, la directiva de cifrado se aplica correctamente.
- Es posible que el cifrado no se inicie en un disco duro muy fragmentado. Desfragmentar el disco duro.

- Cuando los discos duros están cifrados, la hibernación se bloquea desde el momento en que comienza la tarea de cifrado hasta el primer reinicio de un equipo con Microsoft Windows 7/8/8.1/10, y después de la instalación del cifrado del disco duro hasta el primer reinicio de los sistemas operativos Microsoft Windows 8/8.1/10. Cuando se descifran los discos duros, la hibernación se bloquea desde el momento en que la unidad de arranque se descifra por completo hasta el primer reinicio del sistema operativo. Cuando la opción Inicio rápido está activada en Microsoft Windows 8/8.1/10, el bloqueo de la hibernación evita que apague el sistema operativo.

- Los equipos que cuenten con el sistema operativo Windows 7 no permiten cambiar la contraseña durante la recuperación cuando el disco está cifrado con tecnología BitLocker. Una vez que se introduce la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no le solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, no es posible establecer un nuevo código PIN o contraseña. Este problema proviene de las particularidades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.

- No se recomienda utilizar la herramienta xbootmgr.exe con proveedores adicionales activados. Por ejemplo, Dispatcher, Network o Drivers.

- No se admite el formateo de una unidad extraíble cifrada en un equipo que tenga instalado Kaspersky Endpoint Security para Windows.

- No se admite el formateo de una unidad extraíble cifrada con el sistema de archivos FAT32 (la unidad se muestra como cifrada). Para formatear una unidad, vuelva a formatearla con el sistema de archivos NTFS.

- No pueden coexistir varios agentes de descarga en un equipo cifrado.

- Si se intenta restaurar una imagen de un disco GPT de arranque en un estado no cifrado, el sistema operativo puede hacer que el sistema operativo no funcione. Para evitar esto, siga estas recomendaciones:

  - Descifre completamente el disco antes de restaurar la imagen desde la copia de seguridad.

  - Utilice la copia sector por sector al crear la imagen.

  - Elimine los datos de los primeros sectores del disco cifrado antes de restaurar la imagen y reinicializar el disco.

- Es imposible acceder a una unidad extraíble que se cifró previamente en un equipo diferente cuando se cumplen todas las condiciones siguientes de manera simultánea:

  - No hay conexión con el servidor de Kaspersky Security Center.

  - El usuario está intentando la autorización con un nuevo token o contraseña.

  Si ocurre una situación similar, reinicie el equipo. Una vez reiniciado el equipo, se otorgará acceso a la unidad extraíble encriptada.

- Es posible que el Agente de autenticación no admita el descubrimiento de dispositivos USB cuando el modo xHCI para USB está activado en la configuración del BIOS.

- El Cifrado de disco de Kaspersky (FDE) para la parte SSD de un dispositivo que se utiliza para almacenar en caché los datos utilizados con más frecuencia no es compatible con dispositivos SSHD.

- No se admite el cifrado de discos duros en sistemas operativos Microsoft Windows 8/8.1/10 de 32 bits que se ejecutan en modo UEFI.

- Reinicie el equipo antes de volver a cifrar un disco duro descifrado.

- El cifrado del disco duro no es compatible con Kaspersky Anti-Virus para UEFI. No se recomienda utilizar el cifrado del disco duro en equipos que tengan instalado Kaspersky Anti-Virus para UEFI.

- La creación de cuentas del Agente de autenticación basadas en cuentas de Microsoft se admite con las siguientes limitaciones:

  - La tecnología Single Sign-On no es compatible.

  - No se admite la creación automática de cuentas del Agente de autenticación si se selecciona la opción de crear cuentas para los usuarios que inician sesión en el sistema en los últimos N días.

- Si el nombre de una cuenta del Agente de autenticación tiene el formato `<domain>/<Windows account name>`, después de cambiar el nombre del equipo, también debe cambiar los nombres de las cuentas que se crearon para los usuarios locales de ese equipo. Por ejemplo, imagine que hay un usuario local `Ivanov` en el equipo `Ivanov` y una cuenta de Agente de autenticación con el nombre `Ivanov/Ivanov` ha sido creado para este usuario. Si el nombre del equipo `Ivanov` se ha cambiado a `Ivanov-PC`, debe cambiar el nombre de la cuenta del Agente de autenticación para el usuario `Ivanov` de `Ivanov/Ivanov` a `Ivanov-PC/Ivanov`. Puede cambiar el nombre de la cuenta con la tarea de administración de cuentas del Agente de autenticación. Antes de que se haya cambiado el nombre de la cuenta, es posible la autenticación en el entorno previo al arranque utilizando el nombre antiguo (por ejemplo, `Ivanov/Ivanov`).

- Si a un usuario se le permite acceder a un equipo que fue encriptado usando la tecnología Cifrado de disco de Kaspersky solo usando un token, y este usuario necesita completar el procedimiento de recuperación de acceso, asegúrese de que este usuario tenga acceso basado en contraseña a este equipo después de que es acceso al equipo encriptado ha sido restaurado. Es posible que no se guarde la contraseña que estableció el usuario al restaurar el acceso. En este caso, el usuario tendrá que volver a completar el procedimiento para restaurar el acceso al equipo encriptado la próxima vez que se reinicie el equipo.

- Al descifrar un disco duro con la Herramienta de recuperación FDE, el proceso de descifrado puede terminar con un error si los datos del dispositivo de origen se sobrescriben con los datos descifrados. Parte de los datos del disco duro permanecerán cifrados. Se recomienda elegir la opción para guardar los datos descifrados en un archivo en la configuración de descifrado del dispositivo cuando se utiliza la Herramienta de recuperación FDE.

- Si se ha cambiado la contraseña del Agente de autenticación, aparecerá un mensaje con el texto *Su contraseña se ha cambiada correctamente.Aparece la opción Haga clic en Aceptar* y el usuario reinicia el equipo, la nueva contraseña no se guarda. La contraseña anterior se debe utilizar para la autenticación posterior en el entorno previo al arranque.

- El cifrado de disco es incompatible con la tecnología Intel Rapid Start.

- El cifrado de disco es incompatible con la tecnología ExpressCache.

- En algunos casos, al intentar descifrar una unidad cifrada con la Herramienta de recuperación FDE, la herramienta detecta por error el estado del dispositivo como "no cifrado" después de que se completa el procedimiento "Solicitud-Respuesta". El registro de la herramienta muestra un evento que indica que el dispositivo se descifró correctamente. En este caso, debe reiniciar el procedimiento de recuperación de datos para descifrar el dispositivo.

- Una vez que el complemento de Kaspersky Endpoint Security para Windows se actualiza en Web Console, las propiedades del equipo del cliente no muestran la clave de recuperación de BitLocker hasta que se reinicia el servicio de Web Console.

- Para ver las otras limitaciones del soporte de cifrado de disco completo y una lista de dispositivos para los que el cifrado de discos duros es compatible con restricciones, consulte la Base de conocimientos de soporte técnico.

Cifrado de archivos (FLE)

- El cifrado de archivos no es compatible con equipos basados en Arm.
- El cifrado de archivos y carpetas no es compatible con sistemas operativos Microsoft Windows Embedded.
- Una vez instalada la aplicación, debe reiniciar el sistema operativo para que el cifrado de archivos y carpetas funcione correctamente.
- La aplicación admite el cifrado de archivos solo en dispositivos con sistemas de archivos NTFS y FAT32. Si un archivo cifrado se transfiere a un dispositivo con un sistema de archivos no soportado (por ejemplo, exFAT), el archivo de dicho dispositivo no se cifrará y se podrá modificar.
- Si un archivo cifrado se almacena en un equipo que tiene la funcionalidad de cifrado disponible y usted accede al archivo desde un equipo donde el cifrado no está disponible, se proporcionará acceso directo a este archivo. Un archivo cifrado que se almacena en una carpeta de red en un equipo que tiene la función de cifrado disponible se copia en forma descifrada a un equipo que no tiene la función de cifrado disponible.
- Se recomienda descifrar los archivos que se cifraron con Encrypting File System antes de cifrar los archivos con Kaspersky Endpoint Security para Windows.
- Después de cifrar un archivo, su tamaño aumenta en 4 KB.
- Después de cifrar un archivo, el atributo de *Archivo comprimido* se establece en las propiedades del archivo.
- Al copiar el archivo descifrado, por ejemplo, en un medio extraíble, el archivo puede permanecer cifrado. Esto puede suceder porque cuando el administrador de archivos (por ejemplo, explorer.exe) intenta obtener acceso al archivo cifrado, guarda el hash del archivo en una lista especial del proceso. Después de descifrar el archivo, cuando el administrador de archivos intenta obtener acceso al archivo, el proceso busca el hash del archivo en la lista. Si se encuentra el hash, Kaspersky Endpoint Security deja el archivo cifrado. Para evitar esto, debe borrar la lista del proceso. El sistema operativo borra automáticamente la lista del proceso a medida que se completa. Puede vaciar manualmente la lista. Para hacerlo, puede reiniciar el equipo, reiniciar el proceso que está usando para obtener acceso al archivo (por ejemplo, explorer.exe), o usar un administrador de archivos diferente que no haya usado para acceder al archivo cifrado archivo.
- Si un archivo que se descomprime de un archivo cifrado tiene el mismo nombre que un archivo que ya existe en su equipo, el nuevo archivo que se descomprimió de un archivo cifrado sobrescribirá al último. No se notifica al usuario sobre la operación de sobrescritura.
- Antes de descomprimir un archivo cifrado, asegúrese de tener suficiente espacio libre en el disco para alojar los archivos desempaquetados. Si no tiene suficiente espacio en disco, el desempaquetado del archivo puede completarse pero los archivos pueden dañarse. En este caso, es posible que Kaspersky Endpoint Security no muestre ningún mensaje de error.
- La interfaz de Administrador de archivos portátil no muestra mensajes sobre errores que ocurren durante su funcionamiento.
- Kaspersky Endpoint Security para Windows no inicia el Administrador de archivos portátil en un equipo que tiene instalado el componente Cifrado de archivos.

- No puede usar el Administrador de archivos portátil para acceder a una unidad extraíble si las siguientes condiciones se cumplen simultáneamente:

  - No hay conexión con Kaspersky Security Center;
  - Kaspersky Endpoint Security para Windows no está instalado en el equipo.
  - El cifrado de datos (FDE o FLE) no se ha realizado en el equipo.

  El acceso es imposible aunque se conozca la contraseña del Administrador de archivos portátil.

- Cuando se utiliza el cifrado de archivos, la aplicación es incompatible con el cliente de correo Sylpheed.

- Kaspersky Endpoint Security para Windows no es compatible con la regla de restricción de acceso a archivos cifrados para algunas aplicaciones. Esto se debe al hecho de que algunas operaciones de archivo las realiza una aplicación de terceros. Por ejemplo, el copiado de archivos lo realiza el administrador de archivos, no la aplicación en sí. De esta forma, si el acceso a los archivos cifrados se deniega al cliente de correo Outlook, Kaspersky Endpoint Security permitirá al cliente de correo acceder al archivo cifrado si el usuario ha copiado archivos en el mensaje de correo electrónico mediante el portapapeles o usando la función de arrastrar y soltar. La operación de copiado la realiza un administrador de archivos, para el que no se especifican las reglas de restricción de acceso a archivos cifrados (es decir, se permite el acceso).

- Cuando las unidades extraíbles están cifradas con soporte para modo portátil, el control de antigüedad de la contraseña no se puede desactivar.

- No se admite el cambio de la configuración del archivo de página. El sistema operativo utiliza los valores predeterminados en lugar de los valores de los parámetros especificados.

- Utilice la extracción segura cuando trabaje con unidades extraíbles cifradas. No podemos garantizar la integridad de los datos si la unidad extraíble no se extrae de forma segura.

- Una vez que los archivos están cifrados, sus originales no cifrados se eliminan de forma segura.

- No se admite la sincronización de archivos offline mediante el Client-Side Caching (CSC). Tampoco se admite el cifrado de archivos sin conexión ni la tecnología Branch Caching sobre SMB para servidores. Se recomienda prohibir la administración offline de recursos compartidos a nivel de directiva del grupo. Los archivos que están en modo offline se pueden editar. Después de la sincronización, es posible que se pierdan los cambios realizados en un archivo offline.

- No se admite la creación de un archivo comprimido cifrado en la raíz del disco duro del sistema.

- Puede experimentar problemas al acceder a archivos cifrados a través de la red. Se recomienda mover los archivos a una fuente diferente o asegurarse de que el equipo que se utiliza como servidor de archivos esté administrado por el mismo Servidor de administración de Kaspersky Security Center.

- Cambiar la distribución del teclado puede hacer que se bloquee la ventana de introducción de la contraseña para un archivo autoextraíble cifrado. Para resolver este problema, cierre la ventana de introducción de la contraseña, cambie la distribución de teclado en su sistema operativo y vuelva a introducir la contraseña para el archivo comprimido cifrado.

- Cuando se utiliza el cifrado de archivos en sistemas que tienen varias particiones en un disco, se recomienda utilizar la opción que determina automáticamente el tamaño del archivo pagefile.sys. Una vez que el equipo se reinicia, el archivo pagefile.sys puede moverse entre las particiones del disco.

- Después de aplicar las reglas de cifrado de archivos, incluidos los archivos de la carpeta *Mis documentos*, asegúrese de que los usuarios a los que se les ha aplicado el cifrado puedan acceder correctamente a los archivos cifrados. Para hacerlo, haga que cada usuario inicie sesión en el sistema cuando haya una conexión a Kaspersky Security Center disponible. Si un usuario intenta acceder a archivos cifrados sin una conexión a Kaspersky Security Center, el sistema puede bloquearse.

- Si los archivos del sistema se incluyen de alguna manera en el alcance del cifrado de archivos, es posible que en los informes aparezcan eventos relacionados con errores al cifrar estos archivos. Los archivos especificados en estos eventos no están realmente encriptados.

- Los procesos PICO no son compatibles.

- No se admiten las rutas que distinguen entre mayúsculas y minúsculas. Cuando se aplican reglas de cifrado o reglas de descifrado, las rutas de los eventos del producto se muestran en minúsculas.

- No se recomienda cifrar los archivos que utiliza el sistema al inicio. Si estos archivos están cifrados, un intento de acceder a archivos cifrados sin una conexión a Kaspersky Security Center puede hacer que el sistema se bloquee o genere solicitudes de acceso a los archivos no cifrados.

- Si los usuarios trabajan conjuntamente con un archivo en la red bajo reglas FLE a través de aplicaciones que utilizan el método de asignación de archivo a memoria (como WordPad o FAR) y aplicaciones diseñadas para trabajar con archivos grandes (como Notepad ++), el archivo en forma no cifrada se puede bloquear indefinidamente sin la capacidad de acceder a él desde el equipo en el que reside.

- Kaspersky Endpoint Security no cifra los archivos que se encuentran en el almacenamiento en la nube de OneDrive o en otras carpetas que tienen OneDrive como nombre. Kaspersky Endpoint Security también bloquea la copia de archivos cifrados a carpetas de OneDrive si esos archivos no se añaden a la regla de descifrado.

- Cuando se instala el componente de cifrado de archivos, la gestión de usuarios y grupos no funciona en modo WSL (Windows Subsystem for Linux).

- Cuando está instalado el componente de cifrado de nivel de archivo, no se admite POSIX (Portable Operating System Interface) para cambiar el nombre y eliminar archivos.

- No se recomienda cifrar os archivos temporales, ya que esto puede provocar la pérdida de datos. Por ejemplo, Microsoft Word crea archivos temporales al procesar un documento. Si se cifran los archivos temporales, pero no el archivo original, el usuario puede recibir un error de *Acceso denegado* al intentar guardar el documento. Además, Microsoft Word puede llegar a guardar el archivo, pero no se podrá abrir el documento la próxima vez que se intente hacerlo, lo cual quiere decir que se perderán los datos. Para evitar la pérdida de datos, deberá excluir la carpeta de archivos temporales de las reglas de cifrado.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- No puede analizar un objeto puesto en cuarentena como resultado de la tarea *Mover archivo a Cuarentena*.

- No es posible colocar en cuarentena un Alternate Data Stream (ADS) que supere los 4 MB. Kaspersky Endpoint Security omite todos los ADS de este tamaño sin notificar al usuario.

- Kaspersky Endpoint Security no ejecuta tareas *Análisis de IOC* en las unidades de red si la ruta de la carpeta en las propiedades de la tarea comienza con la letra de una unidad. Kaspersky Endpoint Security solo admite el formato de ruta UNC para tareas de *Análisis de IOC* en las unidades de red. Por ejemplo, `\\server\shared_folder`.

- Para asegurar que la tarea *Análisis de IOC* que utiliza los términos de EmailItem funciona correctamente, el complemento web de Kaspersky Endpoint Security debe actualizarse a la última versión.

- En los equipos basados en Arm, la tarea *Análisis de IOC* tarea admite archivos de correo electrónico solo de los siguientes clientes de correo: versiones de 32 y 64 bits de Outlook 2016 y Outlook 2021, 2024 y 365 para Arm64.

- La importación de un archivo de configuración de una aplicación termina en un error si la configuración de integración con Kaspersky Sandbox está activada en el archivo de configuración. Antes de exportar los ajustes de la aplicación, desactive Kaspersky Sandbox. Luego, realice el procedimiento de exportación/importación. Una vez importado el archivo de configuración, active Kaspersky Sandbox.

- Al importar una directiva desde un archivo KLP, no se aplica el valor del parámetro que determina la aceptación de los términos y condiciones del Contrato de Kaspersky Detection and Response Expert. Como resultado, después de importar la directiva, Kaspersky Endpoint Security no realiza las funciones del Agente de EDR. Para que el Agente de EDR funcione, abra la directiva, cambie cualquier parámetro y guarde la configuración de la directiva.

- Cuando se detecta un indicador de compromiso durante la ejecución de una tarea de *Análisis de IOC*, la aplicación pone en cuarentena solo un archivo para el término FileItem. La cuarentena de archivos para otros términos no es compatible.

- Se requiere el complemento web Kaspersky Endpoint Security para Windows 11.7.0 o versiones posteriores para gestionar los detalles de la alerta. Los detalles de la alerta son necesarios al trabajar con soluciones Endpoint Detection and Response (EDR Optimum y EDR Expert). Los detalles de la alerta están disponibles solo en Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console.

- Es posible que migrar la configuración de [KES + KEA] a la configuración de [KES + agente integrado] se complete con un error de eliminación de la aplicación Kaspersky Endpoint Agent. El error de eliminación de la aplicación se corrigió en la versión más reciente de Kaspersky Endpoint Agent. Para eliminar Kaspersky Endpoint Agent, reinicie el equipo y cree una tarea de eliminación de la aplicación.

- La configuración [KES+KEA+agente integrado] no es compatible. Esta configuración afecta a la interacción entre las aplicaciones y la solución Detection and Response que se despliega en nuestra organización. Además, usar Kaspersky Endpoint Agent y el agente integrado en el mismo equipo puede provocar una duplicación de la telemetría y un aumento de la carga en el equipo y en la red. Tras migrar a la configuración [KES+agente integrado], asegúrese de que Kaspersky Endpoint Agent se ha eliminado del equipo. Si Kaspersky Endpoint Agent sigue funcionando tras la migración, desinstale la aplicación manualmente (por ejemplo, usando la tarea *Desinstalar aplicación en remoto*).

  El instalador le permite desplegar Kaspersky Endpoint Agent en un equipo que tenga instalados Kaspersky Endpoint Security y el agente integrado. Kaspersky Endpoint Agent y el agente integrado también se pueden instalar en un equipo como resultado de la tarea *Cambiar componentes de la aplicación*. El comportamiento depende de las versiones de Kaspersky Endpoint Security y Kaspersky Endpoint Agent.

- Al generar detalles de alerta, la aplicación proporciona información sobre la amenaza detectada, incluidos los hashes de los archivos modificados. Kaspersky Endpoint Security calcula el hash del archivo mientras genera los detalles de la alerta. Tenga en cuenta que el hash original del archivo cuando se generó el evento de modificación del archivo puede no ser el mismo que el hash calculado cuando se generaron los detalles de la alerta.

- El agente integrado, EDR (KATA), reanuda el aislamiento de red de un equipo después de reiniciarlo, incluso si el período de aislamiento ha expirado. Para evitar el aislamiento repetido del equipo, debe desactivar el aislamiento de la red en la consola de Kaspersky Anti Targeted Attack Platform.

- Recomendamos actualizar la aplicación después de que finalice el aislamiento de la red. Después de actualizar Kaspersky Endpoint Security, se puede detener el aislamiento de la red.

- Los agentes integrados para EDR (KATA), EDR Optimum y EDR Expert no son compatibles entre sí. Por lo tanto, la activación del agente integrado de EDR con una licencia independiente de Kaspersky Endpoint Detection and Response Add-on se puede omitir si ha activado Kaspersky Endpoint Security con una funcionalidad de EDR diferente. Por ejemplo, la activación del agente integrado de EDR (KATA) con una licencia independiente se omite si activó Kaspersky Endpoint Security con la licencia [KES+EDR Optimum].

- En Kaspersky Endpoint Security versión 12.1, el agente EDR (KATA) integrado no admite los siguientes metarchivos para la tarea *Obtener metarchivos NTFS*: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Se ha agregado compatibilidad para estos metaarchivos a Kaspersky Endpoint Security versión 12.2.

- Al migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para la solución Kaspersky Anti Targeted Attack Platform (EDR), es posible que encuentre errores al conectar el equipo a los servidores del Nodo Central. El motivo es que el asistente de migración de Web Console omite las siguientes configuraciones de directivas y no las migra:

  - Prohibición de modificar la configuración **Configuración de conexión** ("candado").

    De forma predeterminada, la configuración se puede modificar (el "candado" está abierto). Por lo tanto, la configuración no se aplica en el equipo. Debe prohibir la modificación de la configuración y cerrar el "candado".

  - Contenedor criptográfico.

    Si está utilizando la autenticación bidireccional para conectarse a los servidores del Nodo Central, debe volver a agregar el contenedor criptográfico. El asistente de migración migra correctamente el certificado TLS del servidor.

  El Asistente de migración de directivas y tareas de la Consola de administración (MMC) migra todas las configuraciones a la solución Kaspersky Anti Targeted Attack Platform (EDR).

- El estado de activación de la aplicación aparece de forma incorrecta si la aplicación se instala en el modo Endpoint Detection and Response Agent para admitir la solución Kaspersky Managed Detection and Response sin conexión a Kaspersky Security Center. Una vez descargado el archivo BLOB, el área de notificaciones de la barra de tareas de Windows muestra un estado incorrecto: *La aplicación no está activada*. Sin embargo, la interfaz de la aplicación muestra el estado de activación correctamente. Reinicie el equipo para que la aplicación funcione correctamente.

- Kaspersky Endpoint Security permite la integración con la solución Kaspersky Anti Targeted Attack Platform mediante el componente EDR (KATA) o Endpoint Sensor (no compatible). Tenga en cuenta que solo puede usar uno de los componentes para interactuar con Kaspersky Anti Targeted Attack Platform. Para ver el estado del componente, abra las propiedades del equipo en la Consola de administración (MMC), en la sección **Aplicaciones**, abra las propiedades de Kaspersky Endpoint Security para Windows y vaya a la sección **Componentes**. Las siguientes consideraciones especiales se aplican a la visualización del estado de los componentes para la interacción con Kaspersky Anti Targeted Attack Platform:

  - Para el complemento de administración 12.0 y versiones anteriores, la aplicación muestra el estado actual de **Endpoint Server**. En Kaspersky Endpoint Security 12.0 y versiones anteriores, el componente EDR (KATA) no está disponible. El componente EDR (KATA) se introdujo en la versión 12.1.

  - Para el complemento de administración 12.1 y versiones posteriores, la aplicación muestra el estado general de **Endpoint Detection and Response (KATA)**, que puede significar el estado del Endpoint Sensor o el estado del componente EDR (KATA). Esto depende de la versión de la aplicación instalada en el equipo del usuario y de los componentes disponibles que puede usar para interactuar con Kaspersky Anti Targeted Attack Platform.

- A partir de Kaspersky Endpoint Security versión 12.6 y posteriores, Kaspersky Security Center Web Console versión 14.2 y anteriores no muestran correctamente el nombre del componente **Endpoint Detection and Response (KATA)** en las propiedades del equipo. En lugar del componente **Endpoint Detection and Response (KATA)**, la aplicación muestra el nombre del componente **Endpoint Detection and Response Expert (KATA EDR)**. Para ver la lista de componentes, abra las propiedades del equipo en Web Console, en la sección **Aplicaciones**, abra las propiedades de Kaspersky Endpoint Security para Windows y vaya a la sección **Componentes**. A partir de Kaspersky Security Center Web Console versión 15.1 y posteriores, la aplicación muestra correctamente el nombre del componente.

- Al actualizar el complemento de administración de Kaspersky Endpoint Detection and Response a la versión 15.3 instalada en las versiones 14.0–14.2 de Web Console, los detalles de la alerta se muestran incorrectamente. Para que los detalles de la alerta funcionen correctamente, reinicie el Servidor de administración de Kaspersky Security Center.

- El complemento de administración de Kaspersky Endpoint Detection and Response versión 15.4 y posterior no es compatible con Kaspersky Security Center versión 14.0. Después de actualizar el complemento de administración, los detalles de la alerta se muestran incorrectamente.

- Las soluciones de clase Kaspersky Extended Detection and Response (XDR) versión 1.4 no son compatibles con el complemento web de Kaspersky Endpoint Security para Windows versión 12.12 o posteriores. Puede dejar la versión actual del complemento web o actualizar la solución XDR a la versión 2.0 o posterior.

- Kaspersky Endpoint Security no envía a Kaspersky Sandbox objetos destinados a la arquitectura Arm.

- Kaspersky Endpoint Security admite hasta 10 000 reglas de filtrado de eventos de inclusión y exclusión de EDR Expert (on-premises) en total.

- Las reglas de filtrado de eventos de EDR Expert (on-premises) no se pasarán de la directiva a los dispositivos administrados que ejecuten Kaspersky Endpoint Security versión 14.0 o anterior si se supera el límite admitido de reglas de filtrado almacenadas. La aplicación mostrará la advertencia correspondiente.

- Las versiones 12.11–14.1 de Kaspersky Endpoint Security para Windows no admiten los siguientes eventos de telemetría de EDR Expert (on-premises):

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change
  - SCCM Deployment Task
  - Smb Connection Open

  A partir de la versión 14.2, Kaspersky Endpoint Security admite todos estos eventos de telemetría de EDR Expert (on-premises), excepto LDAP Attribute Change.

Otras limitaciones

- Los sistemas operativos Windows, a partir de la versión 11 24H2, admiten la tecnología UDP Receive Segment Coalescing Offload (URO). La tecnología está activada de forma predeterminada si hay una tarjeta de red compatible y controladores instalados en el equipo. Desactivar URO en el equipo de un usuario puede reducir significativamente el rendimiento de la aplicación.

- Kaspersky Endpoint Security es compatible con el subsistema WSL (Windows Subsystem for Linux) con restricciones:

  - WSL 1. La aplicación supervisa el tráfico de red y detecta amenazas a través de HTTP / HTTPS. Debido al hecho de que Kaspersky Endpoint Security utiliza su propio certificado para analizar conexiones HTTPS seguras, el funcionamiento de algunas aplicaciones de terceros puede interrumpirse.

  - WSL 2. La aplicación no es compatible con WSL 2.

- Si la aplicación devuelve errores o se bloquea durante el funcionamiento, puede reiniciarse automáticamente. Si la aplicación encuentra errores recurrentes que provocan el fallo de la aplicación, esta realiza las operaciones siguientes:

  1. Desactiva las funciones de control y protección (la funcionalidad de cifrado permanece activa).

  2. Informa al usuario de que las funciones se han desactivado.

  3. Trata de restablecer la funcionalidad de la aplicación después de actualizar las bases de datos antivirus o de aplicar las actualizaciones de los módulos de la aplicación.

- Las direcciones web que se añadir a la lista de confianza pueden procesarse incorrectamente.

- En la consola de Kaspersky Security Center, no puede guardar un archivo en el disco desde la carpeta **Avanzado → Repositorios → Amenazas activas**. Para guardar el archivo, debe desinfectar el archivo infectado. Al realizar la desinfección, la aplicación guarda una copia del archivo en la Copia de seguridad. Ahora, puede guardar el archivo en el disco desde la carpeta **Avanzado → Repositorios → Copia de seguridad**.

- La herencia de la configuración de la transferencia de datos al Servidor de administración (**Configuración general → Informes y Almacenamiento → Transferencia de datos al Servidor de administración**) difiere de la herencia de otras configuraciones. Si permitió cambiar la configuración de transmisión de datos en la directiva (el "bloqueo" está abierto), esta configuración se restablecerá a los valores predeterminados en las propiedades del equipo local en la consola si no se definieron antes. Si esta configuración se definió de forma previa, se restaurarán sus valores. Al eliminar una directiva, la configuración se hereda de la misma manera. En estos casos, se heredan de la directiva otras configuraciones en las propiedades del equipo local.

- Kaspersky Endpoint Security supervisa el tráfico HTTP que cumple con los estándares RFC 2616, RFC 7540, RFC 7541, RFC 7301. Si Kaspersky Endpoint Security detecta otro formato de intercambio de datos en el tráfico HTTP, la aplicación bloquea esta conexión para evitar que se descarguen archivos maliciosos de Internet.

- Kaspersky Endpoint Security evita la comunicación a través del protocolo QUIC. Los navegadores usan el protocolo de transporte estándar (TLS o SSL) independientemente de que la compatibilidad con QUIC esté activada en el navegador o no.

- Cuando el software de terceros funciona con la biblioteca Libcurl, pueden producirse errores de conexión TLS. Esto puede estar relacionado con el certificado de Kaspersky que utiliza Kaspersky Endpoint Security para analizar conexiones cifradas. Para continuar trabajando, puede desactivar la validación de certificados para software de terceros (no recomendado) o agregar un cuerpo de certificado de Kaspersky al almacenamiento de certificados cURL. Para obtener información detallada, consulte la Base de conocimiento de Kaspersky.

- Cuando se inicia Kaspersky Endpoint Security para Windows por primera vez, es posible que una aplicación firmada digitalmente se coloque temporalmente en el grupo incorrecto. Después, la aplicación firmada digitalmente se incluirá en el grupo correcto.

- Durante una nueva exploración de un objeto malicioso que fue bloqueado por software de terceros, no se notifica al usuario cuando se detecta nuevamente la amenaza. El evento de nueva detección de amenazas se muestra en el informe de la aplicación y en el informe de Kaspersky Security Center.

- El informe de Kaspersky Security Center sobre el cifrado de dispositivos no incluirá información sobre los dispositivos que se cifraron con Microsoft BitLocker en plataformas del servidor o en estaciones de trabajo en las que no está instalado el componente Control de dispositivos.

- No se puede activar la visualización de todas las entradas del informe en Kaspersky Security Center Web Console. En Web Console, solo se puede cambiar la cantidad de entradas que se muestra en los informes. De manera predeterminada, Kaspersky Security Center Web Console muestra 1000 entradas por informe. Puede activar la visualización de todas las entradas de los informes en Consola de administración (MMC).

- No se puede establecer la visualización de más de 1000 entradas por informe en Kaspersky Security Center Console. Si establece un valor superior a 1000, Kaspersky Security Center Console mostrará 1000 entradas por informe.

- Cuando se utiliza una jerarquía de directivas, se puede acceder a la configuración de la sección Cifrado de unidades extraíbles en una directiva secundaria para editarla, si la directiva principal prohíbe la modificación de esa configuración.

- Debe activar Audit Logon en la configuración del sistema operativo para garantizar el correcto funcionamiento de las exclusiones para la protección de carpetas compartidas frente al cifrado externo.

- Si la protección de carpetas compartidas está activada, Kaspersky Endpoint Security para Windows supervisa los intentos de cifrar las carpetas compartidas para cada sesión de acceso remoto que se inició antes del inicio de Kaspersky Endpoint Security para Windows, incluso si el equipo desde el que se inició la sesión de acceso remoto ha sido añadido a las exclusiones. Si no desea que Kaspersky Endpoint Security para Windows supervise los intentos de cifrar las carpetas compartidas para las sesiones de acceso remoto que se iniciaron desde un equipo que se añadió a las exclusiones y que se iniciaron antes del inicio de Kaspersky Endpoint Security para Windows, finalice y vuelva a establecer la sesión de acceso remoto o reinicie el equipo en el que está instalado Kaspersky Endpoint Security para Windows.

- Si la tarea de actualización se ejecuta con los permisos de una cuenta de usuario específica, los parches del producto no se descargarán cuando se actualice desde una fuente que requiera autorización.

- Es posible que la aplicación no se inicie debido a un rendimiento insuficiente del sistema. Para resolver este problema, use la opción Ready Boot o aumente el tiempo de espera del sistema operativo para iniciar los servicios.

- La aplicación no puede funcionar en Safe Mode de Windows.

- No podemos garantizar el funcionamiento de Audio Control hasta después del primer reinicio luego de instalar la aplicación.

- En la Consola de administración (MMC), en la configuración de la Prevención de intrusiones en la ventana para configurar los permisos de las aplicaciones, el botón **Eliminar** no está disponible. Puede eliminar una aplicación de un grupo de confianza mediante el menú contextual de la aplicación.

- En la interfaz local de la aplicación, en la configuración de Prevención de intrusiones, los permisos de la aplicación y los recursos protegidos no están disponibles para su visualización si el equipo está gestionado por una directiva. Los controles de desplazamiento, búsqueda, filtro y otras ventanas no están disponibles. Puede ver los permisos de la aplicación en las propiedades de la directiva en Kaspersky Security Center Console.

- Cuando los archivos de seguimiento rotados están activados, no se crean seguimientos para el componente AMSI y el complemento de Outlook.
- Los seguimientos de rendimiento no se pueden recopilar manualmente en Windows Server 2008.
- No se admiten seguimientos de rendimiento para el tipo de seguimiento "Reiniciar".
- El registro de volcado no es compatible con el proceso Pico.
- Deshabilitar la opción **Desactivar administración externa de los servicios del sistema** no le permitirá detener el servicio de la aplicación que se instaló con el parámetro `AMPPL=1` (de forma predeterminada, el valor del parámetro se establece en `1` comenzando con la versión del sistema operativo Windows 10RS2). El parámetro `AMPPL` con un valor de `1` habilita el uso de la tecnología de Procesos de protección para el servicio del producto.
- Para ejecutar un análisis personalizado de una carpeta, el usuario que inicia el análisis personalizado debe tener los permisos para leer los atributos de esta carpeta. De lo contrario, el análisis personalizado de carpetas será imposible y terminará con un error.
- Cuando una regla de análisis definida en una directiva incluye una ruta sin el carácter `\` al final, por ejemplo, `C:\folder1\folder2`, el análisis se ejecutará para la ruta `C:\folder1\`.
- Si utiliza directivas de restricción de software (Software Restriction Policies, SRP), es posible que el equipo no cargue (muestre una pantalla negra). Para evitar disfunciones, debe permitir el uso de bibliotecas de aplicaciones en las propiedades de SRP. En las propiedades de SRP, añada la regla con el nivel de seguridad **Sin restricciones** para el archivo khkum.dll (elemento de menú **Nueva regla de hash**). El archivo se encuentra en la carpeta `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Si ha seleccionado este método, debe además desactivar la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación** de la configuración de la tarea *Actualización* de Kaspersky Endpoint Security. Para obtener más información sobre SRP, consulte la documentación de Microsoft.

  También puede desactivar SRP y usar el componente Control de aplicaciones de Kaspersky Endpoint Security para controlar el uso de la aplicación.
- Si el equipo pertenece a un dominio del objeto de directivas de grupo (Group Policy Object, GPO) de Microsoft con el parámetro DriverLoadPolicy establecido en 8 (solo Good only), reiniciar el equipo con Kaspersky Endpoint Security instalado provoca un BSOD. Para que se produzca un fallo, el parámetro Early Launch Antimalware (ELAM) de la directiva de grupo debe estar establecido en 1 (Good and unknown). La configuración de ELAM se encuentra en la directiva, en: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.
- No se admite la administración de la configuración del complemento de Outlook a través de Rest API.
- La configuración de ejecución de tareas para un usuario específico no se puede transferir entre dispositivos a través de un archivo de configuración. Después de aplicar la configuración desde un archivo de configuración, especifique manualmente el nombre de usuario y la contraseña.
- Después de instalar una actualización, la tarea de comprobación de integridad no funciona hasta que se reinicia el sistema para aplicar la actualización.

- Cuando el nivel de seguimiento rotado se cambia a través de la utilidad de diagnóstico remoto, Kaspersky Endpoint Security para Windows muestra incorrectamente un valor en blanco para el nivel de seguimiento. Sin embargo, los archivos de seguimiento se escriben según el nivel de seguimiento correcto. Cuando el nivel de seguimiento rotado se cambia a través de la interfaz local de la aplicación, el nivel de seguimiento se modifica correctamente pero la utilidad de diagnóstico remoto muestra incorrectamente el nivel de seguimiento que fue definido por última vez por la utilidad. Esto puede hacer que el administrador no tenga información actualizada sobre el nivel de seguimiento actual, y la información relevante puede estar ausente de los seguimientos si un usuario cambia manualmente el nivel de seguimiento en la interfaz local de la aplicación.

- En la interfaz local, la configuración de Protección con contraseña no permite cambiar el nombre de la cuenta de administrador (de forma predeterminada, KLAdmin). Para cambiar el nombre de la cuenta de administrador, debe deshabilitar Protección con contraseña y, a continuación, habilitar Protección con contraseña y especificar un nuevo nombre de la cuenta de administrador.

- Cuando la aplicación Kaspersky Endpoint Security se instala en un servidor Windows Server 2019, no es compatible con Docker. La implementación de contenedores Docker en un equipo con Kaspersky Endpoint Security provoca un bloqueo (BSOD).

- Si Kaspersky Endpoint Security está instalado en un servidor del SQL Server DBMS, la aplicación envía solicitudes a la instancia del servidor. Esto es necesario para analizar los trabajos del agente de SQL Server y evitar la ejecución de trabajos maliciosos. Kaspersky Endpoint Security utiliza la cuenta de usuario SQL Server para analizar trabajos. La aplicación envía solicitudes al servidor al analizar la memoria del sistema y después de actualizar las bases de datos antivirus.

- La compatibilidad de Kaspersky Endpoint Security y el software de Secret Net Studio es limitada:

  - La aplicación Kaspersky Endpoint Security no es compatible con el componente antivirus del software de Secret Net Studio.

    La aplicación no se puede instalar en un equipo donde se implementa Secret Net Studio con el componente antivirus. Para que la interoperabilidad sea posible, debe eliminar el componente antivirus de Secret Net Studio.

  - La aplicación Kaspersky Endpoint Security no es compatible con el componente protección de disco y cifrado de datos del software de Secret Net Studio.

    La aplicación no se puede instalar en un equipo en el que se implementa Secret Net Studio con el componente de protección del disco y cifrado de datos. Para que la interoperabilidad sea posible, debe eliminar el componente protección del disco y cifrado de datos de Secret Net Studio.

  - Secret Net Studio no es compatible con el componente Cifrado de archivos (FLE) de Kaspersky Endpoint Security.

    Cuando instala Kaspersky Endpoint Security con el componente Cifrado de archivos (FLE), Secret Net Studio puede funcionar con errores. Para garantizar la interoperabilidad, debe eliminar el componente Cifrado de archivos (FLE) de Kaspersky Endpoint Security.

- Al importar reglas de Control de integridad del sistema, la aplicación verifica el ID y el nombre de la regla. Si los ID de las reglas son los mismos, Kaspersky Endpoint Security reemplaza las reglas existentes con la nueva regla. Al exportar reglas, la aplicación asigna los ID automáticamente. Pueden existir reglas con ID idénticos; por ejemplo, si ha editado manualmente los archivos XML de reglas exportados. Si los ID de las reglas son únicos, pero los nombres de las reglas son los mismos, Kaspersky Endpoint Security añade `(1)`, y así sucesivamente, al nombre de la regla.

- A partir de la versión 12.11 de Kaspersky Endpoint Security para Windows, no es posible ver la configuración de una directiva principal que esté abierta en un grupo secundario en Web Console. Web Console también muestra una advertencia: *Esta directiva es heredada. Solo puede editar la configuración de la directiva en el grupo de administración en el que se creó*.

- Las notificaciones emergentes de más de 256 caracteres no aparecen en la Consola de administración (MMC).

- Los nombres de los componentes de la directiva y del paquete de instalación pueden ser diferentes. Por ejemplo, Endpoint Detection and Response Expert (on-premises) puede denominarse Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises), Kaspersky Anti Targeted Attack Platform Integration. Los nombres de los componentes también pueden diferir según la versión de la aplicación.

Glosario

Administrador de archivos portátil

Aplicación que brinda una interfaz para trabajar con archivos cifrados en unidades extraíbles cuando las funciones de cifrado necesarias para ello no están disponibles en el equipo.

Agente de autenticación

Interfaz que le permite completar la autenticación para acceder a discos duros cifrados y cargar el sistema operativo después del cifrado del disco duro de arranque.

Agente de red

Un componente de Kaspersky Security Center que permite la interacción entre el servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es común a todas las aplicaciones de Kaspersky que se ejecutan con Windows. Las versiones dedicadas del Agente de red están destinadas para aplicaciones que se ejecutan con otros sistemas operativos.

Archivador

Uno o varios archivos comprimidos en un solo archivo comprimido. Se requiere una aplicación especializada llamada "archivador" para comprimir y descomprimir datos.

Archivo de IOC

Un archivo que contiene un conjunto de indicadores de compromiso (IOC) que la aplicación intenta hacer coincidir para contar una detección. La probabilidad de detección puede ser mayor si se encuentran coincidencias exactas con múltiples archivos de IOC para el objeto como resultado del análisis.

Archivo infectable

Un archivo que, por su estructura o formato, puede ser utilizado por intrusos como "contenedor" y distribuidor de un código malicioso. Como regla, estos son archivos ejecutables, con extensiones de archivo como .com, .exe y .dll. Existe un riesgo realmente elevado de intrusión de código malicioso en estos archivos.

Archivo infectado

Un archivo que contiene código malicioso (se ha detectado código de software malicioso [malware] conocida durante el análisis del archivo). Kaspersky no recomienda utilizar estos archivos, ya que podrían infectar el equipo.

Autenticación de Kerberos

Mecanismo de autenticación mutua por parte del cliente y el servidor antes de establecer una conexión entre ellos, lo que permite comunicarse a través de redes no seguras. El mecanismo se basa en un ticket, que el usuario obtiene de un centro de autenticación de confianza.

Base de datos de direcciones web maliciosas

Lista de direcciones web cuyo contenido puede considerarse como peligroso. Los expertos de Kaspersky se encargan de crear la lista. Se actualiza con regularidad y está incluida en el kit de distribución de la aplicación de Kaspersky.

Base de datos de direcciones web phishing

Una lista de direcciones web que los especialistas de Kaspersky han determinado como relacionadas con phishing. La base de datos se actualiza con regularidad y forma parte del kit de distribución de la aplicación de Kaspersky.

Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas de la seguridad del equipo que conoce Kaspersky a la fecha en la que se publica la base de datos antivirus. Las firmas de bases de datos antivirus ayudan a detectar código malicioso en objetos analizados. Los autores de estas bases de datos antivirus son especialistas de Kaspersky, que las actualizan cada hora.

Certificado de licencia

Un documento que Kaspersky transfiere al usuario junto con el archivo clave o el código de activación. Contiene información sobre la licencia que se concede al usuario.

Clave activa

Clave que utiliza la aplicación actualmente.

Cloud Discovery

Cloud Discovery administra el acceso de los usuarios a los servicios en la nube. Los servicios en la nube incluyen, por ejemplo, Microsoft Teams, Salesforce y Microsoft Office 365. Los servicios en la nube se agrupan en categorías; por ejemplo *uso compartido de archivos*, *mensajería*, *correo electrónico*.

Cobertura de protección

Objetos que son analizados constantemente por el componente Protección frente a amenazas básicas cuando este se ejecuta. Las coberturas de protección de los distintos componentes tienen distintas propiedades.

Cobertura del análisis

Objetos que Kaspersky Endpoint Security analiza mientras realiza una tarea de análisis.

Desinfección

Método de procesamiento de objetos infectados que da lugar a la recuperación completa o parcial de datos. No se pueden desinfectar todos los objetos infectados.

Emisor del certificado

El centro de certificación que emitió el certificado.

Falsa alarma

Una falsa alarma se produce cuando la aplicación Kaspersky notifica un archivo que no está infectado como infectado, porque la firma del archivo es similar a la de un virus.

Forma normalizada de la dirección de un recurso web

La forma normalizada de la dirección de un recurso web es una representación textual de la dirección de un recurso web obtenido a través de la normalización. La *normalización* es un proceso mediante el que la representación textual de la dirección de un recurso web cambia de acuerdo con reglas concretas (por ejemplo, exclusión del nombre de usuario, contraseña y puerto de conexión de la representación textual de la dirección del recurso web; además, la dirección del recurso web cambia de mayúsculas a minúsculas).

En cuanto al funcionamiento de componentes de protección, el fin de la normalización de las direcciones de recursos web consiste en evitar analizar varias veces direcciones de sitios web que puedan diferir en la sintaxis, pese a ser físicamente equivalente.

Ejemplo:

Forma no normalizada de una dirección: www.Example.com\.

Forma normalizada de una dirección: www.example.com.

Grupo de administración

Un conjunto de dispositivos que comparten funciones comunes y un conjunto de aplicaciones de Kaspersky instaladas en ellos. Los dispositivos se agrupan de modo que se puedan administrar de forma práctica como una sola unidad. Un grupo puede incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada una de las aplicaciones instaladas en el grupo.

IOC

Indicador de compromiso. Un conjunto de datos sobre una actividad u objeto malicioso.

Light Agent

Componente Kaspersky Endpoint Security for Virtualization Light Agent. Se instala en cada máquina virtual que debe protegerse.

Máscara

Representación del nombre de un archivo y de su extensión mediante comodines.

Las máscaras de archivos pueden contener cualquier carácter que se permita en los nombres de archivos, incluidos comodines:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. La máscara ** solo puede usarse para crear exclusiones del análisis.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Módulo de plataforma segura

Un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del equipo e interactúa con todos los otros componentes del sistema a través del bus de hardware.

Objeto OLE

Un archivo adjunto o un archivo incrustado en otro archivo. Las aplicaciones de Kaspersky permiten analizar objetos OLE en busca de virus. Por ejemplo, si incluye una tabla de Microsoft Excel® en un documento de Microsoft Office Word, la aplicación analizará la tabla como un objeto OLE.

OpenIOC

Estándar abierto de descripciones de indicadores de compromiso (IOC) basado en XML y que incluye más de 500 indicadores de compromiso diferentes.

Servidor de integración

Componente Kaspersky Endpoint Security for Virtualization Light Agent. Interactúa entre los componentes de Kaspersky Endpoint Security y la infraestructura virtual.

SVM

Máquina virtual segura: una máquina virtual especial en la que está instalado el servicio de servidor de análisis (Servidor de protección, un componente de Kaspersky Endpoint Security for Virtualization Light Agent).

Tarea

Funciones realizadas por la aplicación de Kaspersky como tareas, por ejemplo: Protección de archivos de tiempo real, Análisis completo de dispositivo, Actualización de bases de datos.

Apéndices

Esta sección contiene información que complementa el cuerpo del documento.

Apéndice 1. Configuración de la aplicación

Puede utilizar una directiva, tareas o la interfaz de la aplicación para configurar Kaspersky Endpoint Security. En las secciones correspondientes se proporciona información detallada sobre los componentes de la aplicación.

Protección frente a amenazas en archivos

El componente Protección frente a amenazas en archivos le permite evitar la infección del sistema de archivos del equipo. De forma predeterminada, el componente Protección frente a amenazas en archivos reside permanentemente en la RAM del equipo y analiza todos los archivos abiertos, guardados o ejecutados en tiempo real. Este componente analiza archivos en todas las unidades del equipo, incluidas las unidades conectadas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

El componente analiza los archivos a los que accede el usuario o la aplicación. Si se detecta un archivo malicioso, Kaspersky Endpoint Security bloquea la operación del archivo. A continuación, la aplicación desinfecta o elimina el archivo malicioso, en función de la configuración del componente Protección frente a amenazas en archivos.

Cuando se intenta acceder a un archivo cuyo contenido reside en el almacenamiento en la nube de OneDrive, Kaspersky Endpoint Security descarga el contenido y lo analiza.

Configuración de componente Protección frente a amenazas en archivos

Parámetro	Descripción
Nivel de seguridad *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Para Protección frente a amenazas en archivos, Kaspersky Endpoint Security puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*. • **Alto**. Si se selecciona este nivel de seguridad de archivos, el componente Protección frente a amenazas en archivos realiza el control más estricto de todos los archivos abiertos, guardados y ejecutados. El componente Protección frente a amenazas en archivos analiza todos los tipos de archivos en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. También analiza archivos comprimidos, paquetes de instalación y objetos OLE incrustados. • **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección frente a amenazas en archivos solo analiza los formatos de archivos especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo y en los objetos de OLE incrustados. El componente Protección frente a amenazas en archivos no analiza los archivos ni los paquetes de instalación. • **Bajo**. La configuración de este nivel de seguridad garantiza la velocidad máxima de análisis. El componente Protección frente a amenazas en archivos solo analiza los archivos con extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. El componente Protección frente a amenazas en archivos no analiza los archivos compuestos.
Tipos de archivos *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	**Todos los archivos**. Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones). **Archivos analizados por formato**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares. **Archivos analizados por extensión**. Si se activa este parámetro, la aplicación analiza únicamente los archivos infectables. El formato de archivo se determina en función de su extensión.

Parámetro	Descripción
Cobertura del análisis	Contiene objetos que son analizados por el componente Protección frente a amenazas en archivos. Los objetos de análisis pueden ser discos duros, unidades extraíbles o de red, carpetas, archivos individuales o máscaras que engloben varios archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza los archivos ejecutados en cualquier disco duro, en las unidades de red o en las unidades extraíbles. El alcance de protección de estos objetos no puede modificarse ni eliminarse. Solo puede excluir un objeto (por ejemplo, una unidad extraíble) de los análisis.
Aprendizaje automático y análisis de firmas *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	El método de aprendizaje automático y análisis de firmas utiliza la base de datos de Kaspersky Endpoint Security, que contiene descripciones de las amenazas conocidas y métodos para erradicarlas. La protección que utiliza este método proporciona el nivel de seguridad mínimo aceptable. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.
Análisis heurístico *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
Acción al detectar una amenaza	**Desinfectar; eliminar si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si falla la desinfección, la aplicación elimina el archivo. **Desinfectar; bloquear si la desinfección falla**. Si se elige esta opción, la aplicación automáticamente trata de desinfectar el archivo infectado que se detecta. Si la desinfección falla, la aplicación bloquea este archivo. **Bloquear**. Si se selecciona esta opción, la aplicación bloquea automáticamente el archivo infectado sin intentar desinfectarlo ni eliminarlo. Antes de intentar desinfectar o eliminar un archivo infectado, la aplicación crea una copia de seguridad del archivo en caso de que necesite restaurarlo o que sea posible desinfectarlo en el futuro.
Analizar solamente archivos nuevos y modificados	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
Analizar archivos	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos en formatos de Microsoft Office	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
Analizar archivos de formatos de correo electrónico	Analiza archivos con formato de correo electrónico. La aplicación analiza archivos MSG y EML. Los archivos con formato de correo electrónico también incluyen objetos OLE y archivos MHT. Kaspersky Endpoint Security analiza los archivos con formato de correo electrónico que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
No descomprimir archivos compuestos grandes	Si esta casilla de verificación está marcada, la aplicación no analiza archivos compuestos cuyo tamaño exceda el valor especificado. Si esta casilla de verificación no está marcada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.

Parámetro	Descripción
Descomprimir archivos compuestos en segundo plano	Si la casilla de verificación está marcada, la aplicación proporciona acceso a archivos compuestos cuyo tamaño sea superior al valor especificado antes de analizar estos archivos. En este caso, Kaspersky Endpoint Security extrae y analiza los archivos compuestos en segundo plano. La aplicación proporciona acceso a archivos compuestos cuyo tamaño sea inferior a este valor solo después de extraer y analizar estos archivos. Si la casilla de verificación no está marcada, la aplicación proporciona acceso a archivos compuestos solo después de extraer y analizar archivos de cualquier tamaño.
Modo de análisis *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Kaspersky Endpoint Security analiza los archivos a los que accede el usuario, el sistema operativo o una aplicación que se ejecuta en la cuenta del usuario. **Modo inteligente**. En este modo, Protección frente a amenazas en archivos analiza un objeto en función de un análisis de las acciones aplicadas al objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo. **Al acceder y modificar**. En este modo, Protección frente a amenazas en archivos analiza objetos cuando se intenta abrirlos o modificarlos. **Al acceder**. En este modo, Protección frente a amenazas en archivos analiza objetos solo tras intentar abrirlos. **Al ejecutar**. En este modo, Protección frente a amenazas en archivos solo analiza objetos tras intentar ejecutarlos.
Usar tecnología iSwift *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
Usar tecnología iChecker *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).
Pausar la Protección frente a amenazas en archivos *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Esto detiene temporalmente y automáticamente el funcionamiento de Protección frente a amenazas en archivos a la hora especificada o al trabajar con las aplicaciones especificadas.
Análisis de operaciones de archivos ejecutadas en contenedores de Windows	Si se detecta una amenaza dentro de un contenedor, la aplicación aplica la acción seleccionada para el componente Protección frente a amenazas en archivos. **Detener el contenedor si la desinfección falla**. Es posible que la aplicación no tenga suficientes derechos de lectura y escritura para el objeto detectado. En ese caso, es imposible desinfectar o eliminar el objeto detectado. Si esta casilla de verificación está seleccionada, la aplicación bloquea el objeto detectado y detiene el contenedor. Si esta casilla está desactivada, la aplicación solo bloquea el objeto detectado. **No analizar operaciones de archivos ejecutadas en contenedores de Windows**. Si la casilla de verificación está seleccionada, la aplicación analiza el contenedor solo cuando se inicia. Si la casilla de verificación está desactivada, la aplicación analiza el contenedor continuamente en tiempo real.

Protección frente a amenazas web

El componente Protección frente a amenazas web evita la descarga de archivos maliciosos de internet y también bloquea la conexión a sitios web maliciosos y de phishing. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

Kaspersky Endpoint Security analiza tráfico HTTP, HTTPS y FTP. Kaspersky Endpoint Security analiza direcciones IP y URLs.

Para utilizar Protección frente a amenazas web, debe completar la configuración inicial de la aplicación:

- Para la supervisión del tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitado de forma predeterminada).
- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación supervisa todos los puertos).
- Seleccione las aplicaciones cuyo tráfico desea que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya están presentes en la lista de aplicaciones recomendadas por Kaspersky. Si su navegador no aparece en la lista, agréguelo manualmente.
- Recomendamos inyectar un script de interacción de página web en el tráfico web (de forma predeterminada, la inyección de script está desactivada). Este script permite el registro de eventos de Protección frente a amenazas web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Cuando un usuario intenta abrir un sitio web malicioso o de phishing, Kaspersky Endpoint Security bloqueará el acceso y le mostrará una advertencia.

Configuración de componente Protección frente a amenazas web

Parámetro	Descripción
Nivel de seguridad *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Para la Protección frente a amenazas web, la aplicación puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*. • **Alto**. El nivel de seguridad en el que componente Protección frente a amenazas web realiza el máximo análisis del tráfico web que el equipo recibe a través de HTTP y FTP. Protección frente a amenazas web analiza en detalle todos los objetos del tráfico web mediante todo el conjunto de bases de datos de la aplicación, y realiza el análisis heurístico más exhaustivo posible. • **Recomendado**. El nivel de seguridad que ofrece el equilibrio perfecto entre el rendimiento de la aplicación y la seguridad del tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web. • **Bajo**. La configuración de este nivel de seguridad de tráfico web garantiza el análisis más rápido de tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis superficial.
Acción al detectar una amenaza	**Bloquear**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador. **Informar**. Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, Kaspersky Endpoint Security permite que este objeto se descargue en el equipo, pero añade información sobre el objeto a la lista de amenazas activas.
Contrastar la dirección web en la base de datos de direcciones web maliciosas *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Al analizar los enlaces para determinar si están incluidos en la base de datos de direcciones web maliciosas, se le permite rastrear sitios web que hayan sido incluidos en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web maliciosas, que se incluye en el paquete de instalación de la aplicación y que se actualiza con las actualizaciones de la base de datos de Kaspersky Endpoint Security.
Usar análisis heurístico *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.

Parámetro	Descripción
Contrastar la dirección web en la base de datos de direcciones web de phishing *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.
No analizar tráfico web de direcciones web de confianza	Si se selecciona esta opción, el componente Protección frente a amenazas web no analiza el contenido de páginas o sitios web cuyas direcciones estén incluidas en la lista de direcciones web de confianza. Puede añadir a esta lista de direcciones web de confianza tanto direcciones específicas como máscaras de páginas o sitios web. También puede crear una lista general de exclusiones para conexiones cifradas. En este caso, Kaspersky Endpoint Security no analiza el tráfico HTTPS de las direcciones web de confianza cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control Web están haciendo su trabajo.

Protección frente a amenazas en el correo

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y el análisis heurístico.

Protección frente a amenazas en el correo puede analizar tanto los mensajes entrantes como los salientes. La aplicación es compatible con POP3, SMTP, IMAP y NNTP en los siguientes clientes de correo:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Para analizar el tráfico en los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, debe añadir el certificado de Kaspersky a la tienda de certificados y seleccionar su tienda propia de certificados.

Protección frente a amenazas en el correo no es compatible con otros protocolos y clientes de correo.

Es posible que Protección frente a amenazas en el correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, Protección frente a amenazas en el correo incluye una extensión para Microsoft Office Outlook. La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección frente a amenazas en el correo admite las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365. En equipos basados en Arm, la extensión Protección frente a amenazas en el correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64.

El componente Protección frente a amenazas en el correo no analiza los mensajes si el programa de correo se abre en un navegador.

Cuando se detecta un archivo malicioso en un archivo adjunto, Kaspersky Endpoint Security añade información sobre la acción realizada en el asunto del mensaje, por ejemplo: *[El mensaje ha sido procesado] <asunto del mensaje>*.

Configuración del componente Protección frente a amenazas en el correo

Parámetro	Descripción
Nivel de seguridad *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	Para la Protección frente a amenazas en el correo, la aplicación puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan *niveles de seguridad*. • **Alto**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo analiza los mensajes más exhaustivamente. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico avanzado. El nivel de seguridad de correo Máximo se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo electrónico gratuito desde una red doméstica sin protección centralizada del correo electrónico. • **Recomendado**. El nivel de seguridad de correo electrónico que proporciona el equilibrio perfecto entre el rendimiento de la aplicación y la seguridad del correo electrónico. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico de correo. • **Bajo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo solamente analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza archivos adjuntos en mensajes de correo electrónico. Con este nivel de seguridad, el componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico a una velocidad máxima y con un uso mínimo de recursos del sistema operativo. Se recomienda el nivel de seguridad de correo Mínimo para su uso en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una LAN empresarial con protección centralizada del correo electrónico.
Acción al detectar una amenaza	**Desinfectar; eliminar si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante o saliente, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación eliminará el objeto infectado. La aplicación añade información sobre la acción realizada al asunto del mensaje, por ejemplo: *[Se ha procesado el mensaje] <asunto del mensaje>*. **Desinfectar; bloquear si la desinfección falla**. Cuando se detecta un objeto infectado en un mensaje entrante, la aplicación intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, la aplicación intenta desinfectar el objeto. Si el objeto no se puede desinfectar, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error. **Bloquear**. Si se detecta un objeto infectado en un mensaje entrante, la aplicación añade una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, la aplicación bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.
Cobertura de protección *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	La *Cobertura de protección* incluye objetos que el componente comprueba cuando se ejecuta: Mensajes entrantes y salientes o Solo mensajes entrantes. Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar que los archivos infectados se envíen en archivos. También puede activar el análisis de mensajes salientes si desea evitar que se envíen archivos en formatos particulares, como archivos de audio y vídeo, por ejemplo.
Analizar tráfico POP3, SMTP, NNTP e IMAP	El análisis que realiza el componente Protección frente a amenazas en el correo del tráfico que se transfiere mediante los protocolos POP3, SMTP, NNTP e IMAP.
Conectar el complemento de Microsoft Outlook	Si esta casilla está seleccionada, los mensajes de correo electrónico que se transmitan a través de los protocolos POP3, SMTP, NNTP e IMAP se analizarán con la extensión integrada en Microsoft Outlook. Si el correo se analiza usando la extensión para Microsoft Outlook, se recomienda usar el Cached Exchange Mode. Para información más detallada sobre el Modo caché de Exchange y recomendaciones sobre su uso, consulte la Base de conocimientos de Microsoft.
Análisis heurístico *(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.

Parámetro	Descripción
Analizar archivos adjuntos	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos). Si, durante el análisis, la aplicación detecta una contraseña para un archivo en el texto del mensaje, esta contraseña se utilizará para analizar el contenido del archivo en busca de aplicaciones maliciosas. En este caso, la contraseña no se guardará. Un archivo de descomprime durante el análisis. Si ocurre un error con la aplicación durante el proceso de descomprimir, puede eliminar manualmente los archivos descomprimidos que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tienen el prefijo PR.
Analizar archivos adjuntos con formatos de Microsoft Office	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
No analizar archivos comprimidos de más de N MB	Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en el correo excluye del análisis los archivos adjuntos de los mensajes de correo electrónico si su tamaño supera el valor especificado. Si se desactiva la casilla de verificación, el componente Protección frente a amenazas en el correo analiza archivos adjuntos de cualquier tamaño.
No comprobar archivos durante más de N seg	Si se selecciona la casilla de verificación, el tiempo asignado para analizar los archivos adjuntos a los mensajes de correo electrónico se limita al período especificado.
Filtro de archivos adjuntos	El filtrado de adjuntos no se aplica a los mensajes de correo electrónico salientes. **Desactivar el filtrado**. Si se selecciona esta opción, el componente Protección frente a amenazas en el correo no filtra archivos que están adjuntos a mensajes de correo electrónico. **Renombrar los adjuntos de los tipos seleccionados**. Si se selecciona esta opción, el componente Protección frente a amenazas en el correo cambia el último carácter de la extensión en archivos adjuntos de los tipos especificados con el símbolo de barra baja (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo. **Eliminar los adjuntos de los tipos seleccionados**. Si se selecciona esta opción, el componente Protección frente a amenazas en el correo elimina los archivos adjuntos de los tipos especificados. Puede especificar los tipos de archivos adjuntos para eliminar de los mensajes de correo electrónico en la lista de máscaras de archivos.

Protección frente a amenazas en la red

El componente *Protección frente a amenazas en la red* (también denominado Intrusion Detection System, IDS) supervisa el tráfico de red entrante en busca de actividad característica de los ataques de red. Cuando la aplicación detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante. Las bases de datos de la aplicación ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos. La lista de ataques de red que detecta el componente Protección frente a amenazas en la red se actualiza durante las actualizaciones de módulos de aplicaciones y bases de datos.

Parámetro	Descripción
Tratar el análisis de puerto y el desbordamiento de red como ataques	*Inundación de red* es un ataque a los recursos de red de una organización (como servidores web). Este ataque consiste en enviar una gran cantidad de solicitudes para sobrecargar el ancho de banda de los recursos de la red. Cuando esto sucede, los usuarios no pueden acceder a los recursos de red de la organización. Un ataque de tipo *"Port scan"* consiste en el escaneo de puertos UDP, TCP, puertos y servicios de red en el equipo. Este ataque permite al atacante identificar el grado de vulnerabilidad del equipo antes de realizar tipos de ataques de red más peligrosos. Los ataques de tipo "Port scan" también permiten al atacante identificar el sistema operativo en el equipo y seleccionar los ataques de red apropiados para este sistema operativo. Cuando esta casilla está activada, Kaspersky Endpoint Security supervisa el tráfico de red para detectar estos ataques. Si se detecta un ataque, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación proporciona información sobre el equipo atacante, que es necesaria para emprender acciones de respuesta frente a amenazas. Puede activar la detección de este tipo de ataques en caso de que algunas de sus aplicaciones permitidas realicen operaciones típicas de este tipo de ataques. Esto ayudará a evitar falsas alarmas.
Bloquear dispositivos atacantes durante N min	Si esta opción está activada, el componente Protección frente a amenazas en la red añade al equipo atacante a la lista de bloqueados. Esto quiere decir que el componente Protección frente a amenazas en la red bloquea la conexión de red del equipo atacante después del primer intento de ataque de red durante el período de tiempo especificado. Este bloqueo protege automáticamente al equipo del usuario frente a posibles ataques de red desde la misma dirección en el futuro. El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 999 minutos. Puede ver la lista de rechazados en la ventana de la herramienta Monitor de red. Kaspersky Endpoint Security borra la lista de rechazados al reiniciar la aplicación y cuando se cambian los ajustes de Protección frente a amenazas en la red.
Exclusiones	La lista contiene direcciones IP para las que Protección frente a amenazas en la red no bloquea los ataques de la red. Puede agregar una dirección IP con el puerto y el protocolo especificados. La aplicación no registra ningún dato sobre los ataques de red provenientes de las direcciones IP de la lista de exclusiones.
Protección contra spoofing de MAC	Los *ataques de spoofing de MAC* consisten en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Como resultado, un atacante puede redirigir los datos enviados a un dispositivo a otro dispositivo y obtener acceso a esos datos. Kaspersky Endpoint Security le permite saber si se detecta uno de ataques MAC Spoofing y bloquearlo.

Firewall

El componente Firewall bloquea las conexiones no autorizadas a un equipo mientras se trabaja en Internet o en una red local. Firewall también controla la actividad de red de las aplicaciones en el equipo. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. De forma automática, el firewall crea las reglas de red necesarias para que funcionen la aplicación y el Agente de red. Como resultado, el firewall abre varios puertos en el equipo. Los puertos se abren según la función del equipo (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en el equipo, consulte la Ayuda de Kaspersky Security Center.

Reglas de red

Puede configurar las reglas de la red en los siguientes niveles:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones a los paquetes de red, con independencia de la aplicación. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security tiene reglas de paquetes de red predefinidas con permisos recomendados por los expertos de Kaspersky.

- *Reglas de red de la aplicación*. Las reglas de red de la aplicación imponen restricciones sobre la actividad de red de una aplicación concreta. No solo influyen en las características del paquete de red, sino también en la aplicación concreta a la que va dirigida la aplicación concreta o que emitió este paquete de red.

El componente Prevención de intrusiones en el host proporciona el acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de *derechos de aplicación*.

Durante el primer inicio de la aplicación, Firewall realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.

2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

   Se le recomienda participar en Kaspersky Security Network para ayudar a Firewall a trabajar con más eficacia.

3. Coloca la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima*, *No fiable*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

   Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

   Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la configuración del componente Prevención de intrusiones en el host. Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea la actividad de red de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza *Restricción máxima* se les niega el uso de cualquier conexión de red.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. Si se añade actividad de red a varias reglas, Firewall regula la actividad de red en función de la regla con la prioridad más alta.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si tanto las reglas de paquetes de red como las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se gestiona de acuerdo con las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan de una manera especial. La regla para aplicaciones de la red incluye reglas de acceso en función del estado de la red: *Red pública*, *Red local*, *Red de confianza*. Por ejemplo, a las aplicaciones del grupo de confianza *Restricción máxima* se les niega cualquier actividad de red en redes de cualquier estado de manera predeterminada. Si se especifica una regla de red para una aplicación individual (aplicación principal), los subprocesos de otras aplicaciones se ejecutarán de acuerdo con la regla de red de la aplicación principal. Si no hay una regla de red para la aplicación, los subprocesos se ejecutarán de acuerdo con la regla de acceso a la red del grupo de confianza de la aplicación.

Por ejemplo, ha prohibido cualquier actividad de red en redes de todos los estados para todas las aplicaciones, excepto el navegador X. Si inicia la instalación del navegador Y (subproceso) desde el navegador X (aplicación principal), el instalador del navegador Y accederá a la red y descargará los archivos necesarios. Después de la instalación, se negarán las conexiones de red al navegador Y de acuerdo con la configuración del Firewall. Para prohibir la actividad de red del instalador del navegador Y como un subproceso, debe asignar una regla de red para el instalador del navegador Y.

Tipos de conexión de red

Firewall le permite controlar la actividad de la red en función del tipo de conexión de red. Kaspersky Endpoint Security recibe el tipo de conexión de red del sistema operativo del equipo. El tipo de conexión de red en el sistema operativo lo establece el usuario al configurar la conexión. Puede cambiar el tipo de conexión de red en la configuración de Kaspersky Endpoint Security. Firewall supervisará la actividad de la red en función del tipo de red especificado en la configuración de Kaspersky Endpoint Security, y no en del sistema operativo.

Están disponibles los siguientes tipos de conexión de red:

- **Red pública**. La red no está protegida por aplicaciones antivirus, firewalls ni filtros (como la red wifi de una cafetería). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos a través de carpetas compartidas y acceso remoto al escritorio de este ordenador. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.

  Firewall asigna el tipo *Red pública* a Internet de forma predeterminada. No se puede cambiar el tipo de Internet.

- **Red local**. Red para usuarios con acceso restringido a archivos e impresoras en este ordenador (por ejemplo, para una LAN corporativa o una red doméstica).

- **Red de confianza**. Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.

Configuración del componente Firewall

Parámetro	Descripción
Reglas para paquetes	Tabla con una lista de reglas de paquetes de red. Las reglas de paquetes de red sirven para imponer restricciones a los paquetes de red, con independencia de la aplicación. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. La tabla enumera las reglas de paquetes de red preconfiguradas que recomienda Kaspersky para una protección óptima del tráfico de red de equipos que se ejecutan con los sistemas operativos Microsoft Windows. Firewall establece la prioridad de cada regla de paquetes de red. Firewall procesa las reglas de paquetes de red en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba abajo. Cuando se detecta una conexión de red, Firewall busca la primera regla de paquetes pertinente y la aplica a la actividad de red, que se permitirá o bloqueará según corresponda. Las reglas posteriores que también sean aplicables a la conexión de red se desestimarán. Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones.
Redes disponibles	Esta tabla contiene información sobre las conexiones de red que Firewall detecta en el equipo. El estado *Red pública* se asigna a internet de forma predeterminada. No se puede cambiar el estado de internet.
Reglas para aplicaciones	**Aplicación**. Tabla de aplicaciones que controla el componente Firewall. Las aplicaciones se asignan a grupos de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security usa al controlar la actividad de red de las aplicaciones. Puede seleccionar una aplicación de una lista única de todas las aplicaciones instaladas en equipos bajo la influencia de una directiva y añadir la aplicación a un grupo de confianza. **Reglas de red**. Tabla de reglas de red para aplicaciones que forman parte de un grupo de confianza. De acuerdo con estas reglas, Firewall regula la actividad de red de aplicaciones. La tabla muestra las reglas de red predefinidas que recomiendan los expertos de Kaspersky. Estas reglas de red se han añadido para proteger de manera óptima el tráfico de red de los equipos que ejecutan sistemas operativos Windows. No se puede eliminar las reglas de red predefinidas.

Prevención de ataques de BadUSB

Algunos virus modifican el firmware de los dispositivos USB para engañar al sistema operativo y que detecte el dispositivo USB y lo identifique como teclado. Como resultado, el virus puede ejecutar comandos en su cuenta de usuario para descargar software malicioso, por ejemplo.

El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.

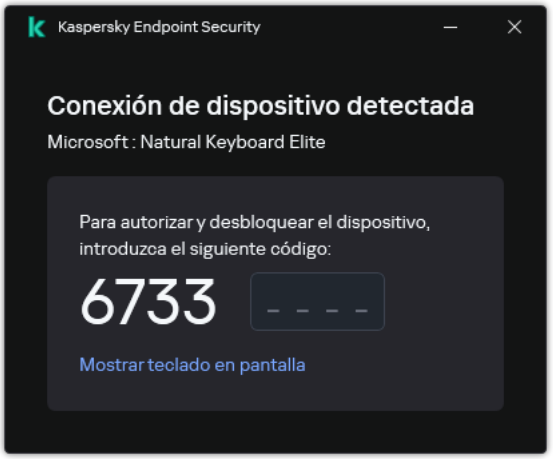
Cuando un dispositivo USB se conecta al equipo y el sistema operativo lo identifica como un teclado, la aplicación solicita al usuario que introduzca desde este teclado un código numérico generado por la aplicación, o bien que utilice el teclado en pantalla si está disponible (vea la figura a continuación). Este procedimiento se conoce como autorización del teclado.

Si el código se ha introducido correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al que se ha conectado) en la lista de teclados autorizados. No será necesario volver a realizar la autorización del teclado cuando se vuelva a conectar el teclado o después de que se reinicie el sistema operativo.

Cuando el teclado autorizado está conectado a un puerto USB diferente del equipo, la aplicación muestra un mensaje para la autorización de este teclado.

Si se introduce el código numérico de forma incorrecta, la aplicación generará un nuevo código. Puede configurar el número de intentos para introducir el código numérico. Si el código numérico se introduce de forma incorrecta muchas veces o si se cierra la ventana de autorización del teclado (ver la figura a continuación), la aplicación bloquea las acciones de ese teclado. Cuando se cumple el período de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación solicita al usuario que realice de nuevo el procedimiento de autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea los teclados que no se hayan autorizado.



Autorización del teclado

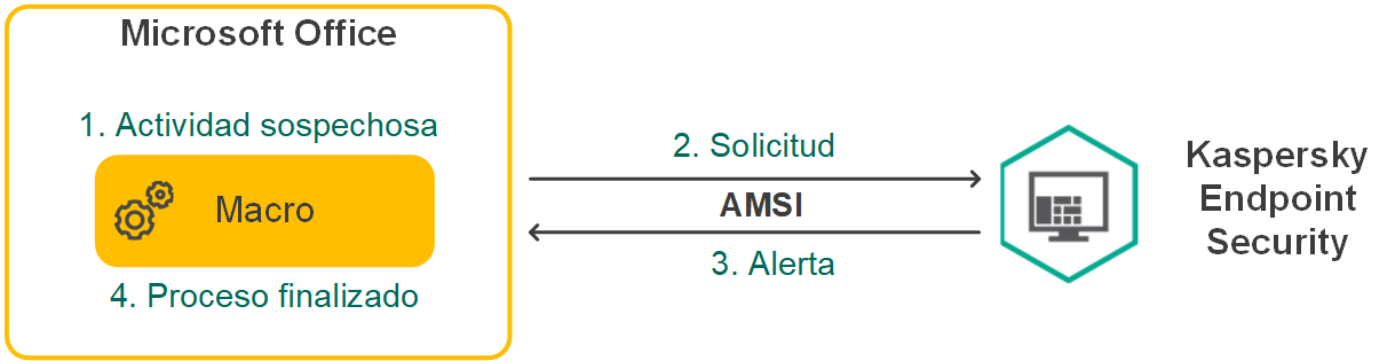
Configuración del componente Prevención de ataques de BadUSB

Parámetro	Descripción
Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB	Si el interruptor se activa, la aplicación bloquea el uso del teclado en pantalla para autorizar el dispositivo USB con el que no se puede introducir un código de autorización.
Prohibir el uso de un código de barras para la autorización de dispositivos USB	Si este interruptor está activado, la aplicación no muestra el código de barras en la notificación de autenticación del escáner de códigos de barras.
Número máximo de intentos de autorización del dispositivo USB	Bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para introducir el código de autorización, la aplicación bloquea el dispositivo USB tras el quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este período, volverá a disponer de cinco intentos para introducir el código de autorización.
Tiempo de espera al alcanzar el número máximo de intentos	Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos de introducir el código de autorización. Los valores válidos son de 1 a 180 (minutos).

Protección AMSI

El componente Protección AMSI está diseñado para admitir la Interfaz de análisis antimalware de Microsoft. La *interfaz de análisis antimalware (AMSI)* permite que las aplicaciones de terceros con soporte de la AMSI envíen a Kaspersky Endpoint Security aquellos objetos para los cuales precisan un análisis adicional (por ejemplo, scripts de PowerShell). Una vez que el análisis se completa, el resultado se devuelve a la aplicación que originó la solicitud. El concepto de "aplicaciones de terceros" incluye, por ejemplo, las aplicaciones de Microsoft Office (vea la imagen de más abajo). Para más detalles sobre AMSI, consulte la documentación de Microsoft.

La protección AMSI únicamente puede detectar una amenaza y notificar a una aplicación de terceros sobre dicha amenaza detectada. Una aplicación de terceros, después de recibir una notificación de una amenaza, no permite acciones maliciosas (por ejemplo, finaliza la acción).



Ejemplo del funcionamiento de AMSI

El componente de protección AMSI puede rechazar una solicitud de una aplicación de terceros si, por ejemplo, esta aplicación sobrepasa el número máximo de solicitudes dentro de un intervalo específico. Cuando esto ocurre, Kaspersky Endpoint Security envía información al respecto al Servidor de administración. El componente Protección AMSI no rechaza las solicitudes de aquellas aplicaciones de terceros para las cuales la integración continua con el componente de protección AMSI está activada.

La protección AMSI está disponible para los siguientes sistemas operativos para estaciones de trabajo y servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión
- Windows Server 2016 Essentials / Standard / Datacenter (modo Server Core incluido)
- Windows Server 2019 Essentials / Standard / Datacenter (modo Server Core incluido)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (modo Server Core incluido)
- Windows Server 2025 Standard / Datacenter

Configuración de Protección AMSI

Parámetro	Descripción
Analizar archivos	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al comprobar archivos, la aplicación realiza una descompresión recursiva. Esto permite detectar amenazas en archivos multinivel (archivos dentro de archivos).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos en formatos de Microsoft Office	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE. La aplicación analiza los archivos con formato Office que tienen menos de 1 MB, independientemente de si la casilla de verificación está seleccionada o no.
No descomprimir archivos compuestos grandes	Si esta casilla de verificación está marcada, la aplicación no analiza archivos compuestos cuyo tamaño exceda el valor especificado. Si esta casilla de verificación no está marcada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.

Prevención de exploits

El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para hacerlo, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malicioso. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

El componente Prevención de exploits también supervisa los puertos de red en busca de procesos de aplicaciones que puedan poner en peligro la seguridad del equipo. La aplicación obtiene información sobre dichos procesos con bases de datos antivirus.

Configuración del componente Prevención de exploits

Parámetro	Descripción
Al detectar vulnerabilidades	**Bloquear**. Si este elemento está seleccionado, al detectar una vulnerabilidad de seguridad, Kaspersky Endpoint Security bloquea el funcionamiento de la vulnerabilidad y crea una entrada de registro con información relevante. **Informar**. Si este elemento está seleccionado, cuando Kaspersky Endpoint Security detecte una vulnerabilidad registrará un evento que contenga información sobre la vulnerabilidad y añadirá información sobre esta vulnerabilidad a la lista de amenazas activas.
Activar protección de la memoria de los procesos del sistema	Si se activa este interruptor, Kaspersky Endpoint Security bloquea los procesos externos que intentan acceder a la memoria de los procesos del sistema.

Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones de su equipo y ofrece esta información a otros componentes de protección mejorar su rendimiento. El componente Detección de comportamientos utiliza firmas de patrones de actividad peligrosa (Behavior stream signatures, BSS) para aplicaciones. Si la actividad de la aplicación coincide con una BSS Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security se basa en bases de datos de reglas heurísticas ofrece protección proactiva al equipo.

El componente Detección de comportamiento también supervisa los puertos de red en busca de procesos de aplicaciones que puedan poner en peligro la seguridad del equipo. La aplicación obtiene información sobre dichos procesos con bases de datos antivirus.

Parámetros del componente Detección de comportamientos

Parámetro	Descripción
Acción al detectar actividad de software malicioso	**Eliminar**. Seleccione este elemento para que, cuando se detecte actividad maliciosa, Kaspersky Endpoint Security elimine el archivo ejecutable de la aplicación maliciosa y cree una copia de seguridad del archivo en Copias de seguridad. **Bloquear**. Seleccione este elemento para que, cuando se detecte actividad maliciosa, Kaspersky Endpoint Security finalice la aplicación. **Informar**. Seleccione este elemento para que, si se detecta actividad maliciosa de parte de una aplicación, Kaspersky Endpoint Security no finalice la aplicación, sino que añada información sobre esta actividad maliciosa a la lista de amenazas activas.

Prevención de intrusiones en el host

El componente Prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus y el servicio en la nube Kaspersky Security Network.

El componente controla el funcionamiento de las aplicaciones mediante el uso de *derechos de las aplicaciones*. Los derechos de las aplicaciones incluyen los siguientes parámetros de acceso:

- Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro)
- Acceso a datos personales (por exemplo, archivos y aplicaciones)

La actividad de red de las aplicaciones está controlada por el componente Firewall utilizando las *reglas de red*.

Durante el primer inicio de la aplicación, el componente Prevención de intrusiones en el host realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

   Se le recomienda participar en Kaspersky Security Network para ayudar al componente Prevención de intrusiones en el host a trabajar con más eficacia.

3. Coloca la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima*, *No fiable*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

   Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

   Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la configuración del componente Prevención de intrusiones en el host. Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea las acciones de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza *Restricción máxima* se les niega el acceso a los módulos del sistema operativo.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

Parámetro	Descripción
Derechos de la aplicación	Tabla de aplicaciones que supervisa el componente Prevención de intrusiones en el host. Las aplicaciones se asignan a grupos de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Puede seleccionar una aplicación de una lista única de todas las aplicaciones instaladas en equipos bajo la influencia de una directiva y añadir la aplicación a un grupo de confianza. Los derechos de acceso a la aplicación se muestran en las siguientes tablas: • **Archivos y registro del sistema**. Tabla de derechos de acceso a recursos del sistema operativo y datos personales para aplicaciones pertenecientes al grupo de confianza. • **Permisos**. Tabla de derechos de acceso a procesos y recursos del sistema operativo para aplicaciones pertenecientes al grupo de confianza. • **Reglas de red**. Tabla de reglas de red para aplicaciones que forman parte de un grupo de confianza. De acuerdo con estas reglas, Firewall regula la actividad de red de aplicaciones. La tabla muestra las reglas de red predefinidas que recomiendan los expertos de Kaspersky. Estas reglas de red se han añadido para proteger de manera óptima el tráfico de red de los equipos que ejecutan sistemas operativos Windows. No se puede eliminar las reglas de red predefinidas.
Recursos protegidos	La tabla contiene los recursos del equipo clasificados. El componente Prevención de intrusiones en el host supervisa los intentos de otras aplicaciones para acceder a recursos de la tabla. Un recurso puede ser una categoría de registro, archivo, carpeta o clave de registro.
Grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security	Un grupo de confianza en el que se ubicarán las aplicaciones que se inicien antes que Kaspersky Endpoint Security.
Actualizar reglas de aplicaciones anteriormente desconocidas desde KSN	Si se selecciona esta casilla, el componente Prevención de intrusiones en el host usa la base de datos de Kaspersky Security Network para actualizar los derechos de las aplicaciones anteriormente desconocidas.
Confiar en aplicaciones firmadas digitalmente	Si se selecciona esta casilla de verificación, el componente Prevención de intrusiones en el host ubica las aplicaciones con la firma digital de los proveedores de confianza en el grupo de confianza *De confianza*. *Los proveedores de confianza* son proveedores de software en los que confía Kaspersky. También puede añadir un certificado de proveedor al almacén de certificados de confianza de forma manual. Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera estas aplicaciones como de confianza y utiliza otros ajustes para determinar su grupo de confianza.
Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días (de 1 a 90)	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security elimina automáticamente información sobre la aplicación (grupo de confianza y derechos de acceso) si se cumplen las siguientes condiciones: • Si coloca manualmente la aplicación en un grupo de confianza o configura sus derechos de acceso. • La aplicación no se ha iniciado durante el período de tiempo definido. Si el grupo de confianza y los derechos de una aplicación se han determinado automáticamente, Kaspersky Endpoint Security elimina la información sobre esta aplicación después de 30 días. No es posible cambiar el período de almacenamiento para la información de las aplicaciones ni desactivar la eliminación automática. La próxima vez que inicie esta aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.
Grupo de confianza para aplicaciones no incluidas en otros grupos	Los elementos en esta lista desplegable determinan a qué grupo de confianza Kaspersky Endpoint Security asignará una aplicación desconocida. Puede elegir uno de los siguientes elementos: • **Restricción mínima**. • **Restricción máxima**. • **No fiable**.

Motor de reparación

El componente Motor de reparación permite a Kaspersky Endpoint Security anular acciones que han sido realizadas por el malware en el sistema operativo.

Al anular la actividad de malware en el sistema operativo, Kaspersky Endpoint Security tramita los siguientes tipos de actividad de malware:

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina archivos ejecutables creados por malware (en todos los medios, excepto en las unidades de red).
  - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado.
  - Restaura los archivos que el malware ha modificado o eliminado.

  La capacidad de recuperar archivos está sujeta a algunas limitaciones.

- **Actividad del Registro**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina las claves del registro que el malware ha creado.
  - No restaura las claves del registro que el malware ha modificado o eliminado.

- **Actividad del sistema**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Finaliza los procesos iniciados por malware.
  - Finaliza los procesos en los que haya penetrado una aplicación maliciosa.
  - No reanuda procesos que el malware haya suspendido.

- **Actividad de red**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Bloquea la actividad de red del malware.
  - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.

La reversión de acciones de malware puede iniciarse durante un análisis antimalware o a pedido de los componentes Protección frente a amenazas en archivos y Detección de comportamiento.

Deshacer las operaciones de un software malicioso (malware) afecta a un conjunto de datos definidos rigurosamente. La anulación no tiene efectos adversos en el sistema operativo ni en la integridad de los datos del equipo.

Kaspersky Security Network



A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

La función de KSN puede dejar de estar disponible en la aplicación en el territorio de EE. UU.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, los servicios de KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web que se analicen, así como sobre la categoría y reputación de los archivos analizados. Para obtener más información sobre la configuración del acceso a KSN, consulte la Ayuda de Kaspersky Security Center.

El uso de Kaspersky Security Network es voluntario. La aplicación le invita a usar en KSN durante la configuración inicial de la aplicación. Los usuarios podrán reanudar o interrumpir su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el sitio web de Kaspersky contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. El archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación, contiene el texto de la Declaración de Kaspersky Security Network.

La infraestructura de las bases de datos de reputación de Kaspersky

Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura para trabajar con las bases de datos de reputación de Kaspersky:

- *Kaspersky Security Network (KSN).* Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky y, a su vez, envían a Kaspersky información sobre los objetos que se detectan en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos.

- *Kaspersky Private Security Network (KPSN)* es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky y a otros datos estadísticos sin enviar datos a Kaspersky desde sus propios equipos. KPSN se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:

    - porque las estaciones de trabajo locales no tienen acceso a Internet;

porque, por motivos legales o debido a las directivas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

Parámetro	Descripción
Activar el modo ampliado de KSN	El *modo KSN ampliado* es un modo en el que Kaspersky Endpoint Security envía información adicional a Kaspersky. Kaspersky Endpoint Security utiliza KSN para detectar amenazas independientemente de la posición del botón.
Activar modo nube	*Modo nube* es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky. Si el interruptor está activado, Kaspersky Endpoint Security usa una versión reducida de las bases de datos antivirus para tener un menor impacto en los recursos del sistema operativo. Kaspersky Endpoint Security descarga la versión ligera de las bases de datos antivirus durante la siguiente actualización después de que se haya seleccionado la casilla. Si el interruptor está desactivado, Kaspersky Endpoint Security usa la versión completa de las bases de datos antivirus. Kaspersky Endpoint Security descarga la versión completa de las bases de datos antivirus durante la siguiente actualización después de que se haya desactivado la casilla.
Estado del equipo cuando los servidores de KSN no están disponibles *(disponible solo en la Consola de Kaspersky Security Center)*	Los elementos de esta lista desplegable permiten indicar qué estado tendrá un equipo en Kaspersky Security Center cuando los servidores de KSN no estén disponibles.
Utilizar Servidor de administración como servidor proxy de KSN *(disponible solo en la Consola de Kaspersky Security Center)*	Cuando esta casilla está activada, Kaspersky Endpoint Security usa el servicio proxy de KSN. Los parámetros de este servicio se configuran a través de las propiedades del Servidor de administración.
Utilizar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible *(disponible solo en la Consola de Kaspersky Security Center)*	Cuando esta casilla está activada y el servicio KSN Proxy no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores KSN pueden ubicarse tanto en el lado de Kaspersky como en el lado de terceros (cuando se utiliza Kaspersky Private Security Network).

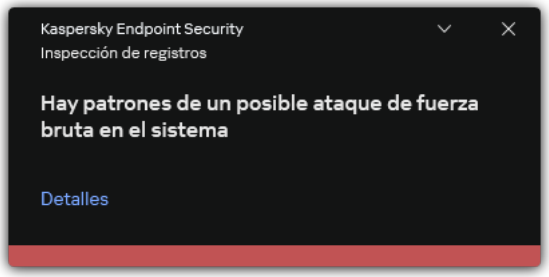
Inspección de registros

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo.

La inspección de registros supervisa la integridad del entorno protegido basándose en los resultados del análisis del Registro de eventos de Windows. Cuando la aplicación detecta señales de comportamientos atípicos en el sistema, informa al administrador debido a que este comportamiento puede indicar un intento de ataque cibernético.

Kaspersky Endpoint Security analiza los registro de eventos de Windows y detecta las violaciones de acuerdo con las reglas. El componente incluye reglas predefinidas. Las reglas predefinidas recibe alimentación del análisis heurístico. También puede añadir sus propias reglas (reglas personalizadas). Cuando se activa una regla, la aplicación crea un evento con el estado *Crítico* (consulte la figura siguiente).

Si desea usar la Inspección de registros, asegúrese de que la configuración de seguridad de la directiva de auditorías esté configurada y que el sistema esté registrando los eventos relevantes (para conocer más detalles, visite el sitio web de soporte técnico de Microsoft).



Notificación de inspección de registros

Configuración de inspección de registros

Parámetro	Descripción
Reglas predefinidas	Lista de reglas de Inspección de registros. Las reglas predefinidas incluyen plantillas para la actividad anormal en el equipo protegido. La actividad anormal puede significar un intento de ataque.
Reglas personalizadas	Lista de reglas de Inspección de registros que añadió el usuario. Puede configurar sus propios criterios para la activación de la regla de Inspección de registros. Para hacerlo, debe introducir un identificador del evento y seleccionar el origen de un evento. Puede seleccionar el origen de un evento desde los registros estándar: *Application*, *Security* o *System*. También puede especificar el registro de una aplicación de terceros.

Anti-Cryptor

El componente Anti-Cryptor analiza la actividad en las carpetas compartidas. Si esta actividad coincide con un tipo de comportamiento típico del cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.

Kaspersky Endpoint Security impide el cifrado externo solo de los archivos ubicados en unidades con el sistema de archivos NTFS y no cifrados por el sistema EFS.

Parámetro	Descripción
Exclusiones por nombre o dirección IP	**Exclusiones por nombre o dirección IP**. Lista de equipos cuyos intentos de cifrar carpetas compartidas no se supervisarán. Para aplicar la lista de equipos excluidos de la protección de carpetas compartidas contra el cifrado externo, deberá activar la opción "Auditar inicio de sesión" en la directiva de auditoría de seguridad de Windows. De manera predeterminada, la opción "Auditar inicio de sesión" no está activada. Para obtener más información acerca de la directiva de auditorías de seguridad de Windows, visite el sitio web de Microsoft. **Exclusiones por máscara**. Exclusiones de la cobertura de protección. Excluir una carpeta de la cobertura de protección puede reducir el número de falsos positivos si su organización usa cifrado de datos al intercambiar archivos mediante carpetas compartidas. Por ejemplo, la Detección de comportamiento puede arrojar falsos positivos si el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Esta actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, añada dicha carpeta a las exclusiones. Usar máscaras: • El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas • Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. • El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
Acción al detectar una amenaza	• **Informar**. Si se selecciona esta opción, al detectar un intento de modificar archivos de carpetas compartidas, Kaspersky Endpoint Security añade información sobre este intento a la lista de amenazas activas, añade una entrada a informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center. • **Bloquear conexión durante (min) N minutos**. Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar archivos en carpetas compartidas, bloquea el acceso a la modificación del archivo para la sesión que ha iniciado la actividad maliciosa y crea copias de seguridad de los archivos modificados. Si el componente Motor de reparación está activado y la opción **Bloquear conexión durante (min) N minutos** está seleccionada, se restauran los archivos modificados a partir de las copias de seguridad.
Cobertura de protección	La *cobertura de protección* es una lista de rutas a carpetas compartidas en las que Kaspersky Endpoint Security supervisa la actividad de los archivos. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara. De forma predeterminada, la aplicación identifica automáticamente las carpetas compartidas y supervisa la actividad de los archivos en todas las carpetas.

Control Web

Control web permite regular el acceso de los usuarios a los recursos web. El componente ayuda a reducir tanto el volumen de tráfico como el tiempo que se malgasta en actividades no laborales. Cuando un usuario intenta abrir un sitio web que se ha restringido mediante Control web, Kaspersky Endpoint Security bloqueará el acceso o le mostrará una advertencia (vea la imagen más abajo).

Para utilizar Web Control, debe completar la configuración inicial de la aplicación:

- Para la supervisión del tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitado de forma predeterminada).
- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación supervisa todos los puertos).

- Seleccione las aplicaciones cuyo tráfico desea que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya están presentes en la lista de aplicaciones recomendadas por Kaspersky. Si su navegador no aparece en la lista, agréguelo manualmente.

- Recomendamos inyectar un script de interacción de página web en el tráfico web (de forma predeterminada, la inyección de script está desactivada). Este script permite el registro de eventos de Control web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Métodos para regular el acceso a los sitios web

Control web permite configurar el acceso a los sitios web a través de estos criterios:

- **Categorías de sitios web**. Para categorizar los sitios web, la aplicación utiliza el servicio en la nube Kaspersky Security Network, el análisis heurístico y la base de datos de sitios web conocidos, que está incluida con las demás bases de datos de la aplicación. Por ejemplo, puede restringir el acceso de los usuarios a la categoría *Redes sociales* o a otras categorías.

- **Tipo de datos**. Puede restringir el acceso de los usuarios a datos de un sitio web y, por ejemplo, ocultar las imágenes. Kaspersky Endpoint Security determina los tipos de datos basándose en el formato de los archivos, no en sus extensiones.

  > Kaspersky Endpoint Security no analiza el contenido de los archivos de almacenamiento. Por ello, si un grupo de imágenes está incluido en un archivo de almacenamiento, Kaspersky Endpoint Security considerará que el tipo de datos es *Archivos* en lugar de *Imágenes*.

- **Direcciones individuales**. Puede especificar una dirección web o usar máscaras.

Los criterios para regular el acceso a los sitios web pueden combinarse. Por ejemplo, puede restringir el acceso al tipo de datos *Archivos de aplicaciones de Office* solo para la categoría de sitios web *Correo electrónico basado en Web*.

Reglas de acceso a sitios web

Control web regula el acceso de los usuarios a los sitios web a través de *reglas de acceso*. Para cada una de estas reglas, puede configurar las siguientes opciones avanzadas:

- Usuarios alcanzados por la regla.

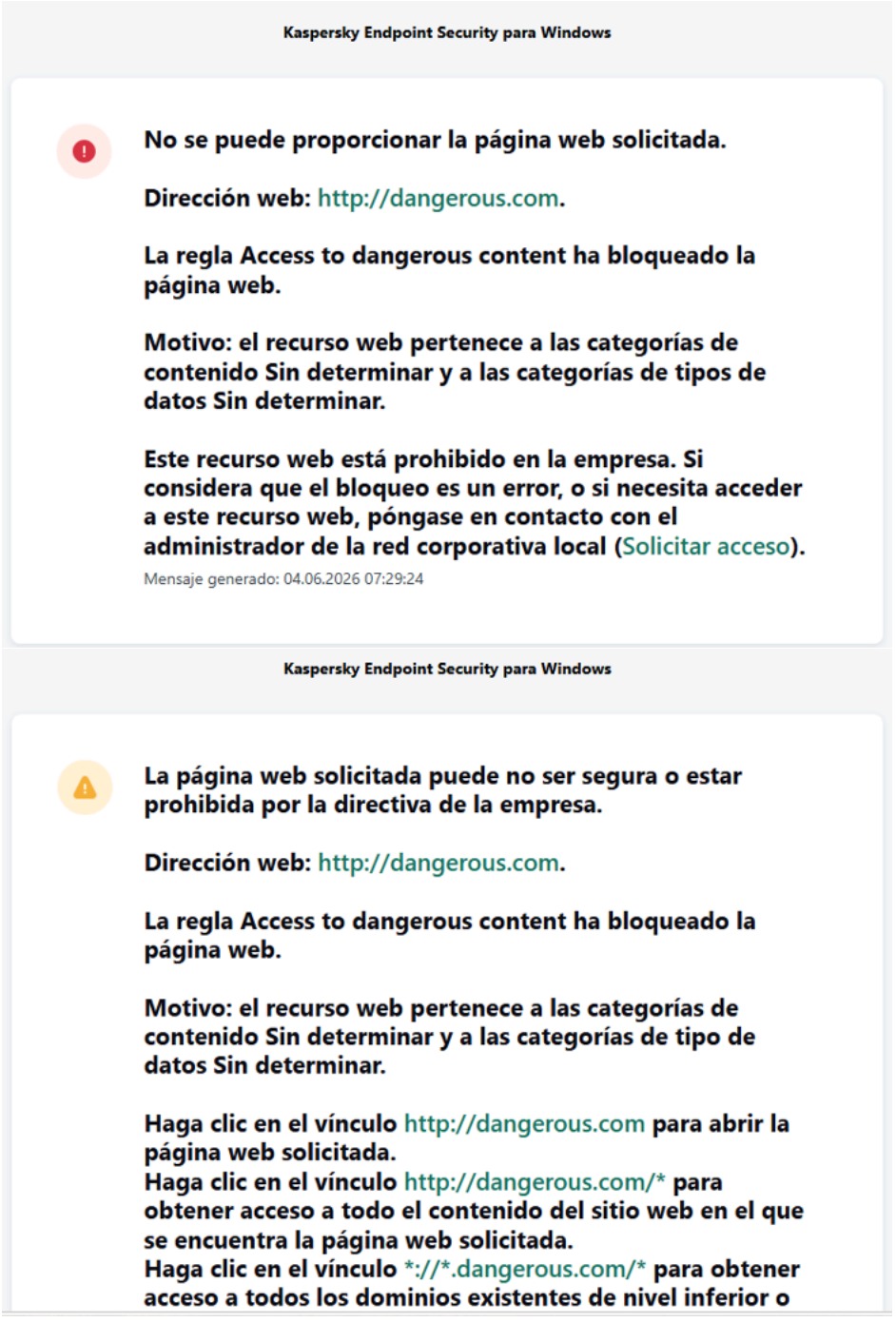
  Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.

- Planificación de reglas.

  Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

Prioridad de las reglas de acceso

Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web *Redes sociales* y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.



Mensajes de Control web

Parámetro	Descripción
Reglas de acceso a recursos web	Lista con las reglas de acceso a recursos web. Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla.
Regla predeterminada	La *regla predeterminada* regula el acceso a los recursos web que no están contemplados en ninguna otra regla. Están disponibles los siguientes opciones: • **Autorizar todo lo que no esté especificado en la lista de reglas**, también conocido como modo de lista de rechazados para sitios web prohibidos. • **Prohibir todo lo que no esté especificado en la lista de reglas**, también conocido como modo de lista de admitidos para sitios web permitidos.
Finalizar sesiones de navegador activas tras aplicar la regla	Si se selecciona la casilla de verificación, Control web finaliza la conexión a los recursos web bloqueados inmediatamente después de aplicar la directiva. El navegador deja de descargar datos de la página web inmediatamente. Cuando actualiza la página web o va a otra página web prohibida, la aplicación muestra una advertencia. Control Web permite desconectar inmediatamente los recursos web solo en navegadores web. Para otras aplicaciones, Control Web solo restringe las nuevas conexiones. Si la casilla de verificación está desactivada, Control web restringe solo las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.
Plantillas	**Advertencia**. El campo de entrada consta de una plantilla del mensaje que se muestra si se activa una regla de advertencia sobre intentos de acceso a un recurso web no deseado. **Mensaje sobre el bloqueo**. El campo de entrada contiene la plantilla del mensaje que aparece si se activa una regla que bloquee el acceso a un recurso web. **Mensaje para el administrador**. La plantilla del mensaje que se enviará al administrador de la LAN si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso a la página web**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada. Se proporcionan variables especiales para administrar la plantilla de mensaje (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensaje para diferentes ordenadores.
Registrar el acceso a páginas permitidas	Kaspersky Endpoint Security dejará constancia de todos los sitios web que se visiten, incluso cuando se trate de sitios web permitidos. Kaspersky Endpoint Security envía eventos a Kaspersky Security Center, al registro local de Kaspersky Endpoint Security y al registro de eventos de Windows. Para supervisar las actividades de los usuarios en Internet, deberá configurar los ajustes de almacenamiento de eventos. Navegadores que admiten la función de supervisión: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. La supervisión de las actividades de los usuarios no funciona en otros navegadores. Si opta por supervisar las actividades en línea de los usuarios, la carga del equipo podría aumentar cuando se necesite descifrar tráfico HTTPS.

Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi). Esto le permite proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos.

Si el Control de dispositivos está activado, la aplicación transmite información sobre los dispositivos conectados a Kaspersky Security Center. Puede ver la lista de dispositivos conectados en Kaspersky Security Center en la carpeta **Avanzado** → **Repositorios** → **Hardware**.

Niveles de acceso a dispositivos

Control de dispositivos controla el acceso a los siguientes niveles:

- **Tipo de dispositivo**. Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

  Puede configurar el acceso a los dispositivos del siguiente modo:

  - Permitir – .
  - Bloquear – .
  - Por las reglas (solo impresoras y dispositivos portátiles) – .
  - Depende del bus de conexión (excepto wifi): .
  - Bloquear con excepciones (solo wifi): .

- **Bus de conexión**. Un *bus de conexión* es una interfaz usada para conectar dispositivos al equipo (por ejemplo, USB o FireWire). Si se selecciona el modo **Depende del bus de conexión** para el tipo de dispositivo, la aplicación permite o deniega el acceso al dispositivo según la interfaz de conexión (por ejemplo, USB).

  Puede configurar el acceso a los dispositivos del siguiente modo:

  - Permitir – .
  - Bloquear – .

- **Dispositivos de confianza**. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

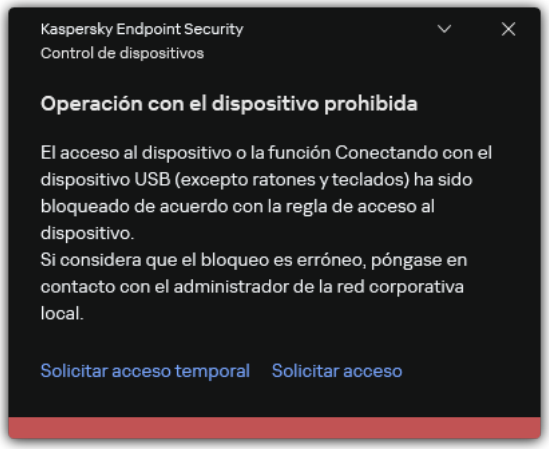
  Puede añadir dispositivos de confianza según los siguientes datos:

  - **Dispositivos por ID**. Cada dispositivo tiene un identificador exclusivo (Hardware ID o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. Ejemplo de ID de dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.
  - **Dispositivos por modelo**. Cada dispositivo tiene un Vendor ID (VID) y un Product ID (PID). Puede ver los ID en las propiedades del dispositivo usando herramientas del sistema operativo. Plantilla para introducir el VID y el PID: `VID_1234&PID_5678`. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.
  - **Dispositivos por máscara de ID**. Si utiliza varios dispositivos con ID similares, puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `WDC_C*`.
  - **Dispositivos por máscara de modelo**. Si utiliza varios dispositivos con VID y PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `VID_05AC&PID_*`.

Control de dispositivos regula el acceso de los usuarios a dispositivos usando *reglas de acceso*. Control de dispositivos también le permite guardar eventos de conexión/desconexión de dispositivos. Para guardar eventos, tiene que configurar el registro de eventos en una directiva.

Cuando el acceso a un dispositivo dependa del bus de conexión (estado), Kaspersky Endpoint Security no guardará ningún evento relacionado con la conexión o desconexión del dispositivo. Para que Kaspersky Endpoint Security guarde eventos de conexión/desconexión, debe autorizar el acceso al tipo de dispositivo correspondiente (estado) o añadir el dispositivo a la lista de dispositivos de confianza.

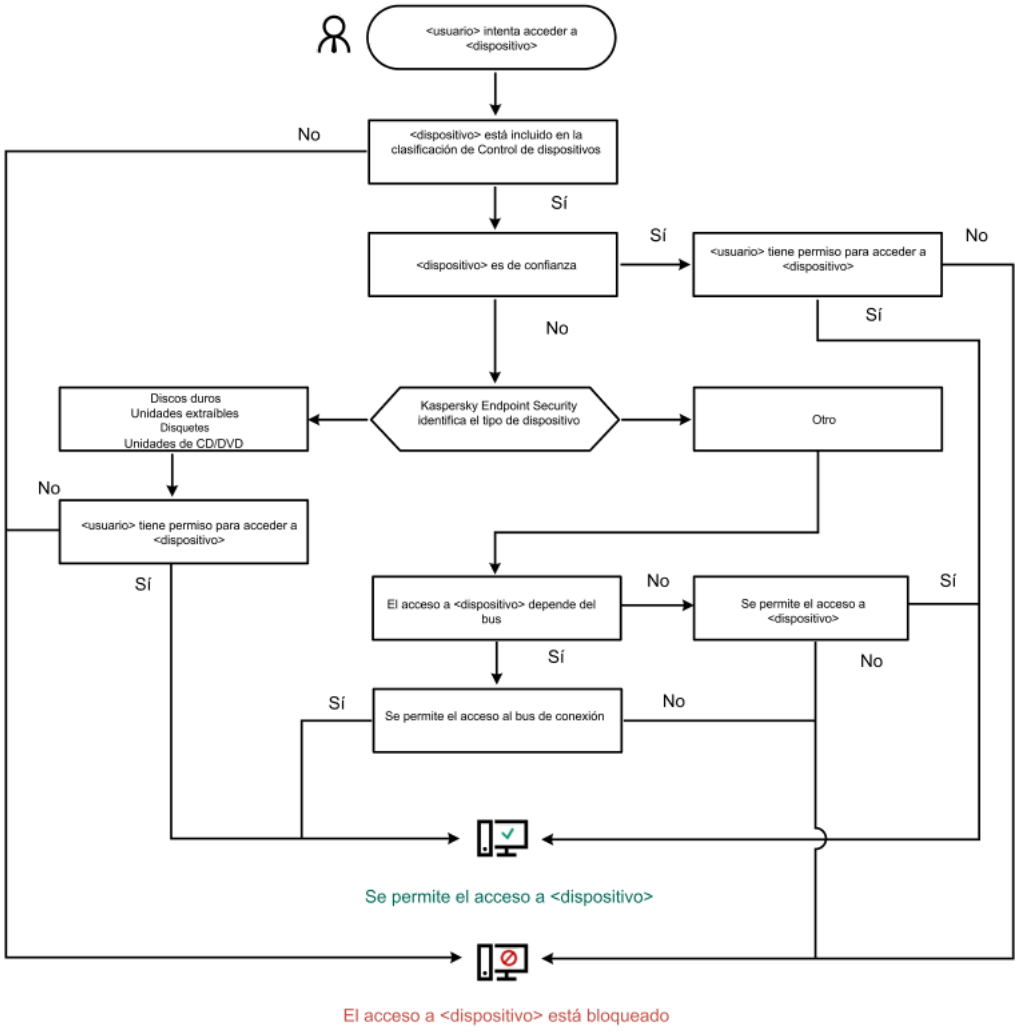
Cuando un dispositivo que está bloqueado por Control de dispositivos se conecte al equipo, Kaspersky Endpoint Security bloqueará el acceso y mostrará una notificación (véase la figura siguiente).



Notificación de Control de dispositivos

Algoritmo de funcionamiento de Control de dispositivos

Kaspersky Endpoint Security toma una decisión sobre si permitir el acceso a un dispositivo después de que el usuario conecte un dispositivo al equipo de la siguiente imagen.



Algoritmo de funcionamiento de Control de dispositivos

Si conecta un dispositivo y se le permite acceder a él, puede editar la regla de acceso y bloquear la posibilidad de utilizarlo. Cuando alguien intente acceder al dispositivo nuevamente (por ejemplo, para ver la estructura de carpetas o para realizar una operación de lectura o escritura), Kaspersky Endpoint Security bloqueará el acceso. Un dispositivo sin sistema de archivos solo se bloquea la próxima vez que se conecta el dispositivo.

Si un usuario del equipo donde se ha instalado Kaspersky Endpoint Security debe solicitar el acceso a un dispositivo que el usuario cree que se bloqueó por equivocación, envíe al usuario las instrucciones para solicitar acceso.

Parámetro	Descripción
Permitir solicitudes de acceso temporal *(disponible solo en la Consola de Kaspersky Security Center)*	Si se selecciona la casilla de verificación, el botón **Solicitar acceso** está disponible a través de la interfaz local de Kaspersky Endpoint Security. Con este botón, el usuario puede solicitar acceso temporal a un dispositivo bloqueado.
Dispositivos y redes wifi	Esta tabla muestra todos los tipos de dispositivos posibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso.
Buses de conexión	Una lista con todos los buses de conexión disponibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso. Kaspersky Endpoint Security permite o deniega el acceso los dispositivos según el tipo de bus de conexión si el modo **Depende del bus de conexión** está seleccionado.
Dispositivos de confianza	Una lista con los dispositivos de confianza y los usuarios que tienen acceso a esos dispositivos.
Fusionar valores al heredar *(disponible solo en la Consola de Kaspersky Security Center)*	Esto fusiona la lista de dispositivos de confianza en las directivas principales y secundarias de Kaspersky Security Center. Para fusionar listas, la directiva secundaria debe configurarse para heredar la configuración de la directiva principal de Kaspersky Security Center. Si la casilla de verificación está seleccionada, los elementos de la lista de la directiva principal de Kaspersky Security Center se muestran en las directivas secundarias. De esta manera, puede, por ejemplo, crear una lista consolidada de dispositivos de confianza para toda la organización. Los elementos de lista heredados de una directiva secundaria no se pueden eliminar ni editar. Los elementos de la lista de dispositivos de confianza que se fusionan durante la herencia se pueden eliminar y editar solo en la directiva principal. Puede añadir, modificar o eliminar elementos de la lista en las directivas de nivel inferior. Si los elementos de las listas de la directiva principal y secundaria coinciden, estos elementos se muestran como el mismo elemento de la directiva principal. Si la casilla de verificación no está seleccionada, los elementos de las listas no se combinan al heredar la configuración de las directivas de Kaspersky Security Center. Esta funcionalidad también permite fusionar listas en perfiles de directivas. Para fusionar listas, en el perfil de mayor prioridad, active la herencia de la configuración de un perfil de menor prioridad. Para obtener más información sobre las prioridades de los perfiles de directivas, consulte la Ayuda de Kaspersky Security Center.
Anti-Bridging	Anti-Bridging impide establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red. La finalidad es resguardar la red de la empresa de los ataques que puedan realizarse a través de redes desprotegidas y no autorizadas. Para bloquear la posibilidad de establecer más de una conexión, Anti-Bridging tiene en cuenta las prioridades de los dispositivos. Cuanto más arriba en la lista se encuentra un dispositivo, mayor es su prioridad. Cuando una conexión activa y una conexión nueva son del mismo tipo (por ejemplo, wifi), Kaspersky Endpoint Security bloquea la conexión activa y permite que se establezca la conexión nueva. Cuando una conexión activa y una conexión nueva no son del mismo tipo (por ejemplo, adaptador de red y wifi), Kaspersky Endpoint Security bloquea la conexión de menor prioridad y autoriza la de mayor prioridad. Anti-Bridging puede operar con los siguientes tipos de dispositivos: adaptador de red, wifi y módem.
Modelos de mensajes	**Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo. **Mensaje para el administrador**. Una plantilla del mensaje que se envía al administrador de la LAN cuando el usuario cree que el acceso al dispositivo está bloqueado o que se ha prohibido una operación con el contenido del dispositivo por error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso al dispositivo**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

Control de aplicaciones

El Control de aplicaciones gestiona el inicio de aplicaciones en los equipos de los usuarios. Esto le permite implementar una directiva corporativa de seguridad al usar aplicaciones. El Control de aplicaciones también reduce el riesgo de infección del equipo al restringir el acceso a las aplicaciones.

La configuración del Control de aplicaciones consta de los siguientes pasos:

1. Creación de categorías de aplicaciones.

   El administrador crea categorías de aplicaciones que el administrador quiere gestionar. Las categorías de aplicaciones están destinadas a todos los equipos de la red corporativa, independientemente de los grupos de administración. Para crear una categoría, puede usar los siguientes criterios: categoría KL (por ejemplo, *Navegadores*) u otra categoría, hash de archivo, proveedor de aplicaciones y otros criterios.

2. Crear reglas de Control de aplicaciones.

   El administrador crea reglas de Control de aplicaciones en la directiva para el grupo de administración. La regla incluye las categorías de aplicaciones y el estado de inicio de las aplicaciones de estas categorías: bloqueadas o permitidas. El administrador puede crear muchas reglas. Una aplicación puede coincidir con los criterios de varias reglas. La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. Kaspersky Endpoint Security comprueba si una aplicación coincide con una regla cada vez que se inicia. Kaspersky Endpoint Security compara secuencialmente la aplicación con todas las reglas de Control de aplicaciones.

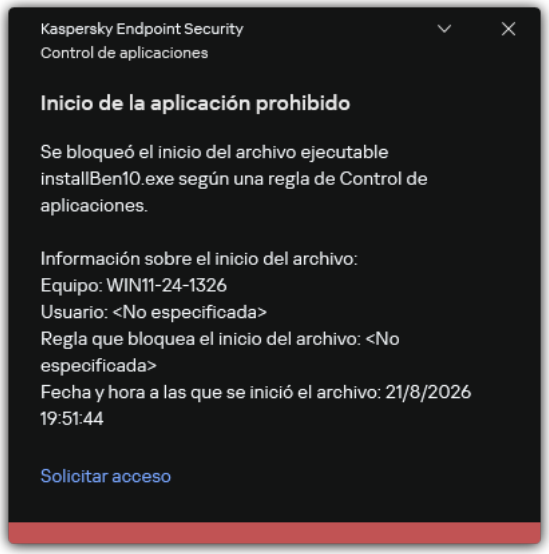
3. Seleccionar el modo de Control de aplicaciones.

   El administrador elige el modo para trabajar con las aplicaciones que no estén incluidas en ninguna de las reglas (listas de aplicaciones admitidas y rechazadas).

Cuando un usuario intenta iniciar una aplicación prohibida, Kaspersky Endpoint Security bloqueará el inicio de dicha aplicación y mostrará una notificación (vea la figura a continuación).

Se proporciona un *modo de prueba* para comprobar la configuración de Control de aplicaciones. En este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite el inicio de aplicaciones, incluidas las prohibidas.
- Muestra una notificación sobre el inicio de una aplicación prohibida y añade información al informe en el equipo del usuario.
- Envía datos sobre el inicio de aplicaciones prohibidas a Kaspersky Security Center.



Notificación de Control de aplicaciones

Modos de funcionamiento de Control de aplicaciones

El componente Control de aplicaciones funciona en dos modos:

- **Lista de rechazados**. En este modo, Control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de Control de aplicaciones.

  Este modo de Control de aplicaciones está activado de forma predeterminada.

- **Lista de permitidos**. En este modo, Control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de Control de aplicaciones.

  Si las reglas de autorización de Control de aplicaciones están totalmente configuradas, el componente bloquea el inicio de todas las aplicaciones nuevas que no haya verificado el administrador de la red de área local, mientras que autoriza el funcionamiento del sistema operativo y de las aplicaciones de confianza en las que los usuarios confían en su trabajo.

  Puede leer las recomendaciones sobre la configuración de reglas de Control de aplicaciones en el modo de lista de admitidos.

El Control de aplicaciones puede configurarse para que funcione en estos modos tanto mediante la interfaz local de Kaspersky Endpoint Security como mediante Kaspersky Security Center.

Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas que son necesarias para las siguientes tareas:

- Creación de categorías de aplicaciones.

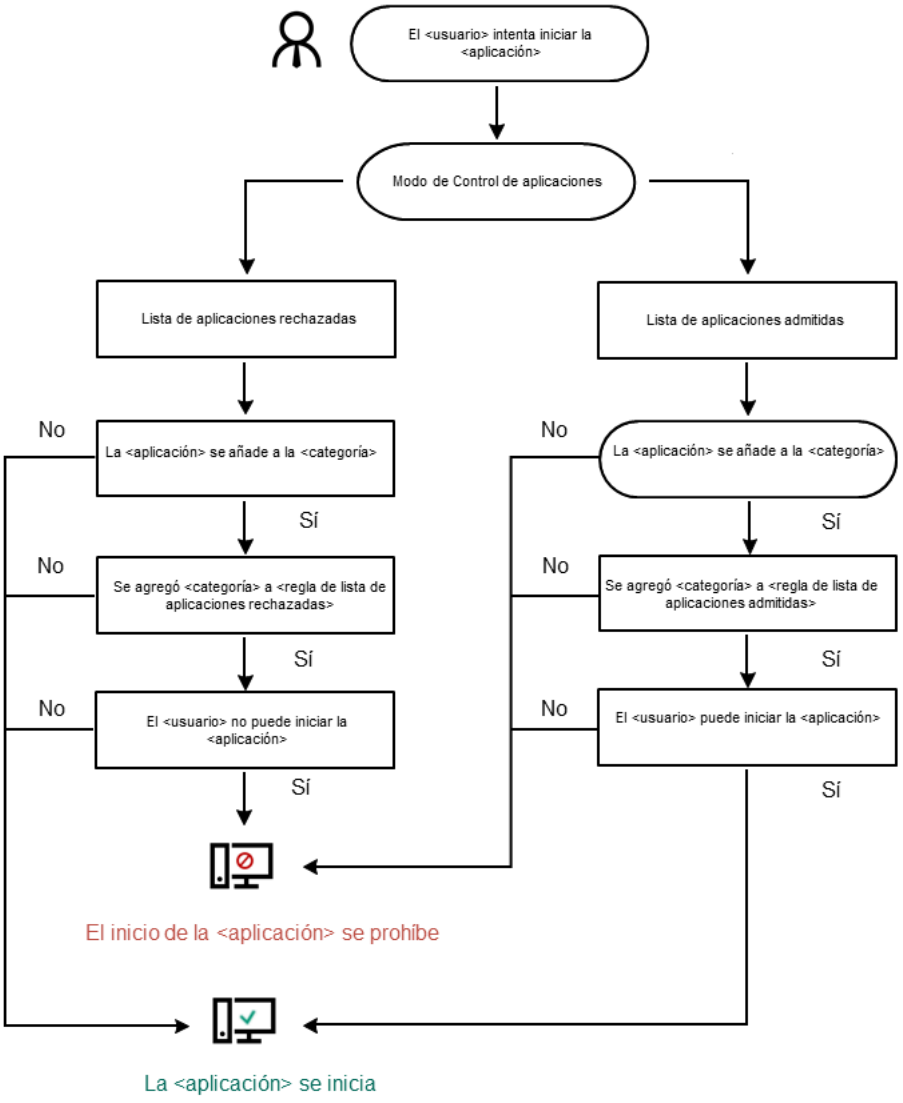
  Las reglas del componente Control de aplicaciones de la consola de administración de Kaspersky Security Center se basan en categorías de aplicaciones predeterminadas, y no en reglas de inclusión y exclusión, como sucede en la interfaz local de Kaspersky Endpoint Security.

- Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN.

Por eso, se recomienda usar Kaspersky Security Center para configurar el funcionamiento del componente Control de aplicaciones.

Algoritmo de funcionamiento de Control de aplicaciones

Kaspersky Endpoint Security utiliza un algoritmo para tomar una decisión sobre el inicio de una aplicación (vea la figura a continuación).



Algoritmo de funcionamiento de Control de aplicaciones

Parámetro	Descripción
Acción al iniciar aplicaciones bloqueadas por reglas	**Aplicar reglas**. Kaspersky Endpoint Security administra el inicio de las aplicaciones en función del modo elegido. **Probar reglas**. Kaspersky Endpoint Security permitirá que una aplicación se inicie aunque el modo de Control de aplicaciones que esté en vigor requiera bloquearla, y dejará constancia de la ejecución en el informe.
Modo de control de inicio de la aplicación	Puede elegir una de las siguientes opciones: • **Lista de rechazados**. Si se selecciona esta opción, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto las prohibidas por las condiciones de las reglas de bloqueo de Control de aplicaciones. • **Lista de permitidos**. Si se selecciona esta opción, Control de aplicaciones impide que los usuarios inicien las aplicaciones que no cumplen con las condiciones de las reglas de autorización de Control de aplicaciones. Cuando se selecciona el modo **Lista de permitidos**, se crean automáticamente dos reglas de Control de aplicaciones: • **Golden Image**. • **Actualizadores de confianza**. No puede modificar la configuración ni eliminar las reglas creadas automáticamente. Puede activar o desactivar estas reglas.
Supervisar carga de los módulos DLL	Si se selecciona, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. La información sobre el módulo de DLL y la aplicación que cargó dicho módulo se registra en el informe. Si planea activar el control sobre los controladores y módulos DLL que se carguen, asegúrese de que, en la configuración Control de aplicaciones, esté activada la regla **Golden Image** predeterminada u otra regla que contenga la categoría KL "**Golden Image\Certificados de confianza**" y garantice que los controladores y módulos DLL de confianza se carguen antes de que se inicie Kaspersky Endpoint Security. Activar la supervisión de la carga de los módulos DLL y los controladores cuando la regla **Golden Image** esté desactivada puede causar inestabilidad en el sistema operativo. Kaspersky Endpoint Security solamente supervisa los controladores y módulos DLL que se carguen desde el momento en que se selecciona la casilla de verificación. Después de seleccionar la casilla de verificación, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.
Usar verificación de firma digital estricta	Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si esta casilla está seleccionada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas con certificados solo del almacén de certificados del sistema de confianza. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección; por ejemplo, la tarea *Análisis antimalware*. Sin embargo, si especifica un certificado de un almacén tienda diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla. Si la casilla está desactivada, Kaspersky Endpoint Security aplica reglas a las aplicaciones firmadas por un certificado de la tienda de certificados raíz de confianza de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección supervisan la actividad de dichas aplicaciones.
Plantillas de mensajes sobre el bloque de aplicaciones	**Mensaje sobre el bloqueo**. Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación. **Mensaje para el administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del inicio de la aplicación**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

Control de anomalías adaptativo

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos en una red de la empresa. El Control de anomalías adaptativo utiliza un conjunto de reglas para supervisar el comportamiento atípico (por ejemplo, la regla *Inicio de Microsoft Powershell desde una aplicación de Office*). Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa. Puede configurar el modo en que el Control de anomalías adaptativo gestiona cada regla y, por ejemplo, permitir la ejecución de scripts de PowerShell que automatizan determinadas tareas de flujo de trabajo. Kaspersky Endpoint Security actualiza el conjunto de reglas junto con las bases de datos de la aplicación. Las actualizaciones de los conjuntos de reglas deben confirmarse manualmente.

Parámetros del Control de anomalías adaptativo

Para configurar el Control de anomalías adaptativo se tienen que realizar los pasos siguientes:

1. Autoaprendizaje del Control de anomalías adaptativo.

   Después de habilitar el Control de anomalías adaptativo, sus reglas funcionan en el *modo de autoaprendizaje*. Durante el aprendizaje, el Control de anomalías adaptativo supervisa la activación de reglas y envía eventos de activación a Kaspersky Security Center. Cada regla tiene su propia duración del modo de autoaprendizaje. La duración del modo de autoaprendizaje es establecida por los expertos de Kaspersky. Por lo general, el modo de autoaprendizaje está activo durante dos semanas.

   Si una regla no se ha activado nunca durante el autoaprendizaje, el Control de anomalías adaptativo considerará las acciones asociadas a esta regla como no típicas. Kaspersky Endpoint Security bloqueará todas las acciones asociadas a esa regla.

   Si se activó una regla durante el autoaprendizaje, Kaspersky Endpoint Security registra los eventos en el informe de activación de las reglas y en el repositorio de **Activación de reglas en el estado Aprendizaje inteligente**.

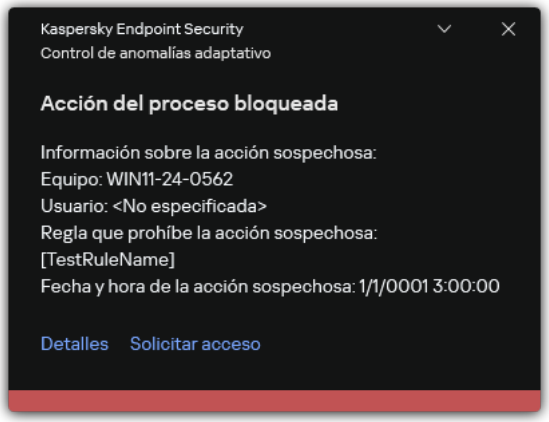
2. Analizar el informe de activación de las reglas.

   El administrador analiza el informe de activación de reglas o el contenido del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. A continuación, el administrador puede seleccionar el comportamiento del Control de anomalías adaptativo cuando se active la regla para bloquearlo o permitirlo. El administrador también puede seguir supervisando el funcionamiento de la regla y ampliar su duración durante el modo de autoaprendizaje. Si el administrador no realiza ninguna acción, la aplicación también seguirá funcionando en el modo de autoaprendizaje. El plazo de aprendizaje se reiniciará.

El Control de anomalías adaptativo se configura en tiempo real a través de los siguientes canales:

- El Control de anomalías adaptativo empieza a bloquear automáticamente las acciones asociadas con las reglas que no se activaron nunca en el modo de autoaprendizaje.
- Kaspersky Endpoint Security añade nuevas reglas o elimina las obsoletas.
- El administrador configura el funcionamiento del Control de anomalías adaptativo tras revisar el informe de activación de las reglas o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. Recomendamos consultar el informe sobre la activación de reglas y el contenido del almacenamiento de **Activación de reglas en el estado Aprendizaje inteligente**.

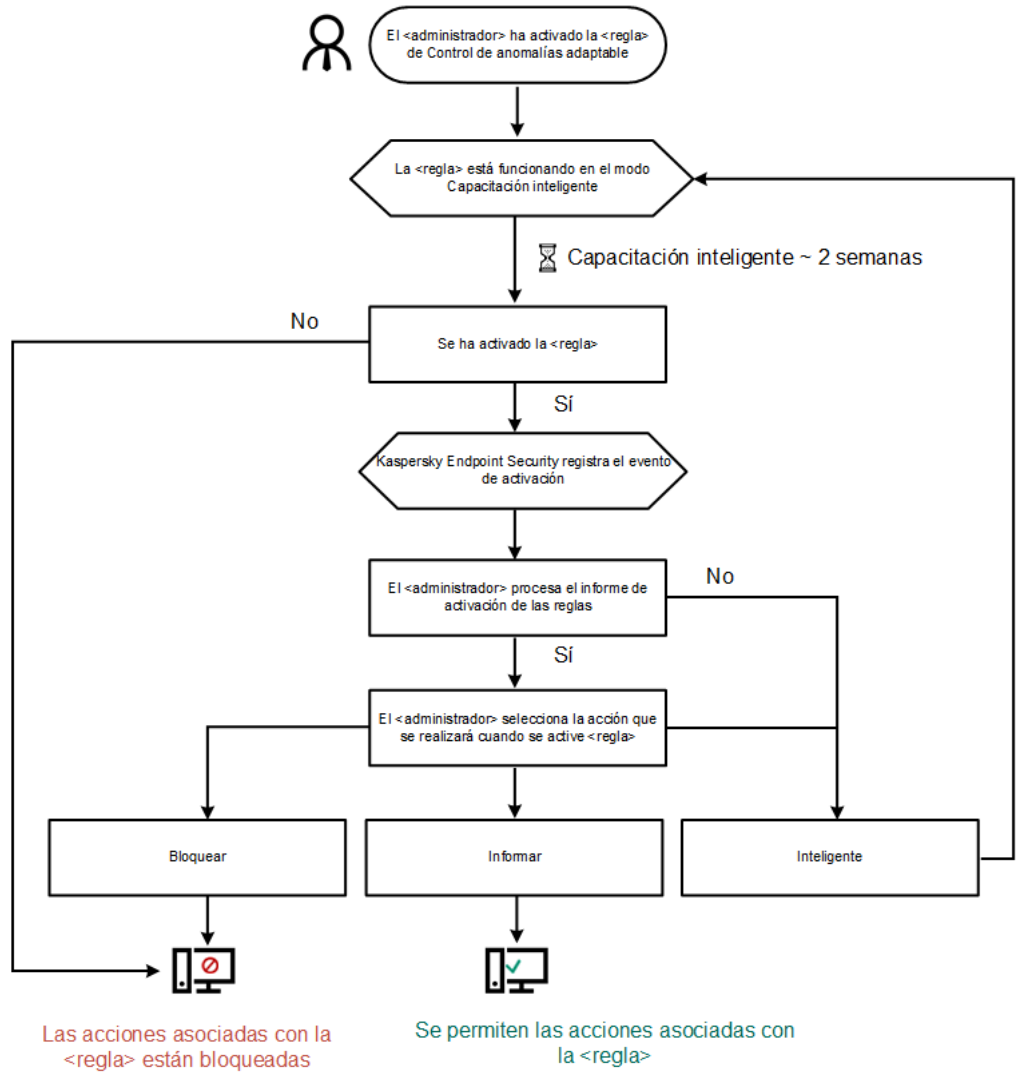
Cuando una aplicación maliciosa intenta realizar una acción, Kaspersky Endpoint Security bloqueará dicha acción y mostrará una notificación (vea la figura a continuación).



Notificación del Control de anomalías adaptativo

Algoritmo de funcionamiento del Control de anomalías adaptativo

Kaspersky Endpoint Security decide si se autoriza o se bloquea una acción que esté asociada con una regla de acuerdo al siguiente algoritmo (consulte la siguiente figura).



Algoritmo de funcionamiento del Control de anomalías adaptativo

Parámetros del componente Control de anomalías adaptativo

Parámetro	Descripción
Informe de estado de reglas de Control de anomalías adaptativo *(disponible solo en la Consola de Kaspersky Security Center)*	Este informe contiene información sobre el estado de las reglas de detección del Control de anomalías adaptativo (por ejemplo, la regla *Desactivado* o *Bloquear*). Este informe se genera para todos los grupos de administración.
Informe de reglas de Control de anomalías adaptativo activado *(disponible solo en la Consola de Kaspersky Security Center)*	Este informe contiene información sobre las acciones no típicas detectadas al usar el Control de anomalías adaptativo. Este informe se genera para todos los grupos de administración.

Parámetro	Descripción
Reglas	Tabla de reglas del Control de anomalías adaptativo Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa.
Plantillas	**Mensaje sobre el bloqueo**. Plantilla del mensaje que se muestra a un usuario cuando se activa una regla del Control de anomalías adaptativo que bloquea una acción no típica. **Mensaje para el administrador**. Plantilla del mensaje que un usuario puede enviar al administrador de la red corporativa local si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo de la actividad de aplicaciones**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de los usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

Control de integridad del sistema

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo.

A partir de la versión 12.6, Kaspersky Endpoint Security para Windows incluye el componente Control de integridad del sistema en lugar del componente Monitor de integridad de archivos. El componente Control de integridad del sistema incluye todas las funciones de Monitor de integridad de archivos y, además, permite supervisar los cambios en el registro y la conexión de dispositivos externos.

El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que pueden indicar infracciones de la seguridad del equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos correspondientes y alerta al administrador. El Control de integridad del sistema puede funcionar en tiempo real y también puede realizar comprobaciones de la integridad del sistema a demanda.

Control de integridad del sistema en tiempo real

En modo de tiempo real, el Control de integridad del sistema rastrea los cambios en los objetos que incluyó en la cobertura del componente (la *cobertura de la supervisión*). El Control de integridad del sistema también permite bloquear el acceso no autorizado a dichos objetos en tiempo real.

Comprobación de integridad del sistema a demanda

La Comprobación de integridad del sistema a demanda es una tarea que puede ejecutar manualmente o según una programación. Para ejecutar la tarea *Comprobación de la integridad del sistema*, debe configurar el alcance del componente (la *cobertura de la supervisión*) y crear una línea de base. Una *línea de base* es un estado registrado de los objetos en el sistema, que la aplicación utiliza como referencia al comparar con el estado actual.

Configuración del Monitor de integridad de archivos

Parámetro	Descripción
Modo de funcionamiento de las reglas de bloqueo	• **Bloquear**. En este modo, el Control de integridad del sistema bloquea las acciones con archivos y claves de registro de la cobertura de la supervisión y genera un evento correspondiente. • **Informar**. En este modo, el Control de integridad del sistema permite acciones con archivos y claves de registro desde el cobertura de la supervisión y genera un evento correspondiente.

Parámetro	Descripción
Control de integridad del sistema en tiempo real	En modo de tiempo real, el Control de integridad del sistema rastrea los cambios en los objetos que incluyó en la cobertura del componente (la *cobertura de la supervisión*). El Control de integridad del sistema también permite bloquear el acceso no autorizado a dichos objetos en tiempo real.
Supervisar dispositivos	El Control de integridad del sistema supervisa la conexión y desconexión de dispositivos externos.
Supervisar archivos y el registro	El Control de integridad del sistema supervisa los cambios en los archivos, las carpetas y el registro.
Comprobación de la integridad del sistema	La Comprobación de integridad del sistema a demanda es una tarea que puede ejecutar manualmente o según una programación. Para ejecutar la tarea *Comprobación de la integridad del sistema*, debe configurar el alcance del componente (la *cobertura de la supervisión*) y crear una línea de base. Una *línea de base* es un estado registrado de los objetos en el sistema, que la aplicación utiliza como referencia al comparar con el estado actual.

Endpoint Sensor

Kaspersky Endpoint Security 11.4.0 no incluye Endpoint Sensor.

Puede administrar el Endpoint Sensor en Kaspersky Security Center Web Console y en la Consola de administración de Kaspersky Security Center. No se puede administrar el Endpoint Sensor en Kaspersky Security Center Cloud Console.

Endpoint Sensor está diseñado para interactuar con Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* es una solución diseñada para detener a tiempo amenazas sofisticadas, como ataques dirigidos, amenazas persistentes avanzadas (APT) y ataques de día cero, entre otras. Kaspersky Anti Targeted Attack Platform incluye tres unidades funcionales:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Puede comprar todas las unidades funcionales o unidades funcionales individuales por separado. Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

La administración de Endpoint Sensor tiene las siguientes limitaciones:

- Puede configurar Endpoint Sensor en una directiva siempre que la versión de Kaspersky Endpoint Security instalada en el equipo sea de la 11.0.0 a la 11.3.0. Para obtener más información sobre cómo configurar Endpoint Sensor utilizando la directiva, consulte los artículos de ayuda de las versiones anteriores de Kaspersky Endpoint Security.
- Si la versión de Kaspersky Endpoint Security instalada en el equipo es la 11.4.0 o posterior, no podrá configurar Endpoint Sensor en la directiva.

Endpoint Sensor se instala en los equipos cliente. Una vez instalado, vigila de forma constante los procesos, las conexiones de red activas y los archivos que se modifican en esos equipos. El componente remite entonces la información al servidor de KATA.

La funcionalidad del componente está disponible con estos sistemas operativos:

- Windows 7 Service Pack 1 Home/Professional/Enterprise;
- Windows 8.1.1 Professional/Enterprise;
- Windows 10 RS3 Home/Professional/Education/Enterprise;
- Windows 10 RS4 Home/Professional/Education/Enterprise;
- Windows 10 RS5 Home/Professional/Education/Enterprise;
- Windows 10 RS6 Home/Professional/Education/Enterprise;
- Windows Server 2008 R2 Foundation/Standard/Enterprise (64 bits);
- Windows Server 2012 Foundation/Standard/Enterprise (64 bits);
- Windows Server 2012 R2 Foundation/Standard/Enterprise (64 bits);
- Windows Server 2016 Essentials/Standard (64 bits).

Para obtener más información sobre el funcionamiento de KATA, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

Sandbox

Kaspersky Endpoint Security para Windows incorpora un agente para la integración con Kaspersky Sandbox. El componente *Sandbox* detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Sandbox analiza el comportamiento de los objetos para detectar la actividad maliciosa y la actividad característica de los ataques dirigidos a la infraestructura de TI de la organización. Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Sandbox). Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Sandbox y la Ayuda de Kaspersky Anti Targeted Attack Platform.

A partir de la versión 12.7, Kaspersky Endpoint Security para Windows admite el componente Sandbox que forma parte de la solución Kaspersky Anti Targeted Attack Platform. A diferencia de la solución Kaspersky Sandbox, el componente KATA Sandbox permite analizar archivos no solo automáticamente, sino también manualmente desde el menú contextual del archivo.

KATA Sandbox requiere la implementación de Kaspersky Anti Targeted Attack Platform 7.0 o posterior.

El componente solo se puede administrar mediante Kaspersky Security Center Web Console. No puede administrar este componente mediante la Consola de administración (MMC).

Configuración del componente Sandbox

Parámetro	Descripción
Modo de integración	**Kaspersky Sandbox**. Integración con la solución Kaspersky Sandbox. La aplicación envía archivos para analizar en Kaspersky Sandbox solo en modo automático. **KATA Sandbox**. Integración con el componente Sandbox de la solución Kaspersky Anti Targeted Attack Platform. Puede seleccionar el modo de envío de archivos para su análisis: • **Manual**. El usuario envía manualmente el archivo para su análisis desde el menú contextual (**Enviar a Sandbox**). • **Automático**. La aplicación detecta objetos automáticamente y los envía a Sandbox para su análisis. • **Combinado**.
Configuración de conexión a servidor	**Tiempo de espera (mseg)**. Tiempo de espera de conexión para el servidor de Sandbox (para Kaspersky Sandbox) o el servidor de Central Node (para KATA). Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de espera de conexión del servidor si su velocidad de conexión es baja o si la conexión es inestable. El tiempo de espera recomendado para las solicitudes es de 0,5 segundos o menos. **Cola de peticiones**. Tamaño de la carpeta de cola de solicitudes. Al enviar varios objetos para su análisis en Sandbox, Kaspersky Endpoint Security crea una cola de solicitudes. De forma predeterminada, el tamaño de la carpeta de cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Sandbox deja de añadir nuevas solicitudes a la cola y envía el evento correspondiente a Kaspersky Security Center. Puede configurar el tamaño de la carpeta de cola de solicitudes en función de la configuración de su servidor. **Certificado TLS del servidor**. Para configurar una conexión de confianza con el servidor de Sandbox (para Kaspersky Sandbox) o el servidor de Central Node (para KATA), debe preparar un certificado TLS. A continuación, debe añadir el certificado al equipo mediante el uso de una directiva. También debe añadir el certificado al servidor de Sandbox (para Kaspersky Sandbox) o al servidor de Central Node (para KATA). **Usar autenticación bidireccional** (solo para KATA Sandbox). Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.
Conexión a servidores Sandbox	**Kaspersky Sandbox**. Configuración de la conexión del servidor de Sandbox. Los servidores utilizan imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows para ejecutar objetos que se deben analizar. Puede introducir una dirección IP (IPv4 o IPv6) o un nombre de dominio completo. **KATA Sandbox**. Configuración de conexión del servidor de Central Node. Central Node elige la configuración óptima para el análisis y equilibra la carga entre los servidores de Sandbox.
Acción al detectar una amenaza	**Mover la copia a la cuarentena, eliminar objeto**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena. **Ejecutar análisis de áreas críticas**. Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco. **Crear tarea de Análisis de IOC**. Si se selecciona esta opción, Kaspersky Endpoint Security crea la tarea *Análisis de IOC automáticamente (tarea de análisis de IOC autónoma)*. Para esta tarea, puede configurar el modo de ejecución, la cobertura del análisis y la acción al detectar un IOC (*Mover la copia a la cuarentena, eliminar objeto* o *Ejecutar análisis de áreas críticas*). Para modificar otros parámetros de la tarea *Análisis de IOC*, vaya a la configuración de la tarea.
Cobertura del Análisis de IOC	**Áreas críticas de archivos**. Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC solo en áreas críticas de archivos del equipo: memoria del núcleo y sectores de arranque. **Áreas de archivos en la unidad de sistema del equipo**. Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC en la unidad de sistema del equipo.
Ejecute la tarea de Análisis de IOC	**Manual**. Modo de ejecución en el que puede ejecutar la tarea *Análisis de IOC* manualmente en el momento que sea conveniente para usted. **Automático**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea *Análisis de IOC* automáticamente después de detectar una amenaza. **Ejecutar solo cuando el equipo está inactivo**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea *Análisis de IOC* si el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security pausa la tarea. Esto significa que la tarea puede tardar varios días en completarse.

Managed Detection and Response

Kaspersky Endpoint Security para Windows admite la integración con la solución Managed Detection and Response. La solución *Kaspersky Managed Detection and Response (MDR)* detecta y analiza automáticamente los incidentes de seguridad en su infraestructura. Para hacerlo, MDR utiliza datos de telemetría recibidos de endpoints y aprendizaje automático. MDR envía datos de incidentes a los expertos de Kaspersky. Luego, los expertos pueden procesar el incidente y, por ejemplo, añadir una nueva entrada a las bases de datos antivirus. De manera alternativa, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener información detallada sobre cómo funciona la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Configuración de Managed Detection and Response

Parámetro	Descripción
Archivo de configuración de MDR	El archivo BLOB contiene el ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra dentro del archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener información detallada sobre un archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

Endpoint Detection and Response

Kaspersky Endpoint Security para Windows incluye un agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante también "EDR Optimum"). A partir de la versión 11.8.0, Kaspersky Endpoint Security para Windows incluye un agente integrado para la solución Kaspersky Endpoint Detection and Response Expert (en adelante también "EDR Expert"). *Kaspersky Endpoint Detection and Response* es una variedad de soluciones para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de las soluciones combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware y ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre las soluciones, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

Kaspersky Endpoint Detection and Response examina y analiza el desarrollo de amenazas e informa al *personal de seguridad* o al *Administrador* del posible ataque, para permitir una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana separada. Una *alerta* es un evento en la infraestructura de TI corporativa que la aplicación ha identificado como inusual o sospechoso, y que puede suponer una amenaza para la seguridad de dicha infraestructura. *Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum y la Ayuda de Kaspersky Endpoint Detection and Response Expert.

Puede configurar el componente Endpoint Detection and Response Optimum en Web Console y Cloud Console. La configuración del componente Endpoint Detection and Response Expert (cloud) solo está disponible en Cloud Console.

Parámetro	Descripción
Activar registro de actividad del sistema avanzado	La telemetría ampliada mejora la precisión de la detección de IOC, pero utiliza más recursos del equipo. Recomendamos activar la telemetría ampliada en el equipo para el análisis de IOC retrospectivo. *Análisis de IOC retrospectivo* es un modo de la tarea *Análisis de IOC* en la que Kaspersky Endpoint Security analiza en busca de indicadores de compromiso utilizando datos durante un período de tiempo determinado. Este modo está diseñado para buscar indicadores de compromiso mediante la telemetría del equipo protegido, como la actividad de la red, los procesos, los archivos y otra telemetría. Si la telemetría ampliada está desactivada, Kaspersky Endpoint Security puede rotar la información sobre los indicadores de compromiso detectados.
Aislamiento de red	Aislamiento automático del equipo de la red en respuesta a amenazas detectadas. Cuando el aislamiento de red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones TCP/IP nuevas en el equipo. La aplicación deja solo las siguientes conexiones activas: • Conexiones enumeradas en exclusiones de aislamiento de red. • Conexiones iniciadas por los servicios de Kaspersky Endpoint Security. • Conexiones iniciadas por el Agente de red de Kaspersky Security Center.
Desbloquear automáticamente el dispositivo aislado en (horas)	El aislamiento de red se puede desactivar automáticamente después de un tiempo especificado o manualmente. De forma predeterminada, Kaspersky Endpoint Security desactiva el aislamiento de red 5 horas después del inicio del aislamiento.
Exclusiones de aislamiento de red	Lista de reglas para las exclusiones del aislamiento de red. Las conexiones de red que coinciden con las reglas no se bloquean en los equipos cuando el aislamiento de red está activado. Para configurar las Exclusiones de aislamiento de red, puede usar una lista de *perfiles de red estándar*. De forma predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones manualmente. Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si el aislamiento de red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center o en los detalles de la alerta.
Prevención de ejecución	Controle la ejecución de archivos ejecutables y scripts y la apertura de archivos en formato Office. Por ejemplo, puede evitar la ejecución de aplicaciones que se consideran inseguras en el equipo seleccionado. La prevención de ejecución es compatible con un conjunto de extensiones de archivos y un conjunto de intérpretes de script. Para utilizar el componente de Prevención de ejecución, debe añadir las normas de prevención de la ejecución. *Regla de prevención de ejecución* es un conjunto de criterios que la aplicación tiene en cuenta al reaccionar a la ejecución de un objeto, por ejemplo, al bloquear la ejecución de un objeto. La aplicación identifica archivos por sus rutas o sumas de comprobación calculadas mediante algoritmos hash MD5 y SHA256.
Acción al ejecutar o abrir un objeto prohibido	**Bloquear y añadir a registro de eventos**. En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Windows y en el registro de eventos de Kaspersky Security Center. **Añadir a registro de eventos**. En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de ejecutar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Windows y Kaspersky Security Center, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de forma predeterminada.
Reglas de Prevención de ejecución	*Regla de prevención de ejecución* es un conjunto de criterios que la aplicación tiene en cuenta al reaccionar a la ejecución de un objeto, por ejemplo, al bloquear la ejecución de un objeto. La aplicación identifica archivos por sus rutas o sumas de comprobación calculadas mediante algoritmos hash MD5 y SHA256.

Parámetro	Descripción
Sandbox en la nube	*Sandbox en la nube* es una tecnología que le permite detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Sandbox en la nube para su análisis. Sandbox en la nube ejecuta estos archivos en un entorno aislado para identificar actividad maliciosa y tomar una decisión sobre su reputación. A continuación, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Sandbox en la nube ha detectado un archivo malicioso, Kaspersky Endpoint Security realizará la acción adecuada para eliminar esta amenaza en todos los equipos donde se detecte este archivo. La tecnología Sandbox en la nube se activa de manera permanente y está disponible para todos los usuarios de Kaspersky Security Network, más allá del tipo de licencia que usen. Si esta casilla de verificación está marcada, Kaspersky Endpoint Security activará el contador de amenazas detectadas a través de Sandbox en la nube en la ventana principal de la aplicación, en **Tecnologías de detección de amenazas**. Kaspersky Endpoint Security también indicará la tecnología de detección de Sandbox en la nube en los eventos de aplicación y en los *Informe de amenazas* en la consola de Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security para Windows admite la integración con las soluciones de Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* es una solución de ciberseguridad empresarial que incluye aplicaciones de Kaspersky que permiten a una organización defenderse contra la mayoría de los tipos de ciberriesgos y cubrir los escenarios de propagación de amenazas más importantes. Los componentes de EDR Expert (on-premises) se implementan en la plataforma abierta de administración única (OSMP). Esta plataforma ejecuta escenarios multiplataforma en una única interfaz y permite integrar aplicaciones de Kaspersky con aplicaciones de terceros en un sistema de seguridad completo.

Uno de los elementos centrales de la solución es *SIEM*. SIEM rastrea los eventos que provienen de todos los componentes y los correlaciona entre sí mediante reglas definidas por el proveedor y el usuario. EDR Expert (on-premises) analiza los registros y la telemetría recibidos de la infraestructura corporativa para detectar ataques automáticamente y permite investigar incidentes utilizando un gráfico de investigación unificado que combina todos los eventos recopilados en EDR Expert (on-premises), incluidos eventos de aplicaciones de Kaspersky y productos de seguridad de la información de terceros.

Para responder a incidentes avanzados, EDR Expert (on-premises) utiliza escenarios predefinidos y definidos por el usuario. También puede usar acciones de respuesta de aplicaciones de terceros y escenarios de respuesta que involucren varias aplicaciones.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security para Windows permite trabajar con el componente Kaspersky Endpoint Detection and Response como parte de la solución Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* es una solución diseñada para detener a tiempo amenazas sofisticadas, como ataques dirigidos, amenazas persistentes avanzadas (APT) y ataques de día cero, entre otras. Kaspersky Anti Targeted Attack Platform incluye tres unidades funcionales:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Puede comprar todas las unidades funcionales o unidades funcionales individuales por separado. Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y supervisa continuamente los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos en el equipo (datos de telemetría) se envía al servidor de Kaspersky Anti Targeted Attack Platform. En este caso, Kaspersky Endpoint Security también envía información al servidor de Kaspersky Anti Targeted Attack Platform sobre las amenazas descubiertas por la aplicación, así como información sobre los resultados del procesamiento de estas amenazas.

La integración de EDR (KATA) y NDR (KATA) se configura en la consola de Kaspersky Security Center. A continuación, el agente integrado se administra mediante la consola de Kaspersky Anti Targeted Attack Platform, incluida la ejecución de tareas, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Configuración de Endpoint Detection and Response Expert (on-premises)

Parámetro	Descripción
Conexión a servidores de recogida de telemetría	Un *servidor de recopilación de telemetría* es un servidor que es parte de una solución SIEM que recopila, normaliza, correlaciona, analiza y almacena información sobre eventos que ocurren en el equipo. Configure lo siguiente para conectarse a los servidores de recopilación de telemetría (KUMA): • **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Tras configurar el servidor, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Dirección y **Puerto** (servidores de recopilación de telemetría)	Configuración para conectar con servidores de recopilación de telemetría. Puede introducir una dirección IP (IPv4 o IPv6). Puede añadir varias direcciones de servidores de recopilación de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.
Enviar telemetría a servidores de recogida de telemetría	Esta funcionalidad le permite desactivar por completo el envío de telemetría al servidor KATA. Por ejemplo, si usa Kaspersky Anti Targeted Attack Platform junto con otra solución que también use telemetría, puede desactivar la telemetría para KATA (EDR). Esto le permite optimizar la carga del servidor para estas soluciones. Si tiene implementados la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Threat Response en KATA (EDR). • **Enviar telemetría solo con IOA**. Permite optimizar la telemetría y enviar solo telemetría con IOA. *Indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que puede indicar un ataque dirigido. La aplicación compara el comportamiento en curso en el sistema con estas reglas y registra los eventos que son indicativos de un ataque dirigido. La aplicación utiliza la tecnología de *análisis de transmisión*, que permite el seguimiento en tiempo real de dichos eventos. • **Retraso máximo de transmisión de eventos (seg)**. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos. • **Limitar el número de paquetes de eventos por transmisión**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos. Esta función permite deshabilitar el almacenamiento en búfer de eventos antes de la sincronización con el servidor.
Activar la limitación de solicitudes	Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. Configurar parámetros de la aplicación: • **Número máximo de eventos por hora**. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora. • **Porcentaje de exceso de límite del evento**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.
Enviar solicitud de sincronización al servidor cada (min.)	Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre la configuración y las tareas de la aplicación modificada.

Parámetro	Descripción
Conexión a servidores de respuesta	A *servidor de respuesta* es un servidor para recibir y analizar datos, estudiar el comportamiento de los objetos y publicar los resultados de dichos estudios. Configure lo siguiente para la conexión de los servidores de respuesta: • **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor diferente. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la plataforma abierta de administración única (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Tras configurar el servidor, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña.
Dirección y **Puerto** (servidores de respuesta)	Configuración para conectar con servidores de respuesta. Puede introducir una dirección IP (IPv4 o IPv6). Puede añadir varias direcciones de servidores de recopilación de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

Configuración de Endpoint Detection and Response (KATA)

Parámetro	Descripción
Enviar solicitud de sincronización al servidor cada (min.)	Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre la configuración y las tareas de la aplicación modificada.
Conexión a servidores de KATA	Configure lo siguiente para la conexión del servidor de Central Node: • **Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). • **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Dirección y **Puerto** (servidores de KATA)	Configuración para conectar con los servidores de Kaspersky Anti Targeted Attack Platform. Introduzca la dirección IP (IPv4 o IPv6) y el puerto del servidor de Central Node para conectarse. Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.
Enviar telemetría a KATA	Esta funcionalidad le permite desactivar por completo el envío de telemetría al servidor KATA. Por ejemplo, si usa Kaspersky Anti Targeted Attack Platform junto con otra solución que también use telemetría, puede desactivar la telemetría para KATA (EDR). Esto le permite optimizar la carga del servidor para estas soluciones. Si tiene implementados la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Threat Response en KATA (EDR). Configurar parámetros de la aplicación: • **Retraso máximo de transmisión de eventos (seg)**. La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos. • **Número máximo de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. El valor predeterminado es de 1024 eventos.

Parámetro	Descripción
Activar la limitación de solicitudes	Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. Configurar parámetros de la aplicación: • **Número máximo de eventos por hora**. La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora. • **Porcentaje de exceso de límite del evento**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.

Network Detection and Response (KATA)

Kaspersky Endpoint Security para Windows permite trabajar con el componente Kaspersky Network Detection and Response como parte de la solución Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* es una solución diseñada para detener a tiempo amenazas sofisticadas, como ataques dirigidos, amenazas persistentes avanzadas (APT) y ataques de día cero, entre otras. Kaspersky Anti Targeted Attack Platform incluye tres unidades funcionales:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Puede comprar todas las unidades funcionales o unidades funcionales individuales por separado. Para obtener información acerca de la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y supervisa continuamente los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos en el equipo (datos de telemetría) se envía al servidor de Kaspersky Anti Targeted Attack Platform. En este caso, Kaspersky Endpoint Security también envía información al servidor de Kaspersky Anti Targeted Attack Platform sobre las amenazas descubiertas por la aplicación, así como información sobre los resultados del procesamiento de estas amenazas.

La integración de EDR (KATA) y NDR (KATA) se configura en la consola de Kaspersky Security Center. A continuación, el agente integrado se administra mediante la consola de Kaspersky Anti Targeted Attack Platform, incluida la ejecución de tareas, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Parámetro	Descripción
Configuración de conexión a servidor	**Tiempo de espera (seg)**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente. **Certificado TLS del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). **Utilizar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe activarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Tras configurar Central Node, también debe activar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security, y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Dirección y **Puerto**	Configuración para conectar con los servidores de Kaspersky Anti Targeted Attack Platform. Introduzca la dirección IP (IPv4 o IPv6) y el puerto del servidor de Central Node para conectarse. Puede añadir varias direcciones de servidor del nodo central. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.
Enviar solicitud de sincronización al servidor NDR cada (min)	Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre la configuración y las tareas de la aplicación modificada.
Retraso máximo de transmisión de eventos (seg)	La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.
Activar la limitación de solicitudes	Esta función ayuda a optimizar la carga en el servidor. Si esta funcionalidad está activada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos.
Número máximo de eventos por hora	La aplicación analiza el flujo de datos de telemetría y restringe el envío de eventos si el flujo de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. La configuración predeterminada es 3000 eventos por hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora.
Porcentaje de exceso de límite del evento	La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la relación de eventos del mismo tipo con respecto al número total de eventos supera el límite configurado en porcentaje. Kaspersky Endpoint Security reanuda el envío de eventos cuando la relación entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. El ajuste predeterminado es 15 %.

Integración de KUMA

Kaspersky Endpoint Security para Windows es compatible con la solución Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* es una solución de gestión de información y eventos (SIEM) para la infraestructura de TI de las organizaciones. KUMA permite detectar, analizar y mitigar las amenazas a la seguridad antes de que puedan causar daños.

Parámetro	Descripción
Retraso máximo al enviar eventos (seg)	La aplicación se sincroniza con el servidor para enviar eventos después de que expire el intervalo de sincronización. El valor predeterminado es 30 segundos.
Conexión a servidores KUMA	**Tiempo de espera (seg)**. Tiempo máximo de espera de una respuesta del servidor de KUMA (de forma predeterminada, el valor es de 5 segundos). Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de KUMA diferente. **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de KUMA. Puede obtener un certificado TLS en la consola de Kaspersky Unified Monitoring and Analysis Platform (consulte las instrucciones en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). Para establecer una conexión de confianza, en la consola de KUMA, en la configuración del conector tcp, debe seleccionar el **With verification** Modo TLS (consulte la configuración del conector de tipo tcp en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre KES y KUMA. Para usar la autenticación bidireccional, debe seleccionar el modo TLS **Custom PFX with client authentication** en la configuración del conector de la consola de KUMA (consulte la configuración del conector en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). A continuación, debe descargar un certificado de servidor y establecer una contraseña para proteger el contenedor criptográfico. El contenedor criptográfico debe estar protegido con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Servidores KUMA	Configuración de la conexión a los servidores de Kaspersky Unified Monitoring and Analysis Platform. Puede introducir una dirección IP (IPv4 o IPv6). Puede añadir varias direcciones de servidor de KUMA. Kaspersky Endpoint Security intenta conectarse al servidor usando la primera dirección IP. Si no se puede establecer una conexión, Kaspersky Endpoint Security intenta conectarse usando la segunda dirección IP de la lista, y así sucesivamente.

Cifrado de disco completo

Puede seleccionar una tecnología de cifrado: Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker (en adelante también llamado simplemente "BitLocker").

Cifrado de disco de Kaspersky

Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.

Después de que se hayan cifrado los discos duros del sistema, en el siguiente inicio de sesión en el equipo, el usuario debe autenticarse en el Agente de autenticación antes de que se pueda acceder a los discos duros y cargar el sistema operativo. Esto requiere la introducción de la contraseña del token o la tarjeta inteligente conectada al equipo, o bien el nombre de usuario y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local que utilice la tarea *Administrar cuentas del Agente de autenticación*. Estas cuentas se basan en las cuentas de Microsoft Windows con las que los usuarios inician sesión en el sistema operativo. También puede usar la tecnología Single Sign-On, que le permite iniciar sesión automáticamente en el sistema operativo utilizando el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

La autenticación de usuario en Agente de autenticación se puede realizar de dos maneras:

- Introduzca el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local con las herramientas de Kaspersky Security Center.
- Introduzca la contraseña de un token o una tarjeta inteligente conectados al equipo.

  El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraran usando el algoritmo de cifrado AES56, no se podrá agregar el archivo del certificado electrónico al comando.

Cifrado de unidad BitLocker

BitLocker es una tecnología de cifrado integrada en los sistemas operativos Windows. Kaspersky Endpoint Security le permite controlar y administrar BitLocker utilizando Kaspersky Security Center. BitLocker cifra los volúmenes lógicos. BitLocker no se puede utilizar para el cifrado de unidades extraíbles. Para obtener más detalles sobre BitLocker, consulte la documentación de Microsoft.

Al cifrar el disco, BitLocker coloca el cargador de arranque y otros archivos auxiliares en la system partition. Esta partición no está cifrada. El sistema operativo crea la partición del sistema automáticamente durante la instalación de Windows. Si el disco está completamente particionado antes de instalar Windows, el sistema operativo no puede crear una partición del sistema. En este caso, cuando inicia el cifrado de disco de BitLocker, el sistema operativo le solicita que vuelva a particionar el disco y cree una partición del sistema. Después de crear una partición del sistema, el sistema operativo inicia el cifrado de BitLocker.

BitLocker proporciona almacenamiento seguro de claves de acceso utilizando un módulo de plataforma segura. Un *Trusted Platform Module* (TPM) es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del equipo e interactúa con todos los otros componentes del sistema a través del bus de hardware. Utilizar el módulo TPM es el modo más seguro de almacenar las clave de acceso de BitLocker, ya que TPM proporciona verificación de integridad del sistema antes del inicio. Sigue pudiendo cifrar unidades en un equipo sin un módulo TPM. En este caso, la clave de acceso se cifrará con una contraseña. BitLocker utiliza los siguientes métodos de autenticación:

- TPM.
- TPM y PIN.
- Contraseña.

Después de cifrar el disco duro del sistema, el usuario debe pasar por el procedimiento de autenticación de BitLocker para iniciar el sistema operativo. Después de la autenticación, BitLocker permite que el usuario inicie sesión. BitLocker no admite la tecnología Single Sign-On (SSO).

Después de cifrar una unidad, BitLocker crea una clave de recuperación. Kaspersky Endpoint Security envía la clave maestra a Kaspersky Security Center para que pueda restaurar el acceso al disco, por ejemplo, si un usuario ha olvidado su contraseña.

Si un usuario cifra un disco con BitLocker, Kaspersky Endpoint Security enviará la clave de recuperación y información sobre el cifrado de disco a Kaspersky Security Center.

Si está utilizando directivas de grupo de Windows, desactive la administración de BitLocker en la configuración de directivas. La configuración de directivas de Windows puede entrar en conflicto con la configuración de directivas de Kaspersky Endpoint Security. Al cifrar una unidad, pueden producirse errores.

Configuración del componente Cifrado de disco de Kaspersky

Parámetro	Descripción
Modo de cifrado	**Cifrar todos los discos duros**. Si se selecciona esta opción, la aplicación cifra todos los discos duros cuando se aplica la directiva. Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo con la aplicación instalada. **Descifrar todos los discos duros**. Si se selecciona esta opción, la aplicación descifra todas las unidades de disco duro cifradas previamente cuando se aplica la directiva. **Dejar sin modificar**. Si se selecciona este elemento, la aplicación revierte el estado de todas las unidades de disco duro cuando se aplica la directiva. Si se cifró la unidad de disco, permanecerá cifrada. Si se descifró, permanecerá descifrada. Este elemento está seleccionado de forma predeterminada.
Durante el cifrado, crear automáticamente cuentas del Agente de autenticación para usuarios de Windows	Si esta casilla de verificación está seleccionada, la aplicación creará cuentas de agente de autenticación según la lista de cuentas de usuario de Windows en el equipo. De forma predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario ha iniciado sesión en el sistema operativo durante los últimos 30 días.
Configuración de la creación de cuentas del Agente de autenticación	**Todas las cuentas del equipo**. Todas las cuentas en el equipo que han estado activas en algún momento. **Todas las cuentas de dominio del equipo**. Todas las cuentas del equipo que pertenecen a algún dominio y que han estado activas en algún momento. **Todas las cuentas locales del equipo**. Todas las cuentas locales en el equipo que han estado activas en algún momento. **Cuenta de servicio con una contraseña única**. La cuenta de servicio es necesaria para acceder al equipo, por ejemplo, cuando el usuario olvida la contraseña. También puede utilizar la cuenta de servicio como cuenta de reserva. Debe introducir el nombre de la cuenta (por defecto, `ServiceAccount`). Kaspersky Endpoint Security crea una contraseña automáticamente. Puede encontrar la contraseña en la consola de Kaspersky Security Center. **Administrador local**. Kaspersky Endpoint Security crea una cuenta de usuario del Agente de autenticación para el administrador local del equipo. **Administrador del equipo**. Kaspersky Endpoint Security crea una cuenta de usuario del Agente de autenticación para la cuenta del administrador del equipo. Puede ver qué cuenta tiene la función de administrador del equipo en las propiedades del equipo en Active Directory. Por defecto, la función de administrador del equipo no está definida, es decir, no corresponde a ninguna cuenta. **Cuenta activa**. Kaspersky Endpoint Security crea automáticamente una cuenta de agente de autenticación para la cuenta que está activa en el momento del cifrado del disco.
Crear automáticamente cuentas del Agente de autenticación para todos los usuarios de este equipo al iniciar sesión	Si esta casilla de verificación está seleccionada, la aplicación verifica la información sobre las cuentas de usuario de Windows en el equipo antes de iniciar el Agente de autenticación. Si Kaspersky Endpoint Security detecta una cuenta de usuario de Windows que no tiene una cuenta de Agente de autenticación, la aplicación creará una nueva cuenta para acceder a las unidades cifradas. La nueva cuenta del Agente de autenticación tendrá la siguiente configuración predeterminada: inicio de sesión protegido con contraseña únicamente y cambio de contraseña en la primera autenticación. Por lo tanto, no es necesario agregar manualmente cuentas del Agente de autenticación mediante la tarea *Administrar cuentas del Agente de autenticación* para equipos con unidades ya cifradas.
Guardar el nombre de usuario introducido en el Agente de autenticación	Si se selecciona la casilla de verificación, la aplicación guarda el nombre de la cuenta del Agente de Autenticación. No se le solicitará introducir el nombre de la cuenta la próxima vez que intente realizar una autorización en el Agente de autenticación con la misma cuenta.

Parámetro	Descripción
Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)	Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado. Activar o desactivar la función **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado. Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden. Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente. Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De forma predeterminada, la casilla de verificación está desactivada.
Utilizar Legacy USB Support (no recomendado)	Esta casilla de verificación activa o desactiva la función Legacy USB Support. *Legacy USB Support* **es** una función BIOS/UEFI que le permite usar dispositivos USB (como un token de seguridad) durante la fase de inicio del equipo antes de iniciar el sistema operativo (modo BIOS). Legacy USB Support no afecta a la compatibilidad con dispositivos USB después del inicio del sistema operativo. Si la casilla está seleccionada, se activará la compatibilidad con dispositivos USB durante el primer inicio del equipo. Cuando la función Legacy USB Support está activada, el Agente de autenticación en el modo BIOS no permite trabajar con tokens a través de USB. Se recomienda usar esta opción solo cuando existe un problema de compatibilidad de hardware y solo para los equipos en los cuales se produce el problema.
Configuración de contraseña	Configuración de seguridad de la contraseña de la cuenta del Agente de autenticación. Cuando se utiliza la tecnología de inicio de sesión único, el Agente de autenticación ignora los requisitos de seguridad de la contraseña especificados en Kaspersky Security Center. Puede definir los requisitos de seguridad de la contraseña en la configuración del sistema operativo.
Utilizar la tecnología de inicio de sesión único (SSO)	La tecnología SSO posibilita el uso de las mismas credenciales de la cuenta para acceder a unidades de disco duro cifradas e iniciar sesión en el sistema operativo. Si la casilla está seleccionada, debe introducir las credenciales de la cuenta para acceder a los discos duros cifrados y, luego, iniciar sesión automáticamente en el sistema operativo. Si la casilla se desactiva, para acceder a discos duros cifrados y posteriormente iniciar sesión en el sistema operativo, debe escribir por separado las credenciales para acceder a unidades cifradas y las credenciales de la cuenta de usuario del sistema operativo.
Ajustar proveedores de credenciales de terceros	Kaspersky Endpoint Security es compatible con el proveedor de credenciales de terceros ADSelfService Plus. Al trabajar con proveedores de credenciales de terceros, el agente de autenticación intercepta la contraseña antes de que se cargue el sistema operativo. Esto significa que un usuario debe introducir la contraseña una sola vez al iniciar sesión en Windows. Después de iniciar sesión en Windows, el usuario puede utilizar las capacidades del proveedor de credenciales de terceros para la autenticación en servicios corporativos, por ejemplo. Los proveedores de credenciales de terceros también permiten que los usuarios restablezcan su propia contraseña de forma independiente. En este caso, Kaspersky Endpoint Security actualizará automáticamente la contraseña para el agente de autenticación. Si está utilizando un proveedor de credenciales de terceros que no es compatible con la aplicación, es posible que encuentre algunas limitaciones en la operación de la tecnología de inicio de sesión único.
Ayuda	**Autenticación**. Texto de ayuda que aparece en la ventana del Agente de autenticación al introducir las credenciales de la cuenta. **Cambiar la contraseña**. Texto de ayuda que aparece en la ventana del Agente de autenticación al cambiar la contraseña de la cuenta del Agente de autenticación. **Recuperar la contraseña**. Texto de ayuda que aparece en la ventana del Agente de autenticación al recuperar la contraseña de la cuenta del Agente de autenticación.

Parámetro	Descripción
Modo de cifrado	**Cifrar todos los discos duros**. Si se selecciona esta opción, la aplicación cifra todos los discos duros cuando se aplica la directiva. Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo con la aplicación instalada. **Descifrar todos los discos duros**. Si se selecciona esta opción, la aplicación descifra todas las unidades de disco duro cifradas previamente cuando se aplica la directiva. **Dejar sin modificar**. Si se selecciona este elemento, la aplicación revierte el estado de todas las unidades de disco duro cuando se aplica la directiva. Si se cifró la unidad de disco, permanecerá cifrada. Si se descifró, permanecerá descifrada. Este elemento está seleccionado de forma predeterminada.
Activar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en tabletas	Uso de la autenticación que requiere la entrada de datos en un entorno de prearranque, incluso si la plataforma no tiene la capacidad de entrada de prearranque (por ejemplo, con los teclados de la pantalla táctil de las tabletas). La pantalla táctil de las tabletas no está disponible en el entorno de prearranque. Para completar la autenticación BitLocker en tabletas, el usuario debe conectar un teclado USB, por ejemplo. Si selecciona, se permite el uso de la autenticación que requiere la entrada de prearranque en las tabletas. Recomendamos utilizar esta configuración solo en dispositivos con herramientas alternativas de entrada de datos en un entorno de prearranque, como un teclado USB, además de los teclados de la pantalla táctil. Si se desactiva, el Cifrado de unidad BitLocker no es posible en tabletas.
Utilizar cifrado de hardware (Windows 8 y versiones posteriores)	Si se selecciona, la aplicación utiliza el cifrado basado en hardware, lo que le permite aumentar la velocidad de cifrado y utilizar menos recursos del equipo.
Cifrar solo el espacio en disco utilizado (Windows 8 y versiones posteriores)	Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado. Activar o desactivar la función **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado. Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden. Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente. Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De forma predeterminada, la casilla de verificación está desactivada.

Parámetro	Descripción
Método de autenticación	**Solo contraseña (Windows 8 y versiones posteriores)** Si se selecciona esta opción, Kaspersky Endpoint Security solicita una contraseña al usuario cada vez que este intenta acceder a la unidad cifrada. Se puede seleccionar cuando el módulo de plataforma segura (TPM) no se está utilizando. **Módulo de plataforma segura (TPM)** Si se selecciona esta opción, BitLocker utiliza el módulo de plataforma segura (TPM). Un *Trusted Platform Module* (TPM) es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del equipo e interactúa con todos los otros componentes del sistema a través del bus de hardware. En equipos con Windows 7 o Windows Server 2008 R2, solo es posible utilizar el cifrado con módulo TPM. El cifrado BitLocker no está disponible en equipos que no cuentan con este módulo. No es posible utilizar una contraseña en tales equipos. Un dispositivo equipado con un módulo de plataforma segura puede crear claves de cifrado que solo con dicho dispositivo se pueden descifrar. El módulo de plataforma segura cifra las claves de cifrado con su propia clave raíz de almacenamiento. La clave raíz de almacenamiento se guarda en el módulo de plataforma segura, lo que proporciona un nivel adicional de protección contra los intentos de piratear las claves de cifrado. Esta acción está seleccionada de forma predeterminada. Puede establecer una capa de protección adicional para acceder a la clave de cifrado, y cifrar la clave con una contraseña o PIN: • **Utilizar PIN para el TPM**. Si esta casilla de verificación está seleccionada, un usuario puede utilizar un código PIN para obtener acceso a una clave de cifrado almacenada en el módulo de plataforma segura (TPM). Si la casilla no está seleccionada, se prohíbe a los usuarios utilizar códigos PIN. Para acceder a la clave de cifrado, un usuario debe introducir la contraseña. • **Módulo de plataforma segura (TPM), o contraseña si el TPM no está disponible**. Si se selecciona esta opción, el usuario podrá utilizar una contraseña para acceder a claves de cifrado cuando el módulo de plataforma segura (TPM) no esté disponible. Si no se seleccionó la casilla de verificación y el módulo TPM no está disponible, no comenzará el cifrado de disco completo. El método de autenticación seleccionado debe configurarse especificando requisitos de contraseña o PIN: • **Longitud mínima de PIN (caracteres)** (el valor predeterminado es 6). • **Longitud mínima de la contraseña (caracteres)** (el valor predeterminado es 8). • **Número máximo de contraseñas/PIN almacenados** (el valor predeterminado es 5). • **Limitar el período de validez de la contraseña / PIN para el TPM (días)** (desactivado de forma predeterminada). • **Usar un PIN mejorado (letras y números)**. El *PIN optimizado* permite utilizar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios. Desactivado de forma predeterminada.
Recrear automáticamente la clave de recuperación (días)	Actualice automáticamente la contraseña para restaurar el acceso a una unidad protegida por BitLocker. Si la casilla está seleccionada, especifique el periodo de validez de la contraseña de la clave de recuperación. Esto evita que la contraseña de la clave de recuperación se reutilice.

Cifrado de archivos

El cifrado de archivos no es compatible con equipos basados en Arm.

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

Puede compilar listas de archivos por extensión o grupos de extensiones y listas de carpetas almacenadas en las unidades del equipo local, así como crear reglas para el cifrado de los archivos creados por aplicaciones específicas. Después de aplicar una directiva, Kaspersky Endpoint Security cifra y descifra los archivos siguientes:

- archivos añadidos individualmente a listas para su cifrado y descifrado;
- archivos almacenados en carpetas añadidos a listas para su cifrado y descifrado;
- Archivos creados por aplicaciones separadas.

El cifrado de archivo tiene las siguientes características especiales:

- Kaspersky Endpoint Security cifra y descifra los archivos de las carpetas predeterminadas solo para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifra ni descifra los archivos de las carpetas predeterminadas de los perfiles de usuario en itinerancia, de los perfiles de usuario obligatorio, de los perfiles de usuario temporal ni de las carpetas redirigidas.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo o aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas se encuentran en la lista de exclusiones del cifrado:
  - %WINDIR%;
  - %PROGRAMFILES% y %PROGRAMFILES(X86)%;
  - Archivos de registro de Windows.

  No se puede ver ni modificar la lista de exclusiones del cifrado. Los archivos y las carpetas de la lista de exclusiones del cifrado se pueden añadir a la lista de cifrado, pero no se cifrarán durante el cifrado de archivos.

Configuración del componente Cifrado de archivos

Parámetro	Descripción
Modo de cifrado	**Dejar sin modificar**. Si se selecciona este elemento, Kaspersky Endpoint Security no cambia los archivos ni las carpetas, los deja sin cifrar o sin descifrar. **De acuerdo con las reglas**. Si se selecciona este elemento, Kaspersky Endpoint Security cifra los archivos y las carpetas según las reglas de cifrado, descifra los archivos y las carpetas según las reglas de descifrado, y regula el acceso de las aplicaciones a los archivos cifrados según las reglas de aplicaciones. **Descifrar todos**. Si se selecciona este elemento, Kaspersky Endpoint Security descifra todos los archivos y carpetas cifrados.
Cifrado	Esta pestaña muestra las reglas de cifrado para los archivos almacenados en las unidades locales. Puede añadir archivos de la siguiente manera: • **Carpetas predeterminadas**. Kaspersky Endpoint Security le permite añadir las siguientes áreas: **Documentos**. Los archivos en la carpeta estándar *Documentos* del sistema operativo y sus subcarpetas. **Favoritos**. Los archivos en la carpeta estándar *Favoritos* del sistema operativo y sus subcarpetas. **Escritorio**. Los archivos en la carpeta estándar *Escritorio* del sistema operativo y sus subcarpetas. **Archivos temporales**. Archivos temporales relacionados con el funcionamiento de aplicaciones instaladas en el equipo. Por ejemplo, las aplicaciones de Microsoft Office crean archivos temporales que contienen copias de seguridad de documentos. **Archivos de Outlook**. Archivos relacionados con el funcionamiento del cliente de correo Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de libretas de direcciones sin conexión (OAB) y archivos de libretas de direcciones personales (PAB). • **Carpeta personalizada**. Puede introducir la ruta de la carpeta. Al añadir una ruta de carpeta, cumpla las siguientes reglas: Use una variable de entorno (por ejemplo, `%FOLDER%\UserFolder\`). Puede usar una variable de entorno solo una vez y solo al comienzo de la ruta. No use rutas relativas. No utilice los caracteres `*` y `?`. No utilice rutas UNC. Utilice `;` o `,` como carácter de separación. • **Archivos por extensión**. Puede seleccionar grupos de extensiones de la lista, como los *Archivos* del grupo de extensiones. También puede añadir la extensión del archivo de forma manual.
Descifrado	Esta pestaña muestra las reglas de descifrado para los archivos almacenados en las unidades locales.

Parámetro	Descripción
Reglas para aplicaciones	La pestaña muestra una tabla que contiene las reglas de acceso a archivos cifrados que afectan a las aplicaciones y las reglas de cifrado de los archivos que se crean o modifican mediante aplicaciones independientes.
Paquetes cifrados	Requisitos de seguridad de la contraseña que se deben cumplir al crear paquetes cifrados.

Cifrado de unidades extraíbles

El cifrado de unidades extraíbles no se admite en equipos basados en Arm.

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si una unidad extraíble con un sistema de archivos no compatible está conectada al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Para proteger los datos de las unidades extraíbles, puede usar los siguientes tipos de cifrado:

- Full Disk Encryption (FDE).

  Cifrado de toda la unidad extraíble, incluido el sistema de archivos.

  No se puede acceder a datos cifrados fuera de la red corporativa. También es imposible acceder a datos cifrados dentro de la red corporativa si el equipo no está conectado a Kaspersky Security Center (p. ej., en un equipo "invitado").

- File Level Encryption (FLE).

  Cifrado solo de los archivos en una unidad extraíble. El sistema de archivos permanece sin cambios.

  El cifrado de archivos en unidades extraíbles proporciona la capacidad de acceder a datos fuera de la red corporativa mediante un modo especial llamado *modo portátil*.

Durante el cifrado, Kaspersky Endpoint Security crea una clave maestra. Kaspersky Endpoint Security guarda la clave maestra en los siguientes repositorios:

- Kaspersky Security Center.
- Equipo del usuario.

  La clave maestra está cifrada con la clave secreta del usuario.

- Unidad extraíble.

  La clave maestra está cifrada con la clave pública de Kaspersky Security Center.

Una vez que se completa el cifrado, se puede acceder a los datos de la unidad extraíble dentro de la red corporativa como si fuera una unidad extraíble convencional sin cifrar.

Acceso a datos cifrados

Cuando se conecta una unidad extraíble con datos cifrados, Kaspersky Endpoint Security realiza las siguientes acciones:

1. Comprueba si hay una clave maestra en el almacenamiento local en el equipo del usuario.

   Si se encuentra la clave maestra, el usuario obtiene acceso a los datos en la unidad extraíble.

   Si la clave maestra no se encuentra, Kaspersky Endpoint Security realiza las siguientes acciones:

   a. Envíe una solicitud a Kaspersky Security Center.

      Después de recibir la solicitud, Kaspersky Security Center envía una respuesta que contiene la clave maestra.

   b. Kaspersky Endpoint Security guarda la clave maestra en el almacenamiento local en el equipo del usuario para operaciones posteriores con la unidad extraíble cifrada.

2. Descifre los datos.

Características especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles tiene las siguientes características especiales:

- La directiva con la configuración preestablecida para el cifrado extraíble de la unidad se forma para un grupo específico de equipos administrados. Por lo tanto, el resultado de aplicar la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al que se conecta la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra archivos de solo lectura almacenados en las unidades extraíbles.
- Los siguientes tipos de dispositivo son compatibles como unidades extraíbles:
  - Medios de datos conectados por medio del puerto USB
  - Discos duros conectados por medio de los puertos USB y FireWire
  - Unidades SSD conectadas por medio de los puertos USB y FireWire

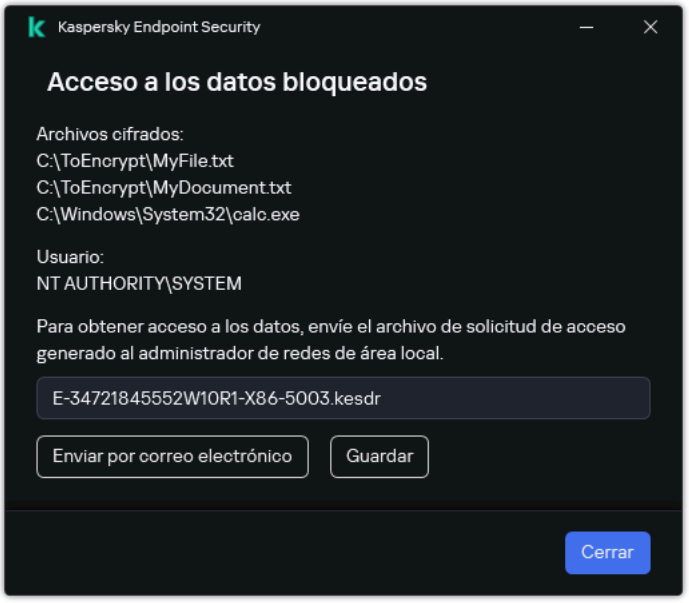
Parámetro	Descripción
Modo de cifrado	**Cifrar toda la unidad extraíble**. Si se selecciona este elemento, cuando se aplique la directiva con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará las unidades extraíbles sector a sector, incluidos sus sistemas de archivos. **Cifrar todos los archivos**. Si se selecciona este elemento, cuando se aplique la directiva con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará todos los archivos almacenados en las unidades extraíbles. Kaspersky Endpoint Security no vuelve a cifrar archivos que ya están cifrados. El contenido del sistema de archivos de una unidad extraíble, incluidos la estructura de carpetas y los nombres de archivos cifrados, no se cifrará y seguirá siendo accesible. **Cifrar solo archivos nuevos**. Si se selecciona este elemento, cuando se aplique la directiva con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará solamente los archivos que se han añadido a unidades extraíbles o que se han modificado tras la última aplicación de la directiva de Kaspersky Security Center. Conviene emplear este modo de cifrado cuando una unidad extraíble se utiliza tanto para fines personales como profesionales. Este modo de cifrado le permite mantener los antiguos archivos sin cambios y cifrar solamente los archivos que el usuario cree en un equipo de trabajo en el que se haya instalado Kaspersky Endpoint Security y se haya activado la funcionalidad de cifrado. Como resultado, el acceso a los archivos personales está siempre disponible, independientemente de si se ha instalado o no Kaspersky Endpoint Security con la funcionalidad de cifrado activada en el equipo. **Descifrar toda la unidad extraíble**. Si se selecciona este elemento, cuando se aplique la directiva con la configuración de cifrado de unidades extraíbles especificada, Kaspersky Endpoint Security descifrará todos los archivos cifrados que se hayan almacenado en las unidades extraíbles, así como los sistemas de archivos de las unidades extraíbles, en caso de haberse cifrado previamente. **Dejar sin modificar**. Si se selecciona este elemento, la aplicación revierte el estado de todas las unidades de disco duro cuando se aplica la directiva. Si se cifró la unidad de disco, permanecerá cifrada. Si se descifró, permanecerá descifrada. Este elemento está seleccionado de forma predeterminada.
Modo portátil	Esta casilla de verificación activa o desactiva la preparación de una unidad extraíble para poder acceder a los archivos almacenados en esta unidad en aquellos equipos fuera de la red corporativa. Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security solicita al usuario que especifique una contraseña antes de cifrar archivos en una unidad extraíble conforme a la aplicación de la directiva. La contraseña es obligatoria para acceder a los archivos cifrados de una unidad extraíble en aquellos equipos fuera de la red corporativa. Puede configurar la seguridad de la contraseña. El modo portátil está disponible para los modos **Cifrar todos los archivos** o **Cifrar solo archivos nuevos**.
Cifrar solo el espacio en disco utilizado	Esta casilla de verificación activa o desactiva el modo de cifrado en el que solo se cifran los sectores ocupados del disco. Se recomienda este modo para nuevas unidades cuyos datos no se han modificado ni eliminado. Si se selecciona, solo se cifran las partes de la unidad ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden. Si se desactiva, se cifra toda la unidad, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente. La habilidad de cifrar solo el espacio ocupado está disponible solo para el modo **Cifrar toda la unidad extraíble**. Una vez iniciado el cifrado, la activación o desactivación de la función **Cifrar solo el espacio en disco utilizado** no cambiará esta configuración. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado.

Reglas personalizadas	Esta tabla contiene los dispositivos que tienen definidas reglas personalizadas de cifrado. Puede crear reglas de cifrado para unidades extraíbles específicas de las siguientes maneras:
	• Añada una unidad extraíble de la lista de dispositivos de confianza para Control de dispositivos.
	• Añada manualmente una unidad extraíble:
	  • Por ID de dispositivo (Hardware ID o HWID)
	  • Por modelo de dispositivo: Vendor ID (VID) y Product ID (PID)

Parámetro	Descripción
Permitir el cifrado de las unidades extraíbles en modo sin conexión	Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security cifra las unidades extraíbles incluso cuando no existe conexión a Kaspersky Security Center. En este caso, los datos requeridos para descifrar las unidades extraíbles se almacenan en el disco duro del equipo al cual está conectada la unidad extraíble y no se transmiten a Kaspersky Security Center. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no cifra las unidades extraíbles cuando no existe conexión a Kaspersky Security Center.
Configuración de contraseñas de cifrado/Administrador de archivos portátil	Configuración de seguridad de contraseña para el Administrador de archivos portátil.

Plantillas (cifrado de datos)

Después del cifrado de datos, Kaspersky Endpoint Security puede restringir el acceso a los datos, por ejemplo, debido a un cambio en la infraestructura de la organización y a un cambio en el Servidor de Administración de Kaspersky Security Center. Si un usuario no tiene acceso a los datos cifrados, puede solicitarle al administrador acceso a los datos. En otras palabras, el usuario tiene que enviar un archivo de solicitud de acceso al administrador. A continuación, el usuario tiene que cargar el archivo de respuesta recibido del administrador a Kaspersky Endpoint Security. Kaspersky Endpoint Security le permite solicitar el acceso a los datos del administrador por correo electrónico (vea la figura a continuación).



Solicitar acceso a los datos cifrados

Se proporciona una plantilla para informar de la falta de acceso a los datos cifrados. Por comodidad del usuario, puede completar los siguientes campos:

- **Para**. Introduzca la dirección de correo electrónico del grupo de administradores con derechos sobre las características de cifrado de datos.
- **Asunto**. Introduzca el asunto del correo electrónico de la solicitud de acceso a archivos cifrados. Por ejemplo, puede añadir etiquetas para filtrar los mensajes.
- **Mensaje del usuario**. De ser necesario, cambie el contenido del mensaje. Puede utilizar variables para obtener los datos necesarios (por ejemplo, la variable `%USER_NAME%`).

Exclusiones

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza de manera independiente y tiene en cuenta las características de los objetos que se gestionan y de las aplicaciones que se instalan en el equipo. Puede que sea necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a ellos, si está seguro de que el objeto o la aplicación son inofensivos. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza, además de la zona de confianza general en una directiva.

A partir de Kaspersky Endpoint Security 12.5 para Windows, puede añadir telemetría EDR a la zona de confianza. Esto permite optimizar los datos que la aplicación envía al servidor de recopilación telemetría para la solución Kaspersky Anti Targeted Attack Platform (EDR).

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y las aplicaciones de confianza se añaden a la zona de confianza. Las exclusiones de análisis predefinidas y las aplicaciones de confianza ayudan a configurar rápidamente Kaspersky Endpoint Security en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esto significa que no necesita configurar manualmente una zona de confianza para la aplicación en los servidores.

A partir de Kaspersky Endpoint Security 12.8 para Windows, puede instalar la aplicación en modo Light Agent para proteger los entornos virtuales. Las exclusiones de análisis y aplicaciones de confianza predefinidas pueden ayudarle a configurar rápidamente Kaspersky Endpoint Security en entornos virtuales Citrix y VMware.

Exclusiones del análisis

Una *exclusión de análisis* es un conjunto de condiciones que se deben cumplir para que Kaspersky Endpoint Security no analice un objeto en busca de virus u otras amenazas. Las exclusiones del análisis permiten utilizar de manera segura software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario. Estas aplicaciones no tienen necesariamente fines maliciosos, pero los atacantes pueden aprovecharlas. Para obtener información detallada sobre las aplicaciones legítimas que los intrusos pueden usar para poner en peligro el equipo o los datos del usuario, visite el sitio web de la Enciclopedia de Kaspersky.

Es posible que Kaspersky Endpoint Security bloquee estas aplicaciones. Para evitar que se bloqueen, puede configurar las exclusiones del análisis para las aplicaciones en uso. Para ello, añada el nombre o la máscara de nombre que figura en la Enciclopedia de Kaspersky a la zona de confianza. Por ejemplo, a menudo se utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security identifica esta actividad como sospechosa y puede que la bloquee. Para evitar el bloqueo de la aplicación, cree una exclusión del análisis con el nombre o la máscara de nombre que se muestra en la Enciclopedia de Kaspersky.

Si la aplicación que recopila la información y la envía para procesarse se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar que esto ocurra, puede excluir la aplicación del análisis mediante la configuración de Kaspersky Endpoint Security como se describe en este documento.

Los siguientes componentes de aplicaciones y tareas que el administrador del sistema configure pueden utilizar exclusiones del análisis:

- Detección de comportamiento.
- Prevención de exploits.
- Prevención de intrusiones en el host.
- Protección frente a amenazas en archivos.
- Protección frente a amenazas web.
- Protección frente a amenazas en el correo.
- Tarea *Análisis antimalware*.

Lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de red y archivos (incluida la actividad maliciosa), así como el acceso al registro del sistema, no supervisa Kaspersky Endpoint Security. De forma predeterminada, Kaspersky Endpoint Security supervisa los objetos que el proceso de cualquier aplicación abre, ejecuta o guarda, y controla la actividad de todas las aplicaciones y el tráfico de red que generan. Una vez que se agrega una aplicación a la lista de aplicaciones de confianza, Kaspersky Endpoint Security deja de supervisar la actividad de la aplicación.

La diferencia entre las exclusiones de análisis y las aplicaciones de confianza es que, para las exclusiones, Kaspersky Endpoint Security no analiza los archivos, mientras que para las aplicaciones de confianza no controla los procesos iniciados. Si una aplicación de confianza crea un archivo malicioso en una carpeta que no está incluida en las exclusiones de análisis, Kaspersky Endpoint Security detectará el archivo y eliminará la amenaza. Si la carpeta se añade a las exclusiones, Kaspersky Endpoint Security omitirá este archivo.

Por ejemplo, si considera que los objetos que emplea el Bloc de notas estándar de Microsoft Windows son seguros, lo que significa que confía en esta aplicación, puede añadir el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza para que los objetos que use dicha aplicación no se supervisen. Esto aumentará el rendimiento del equipo, lo que resulta especialmente importante cuando se usan aplicaciones de servidor.

Además, algunas acciones que Kaspersky Endpoint Security clasifica como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de diferentes aplicaciones. Por ejemplo, la interceptación de texto que se escribe mediante el teclado es un proceso rutinario para intercambiadores de disposición del teclado automáticos (como Punto Switcher). Para tener en cuenta los detalles de este tipo de aplicaciones y excluir su actividad del proceso de análisis, le recomendamos que las agregue a la lista de aplicaciones de confianza.

Las aplicaciones de confianza ayudan a evitar problemas de compatibilidad entre Kaspersky Endpoint Security y otras aplicaciones (por ejemplo, el problema del análisis doble del tráfico de red de un equipo de terceros por parte de Kaspersky Endpoint Security y de otra aplicación antivirus).

Al mismo tiempo, el archivo ejecutable y el proceso de la aplicación de confianza sí que se analizan en busca de virus y otro software malicioso (malware). Puede excluirse completamente una aplicación del análisis de Kaspersky Endpoint Security gracias a las exclusiones del análisis.

Parámetro	Descripción

Tipos de objetos detectados

Independientemente de la configuración de la aplicación, Kaspersky Endpoint Security siempre detecta y bloquea virus, gusanos y troyanos. Pueden provocar daños significativos en el equipo.

- **Virus y gusanos**

  Subcategoría: Virus y gusanos Viruses_and_Worms)

  Nivel de peligrosidad: Alto

  Los gusanos y virus tradicionales ejecutan acciones que no autoriza el usuario. Pueden crear copias de ellos mismos, que son capaces de reproducirse.

  Virus tradicionales

  Cuando un virus tradicional se introduce en un equipo, lo que hace es infectar un archivo, activarse, realizar acciones maliciosas y añadir copias de sí mismo a otros archivos.

  Un virus tradicional se multiplica únicamente en los recursos locales del equipo; no puede penetrar en otros equipos por sí mismo. Solo puede pasar a otro equipo si añade una copia de sí mismo a un archivo almacenado en una carpeta compartida o un CD introducido, o si el usuario reenvía un mensaje de correo electrónico con un archivo infectado como adjunto.

  Un código de virus tradicional puede penetrar en varias zonas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de secuencias de scripts* y *virus de macros*.

  Los virus pueden infectar los archivos a través de una gran diversidad de técnicas. Los virus de *Overwriting* escriben su código sobre el código del archivo que se infecta, con lo que se borra el contenido del mismo. El archivo infectado deja de funcionar y no se puede restaurar. Los virus *Parasitic* modifican los archivos y los dejan parcial o completamente funcionales. Los virus *Companion* no modifican los archivos, pero crean duplicados. Cuando se abre un archivo infectado, se inicia un duplicado de él (lo que es un virus en realidad). También existen los siguientes tipos de virus: virus *Link*, *virus para archivos OBJ*, *virus para archivos LIB*, *virus para código fuente* y muchos otros.

  Gusano

  Como ocurre con los virus tradicionales, el código de los gusanos está diseñado para infiltrarse en un equipo, activarse y realizar acciones maliciosas. La denominación de los gusanos se debe a su capacidad para "arrastrarse" de un equipo a otro y para propagar copias a través de diversos canales sin el permiso del usuario.

  La principal característica que permite distinguir entre varios tipos de gusanos es la forma en que se propagan. En la siguiente tabla, se ofrece una descripción general de varios tipos de gusanos, que se clasifican por el modo en que se propagan.

  Formas de propagación de los gusanos

Tipo	Nombre	Descripción
Gusano de correo electrónico	Email-Worm	Se propagan a través del correo electrónico. Un mensaje de correo electrónico infectado contiene un archivo adjunto con una copia de un gusano o un enlace a un archivo que se ha cargado en un sitio que se puede haber pirateado o creado exclusivamente para dicho propósito. Al abrir el archivo adjunto, se activa el gusano. Al hacer clic en el enlace, descargar y, a continuación, abrir el archivo, el gusano también comienza a realizar sus acciones maliciosas. Después, continúa propagando copias de sí mismo y buscando otras direcciones de correo electrónico, a las que envía mensajes infectados.
Gusano de mensajería instantánea	Gusanos de cliente de MI	Se propagan a través de clientes de MI. Por lo general, dichos gusanos envían mensajes que contienen un enlace a un archivo con una copia del gusano en un sitio web; para ello usan las listas de contactos del usuario. Cuando el usuario descarga y abre el archivo, el gusano se activa.
Gusano IRC	Gusanos de chat de Internet	Se propagan a través de Internet Relay Chats, sistemas de servicios que permiten la comunicación con otros usuarios a través de Internet en tiempo real. Estos gusanos publican un archivo con una copia de ellos mismos o un enlace a un archivo en un chat de Internet. Cuando el usuario descarga y abre el archivo, el gusano se activa.
Gusano de red	Gusanos de red	Estos gusanos se propagan a través de redes de equipos. A diferencia de otros tipos de gusanos, un gusano de red tradicional se propaga sin intervención del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red especialmente creado (exploit) que contiene el código del gusano o una parte de este. Si un equipo "vulnerable" se encuentra en la red, recibe dicho paquete de red. Cuando el gusano penetra completamente en el equipo, se activa.
Gusano de P2P	Gusanos de redes de uso compartido de archivos	Se propagan a través de las redes de uso compartido de archivos entre pares. Para penetrar en una red P2P, el gusano se copia en una carpeta de uso compartido de archivos, que se ubica normalmente en el equipo del usuario. La red P2P muestra información sobre este archivo para que el usuario pueda "encontrar" el archivo infectado en la red al igual que cualquier otro archivo y, a continuación, descargarlo y abrirlo. Los gusanos más sofisticados simulan el protocolo de red de una red P2P determinada: devuelven respuestas positivas a consultas de búsqueda y ofrecen sus copias para descargarlas.
Gusano	Otros tipos de gusanos	Entre otros tipos de gusanos, se incluyen: • Gusanos que propagan copias de sí mismos a través de recursos de red. Con las funciones del sistema operativo, pueden analizar las carpetas disponibles de la red, conectarse a equipos en Internet e intentar obtener acceso completo a sus unidades de disco. A diferencia de los tipos de gusanos descritos previamente, los otros tipos de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano. • Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono móvil a otro).

- **Troyanos (incluye ransomware)**

  Subcategoría: Troyanos

  Nivel de peligrosidad: Alto

A diferencia de los gusanos y los virus, los troyanos no se replican. Por ejemplo, se introducen en un equipo a través del correo electrónico o un navegador cuando el usuario visita una página web infectada. Los troyanos se inician con intervención del usuario. Comienzan a realizar acciones maliciosas inmediatamente después de que se inician.

Los distintos troyanos se comportan de forma diferente en los equipos infectados. Las funciones principales de los troyanos consisten en bloquear, modificar o destruir información, y desactivar equipos o redes. Los troyanos también pueden recibir o enviar archivos, ejecutarlos, mostrar mensajes en la pantalla, solicitar páginas web, descargar e instalar programas y reiniciar el equipo.

Los piratas usan conjuntos de diversos troyanos con frecuencia.

Los distintos tipos de comportamiento de los troyanos se describen en la tabla siguiente.

Tipos de comportamiento de los troyanos en un equipo infectado

Tipo	Nombre	Descripción
Trojan-ArcBomb	Troyanos: "archivos bomba"	Al descomprimirlos, estos archivos aumentan de tamaño de tal forma que el funcionamiento del equipo se ve afectado. Cuando el usuario intenta descomprimir un archivo de esas características, es posible que el equipo se vea ralentizado o se congele; el disco duro puede llenarse de datos "vacíos". Los "archivos bomba" son especialmente peligrosos para los servidores de correo y archivos. Si el servidor usa un sistema automático para procesar la información entrante, un "archivo bomba" puede detener el servidor.
Backdoor	Troyanos para administración remota	Se considera que son los troyanos más peligrosos. En sus funciones, se parecen a las aplicaciones de administración remota que se instalan en los equipos. Estos programas se instalan en un equipo sin que el usuario se dé cuenta de ello, lo que permite que el intruso administre el equipo de forma remota.
Troyano	Troyanos	Incluyen las siguientes aplicaciones maliciosas: • **Troyanos tradicionales**. Estos programas solo ejecutan las funciones principales de los troyanos: bloqueo, modificación o destrucción de información y desactivación de equipos o redes. No cuentan con funciones avanzadas, a diferencia de otros tipos de troyanos descritos en la tabla. • **Troyanos versátiles**. Estos programas tienen funciones avanzadas comunes en varios tipos de troyanos.
Trojan-Ransom	Troyanos de rescate	Toman como "rehén" la información del usuario para modificarla, bloquearla o afectar al funcionamiento del equipo de modo que el usuario pierda la capacidad de usar la información. El intruso pide un rescate al usuario y le promete enviar una aplicación que restaure el rendimiento del equipo y los datos que estaban almacenados en él.
Trojan-Clicker	Troyanos de clic	Acceden a las páginas web desde el equipo del usuario, ya sea enviando comandos a un navegador o cambiando las direcciones web que se especifican en los archivos del sistema operativo. Con estos programas, los intrusos perpetrarán ataques de red y aumentarán las visitas al sitio web mediante un mayor número de visualizaciones de anuncios publicitarios.
Trojan-Downloader	Descargador de troyanos	Acceden a la página web del intruso, descargan otras aplicaciones maliciosas desde ella y las instalan en el equipo del usuario. Pueden contener el nombre de archivo de la aplicación maliciosa que se va a descargar o recibirla desde la página web a la que se accede.
Trojan-Dropper	Troyanos lanzadera	Contienen otros troyanos que instalan en el disco duro y después se instalan. Los intrusos pueden usar programas del tipo Trojan Dropper para los siguientes propósitos: • Instalar una aplicación maliciosa sin que el usuario se dé cuenta: los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (pueden, por ejemplo, advertir sobre la existencia de un archivo dañado o sobre incompatibilidades con el sistema operativo). • Para proteger a otra aplicación maliciosa y evitar que se detecte: no todo el software antivirus puede detectar una aplicación maliciosa en una aplicación del tipo Trojan Dropper.
Trojan-Notifier	Troyanos de notificación	Le informan al atacante que el equipo infectado está accesible y le envían información: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso a través del correo electrónico o el FTP, mediante la página web del intruso o de otro modo. Los programas del tipo Trojan Notifier se usan normalmente como conjuntos compuestos de varios troyanos. Notifican al intruso de que se han instalado correctamente otros troyanos en el equipo del usuario.
Trojan-Proxy	Proxies de troyanos	Permiten al intruso acceder de forma anónima a las páginas web mediante el equipo del usuario; se usan normalmente para enviar correo no deseado.
Trojan-PSW	Software de robo de contraseñas	El software de robo de contraseñas es un tipo de troyano que roba cuentas de usuario, como datos de registro de software. Estos troyanos buscan datos confidenciales en los archivos del sistema y en el Registro, y los envían al "agresor" por correo electrónico, el FTP o mediante acceso a la página web del intruso, o de cualquier otro modo. Algunos de estos troyanos están clasificados en los distintos tipos que se describen en la tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan en Internet (Trojan-GameThief).
Trojan-Spy	Troyanos espía	Espían a los usuarios con el fin de recopilar información sobre las acciones que el usuario lleva a cabo cuando utiliza el equipo. Pueden interceptar los datos que el usuario introduce en el teclado, tomar instantáneas o recopilar listas de aplicaciones activas. Una vez que reciben la información, la transfieren al intruso a través de correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo.
Trojan-DDoS	Troyanos atacantes de redes	Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS). Con frecuencia, los piratas infectan diversos equipos con estos programas, de modo que puedan usar los equipos para atacar un solo servidor a la vez. Los programas de DoS perpetran los ataques desde un solo equipo con conocimiento del usuario. Los programas DDoS (Distributed DoS) perpetran los ataques distribuidos desde varios equipos sin que el usuario del equipo infectado lo perciba.
Trojan-IM	Troyanos que roban información de los usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de usuarios de programas de mensajería instantánea. Transfieren los datos al intruso mediante correo electrónico o FTP, accediendo a la página web del intruso o de otro modo.
Rootkit	Rootkits	Enmascaran otras aplicaciones maliciosas y su actividad, con lo que prolongan la persistencia de las aplicaciones en el sistema operativo. Además, pueden ocultar archivos, procesos en la memoria infectada del equipo o claves del registro que ejecutan aplicaciones maliciosas. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones del equipo del usuario y otros equipos de la red.
Trojan-SMS	Troyanos con formato de mensajes SMS	Infectan teléfonos móviles a través del envío de mensajes a números de teléfono de tarificación especial.

Trojan-GameThief	Troyanos que roban información de los usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, para después enviar estos datos al intruso mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo.
Trojan-Banker	Troyanos que roban cuentas bancarias	Roban datos de cuentas bancarias o de sistemas de dinero electrónico y envían la información al hacker mediante su página web, por correo electrónico, por FTP o usando otros medios.
Trojan-Mailfinder	Troyanos que recopilan direcciones de correo electrónico	Recopilan direcciones de correo electrónico almacenadas en un equipo y las envían al intruso por correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado.

- **Herramientas maliciosas**

  Subcategoría: Herramientas maliciosas

  Nivel de peligrosidad: Medio

  A diferencia de otros tipos de software malicioso (malware), las herramientas maliciosas no llevan a cabo acciones inmediatamente después de que se inicien. Se pueden almacenar e iniciar de forma segura en el equipo del usuario. Los intrusos usan con frecuencia las funciones de estos programas para crear virus, gusanos y troyanos; perpetrar ataques de red en servidores remotos; piratear equipos o llevar a cabo otras acciones maliciosas.

  Varias funciones de herramientas maliciosas se agrupan por los tipos descritos en la tabla siguiente.

  Funciones de herramientas maliciosas

Tipo	Nombre	Descripción
Constructor	Constructores	Permiten la creación de nuevos virus, gusanos y troyanos. Algunos constructores cuentan incluso con una interfaz de ventanas estándar en la que el usuario puede seleccionar el tipo de aplicación maliciosa que creará, la forma de contrarrestar los depuradores y otras funciones.
Dos	Ataques de red	Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS).
Exploit	Exploits	Un *exploit* es un conjunto de datos o un código de programa que usa las vulnerabilidades de la aplicación en la que se procesa para llevar a cabo una acción maliciosa en un equipo. Por ejemplo, un exploit puede escribir o leer archivos, así como solicitar páginas web "infectadas". Los exploits utilizan las vulnerabilidades de distintas aplicaciones o servicios de red. Disfrazado como paquete de red, un exploit se transfiere a través de la red a diversos equipos. Busca equipos con servicios de red vulnerables. Un exploit en un archivo DOC usa las vulnerabilidades de un editor de textos. Puede comenzar a ejecutar las acciones preprogramadas por el pirata cuando el usuario abra el archivo infectado. Un exploit incrustado en un mensaje de correo electrónico busca vulnerabilidades en cualquier cliente de correo electrónico. Puede empezar a realizar acciones maliciosas en cuanto el usuario abra el mensaje infectado en este cliente de correo electrónico. Los Net-Worms se propagan por las redes mediante exploits. Los exploits Nuker son paquetes de red que desactivan equipos.
FileCryptor	Cifradores	Cifran otras aplicaciones maliciosas para ocultarlas frente a las aplicaciones antivirus.
Flooder	Programas para contaminar redes	Envían un gran número de mensajes a través de canales de red. Este tipo de herramientas incluye, por ejemplo, los programas que "contaminan" Internet Relay Chats. Las herramientas de tipo Flooder no incluyen programas que "contaminan" los canales que usa el correo electrónico, los clientes de MI y los sistemas de comunicación móvil. Estos programas se distinguen como los distintos tipos que se describen en esta tabla (Email-Flooder, IM-Flooder y SMS-Flooder).
HackTool	Herramientas de pirateo	Permiten hackear el equipo en el que están instalados o atacar a otro equipo (por ejemplo, añadiendo nuevas cuentas de sistema sin el permiso del usuario o borrando los registros del sistema para ocultar los rastros de su presencia en el sistema operativo). Este tipo de herramientas incluye sniffers, que incluyen funciones maliciosas, como la interceptación de contraseñas. Los sniffers son programas que permiten la visualización del tráfico de la red.
Hoax	Hoaxes	Avisan al usuario con mensajes parecidos a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario que el disco se ha formateado, aunque no haya sucedido en realidad.
Spoofer	Herramientas de spoofing	Envían mensajes y solicitudes de red con una dirección de remitente falsa. Los intrusos usan herramientas del tipo Spoofer para pasar como los verdaderos remitentes del mensaje, por ejemplo.
VirTool	Herramientas que modifican aplicaciones maliciosas	Permiten la modificación de otros programas de software malicioso (malware) para ocultarlos de las aplicaciones antivirus.
Email-Flooder	Programas que "contaminan" direcciones de correo electrónico	Envían diversos mensajes a varias direcciones de correo electrónico y las "contaminan" de ese modo. Un gran volumen de mensajes entrantes impide a los usuarios ver los mensajes útiles en la bandeja de entrada.
IM-Flooder	Programas que "contaminan" el tráfico de clientes de MI	Inundan a los usuarios de clientes de MI con mensajes. El gran volumen de mensajes impide que los usuarios vean los mensajes entrantes útiles.
SMS-Flooder	Programas que "contaminan" el tráfico con mensajes SMS	Envían un gran número de mensajes SMS a teléfonos móviles.

- **Software publicitario**

  Subcategoría: Software publicitario (adware)

  Nivel de peligrosidad: Medio

El software publicitario (adware) muestra información publicitaria al usuario. El software publicitario (adware) muestra anuncios publicitarios en la interfaz de otros programas y dirige las búsquedas a páginas web de publicidad. Algunos de ellos recopilan información de marketing del usuario y la envían al desarrollador. Esta información puede incluir los nombres de los sitios web que visita el usuario o el contenido de sus búsquedas. A diferencia de los programas del tipo Trojan-Spy, el software publicitario (adware) envía esta información al desarrollador con el permiso del usuario.

- **Marcadores automáticos**

  Subcategoría: Software legítimo que pueden utilizar los intrusos para dañar su equipo o datos personales.

  Nivel de peligrosidad: Medio

  La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de internet para FTP, HTTP y Telnet.

  No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

  Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
Client-IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).
Descargador	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
RemoteAdmin	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y gestionarlo. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.
Server-Web	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
NetTool	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
Client-P2P	Clientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
Client-SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
WebToolbar	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.

- **Software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales**

  Subcategoría: Software legítimo que pueden utilizar los intrusos para dañar su equipo o datos personales.

  Nivel de peligrosidad: Medio

  La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de internet para FTP, HTTP y Telnet.

  No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

  Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
Client-IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).

Descargador	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
RemoteAdmin	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y gestionarlo. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.
Server-Web	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
NetTool	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
Client-P2P	Clientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
Client-SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
WebToolbar	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.

- **Objetos comprimidos cuya compresión puede usarse para proteger código malicioso**

  Subcategoría: Archivos comprimidos que pueden causar daños.

  Nivel de peligrosidad: Medio.

  El archivo se comprime con un compresor especial que se utiliza para comprimir malware: virus, gusanos, troyanos. Kaspersky Endpoint Security analiza el módulo de descompresión de los archivos SFX (autoextraíbles).

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen utilizando compresores especiales. Los expertos de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

- **Objetos comprimidos varias veces**

  Subcategoría: Archivos comprimidos que pueden causar daños.

  Nivel de peligrosidad: Medio.

  El archivo se comprime con un compresor especial que se utiliza para comprimir malware: virus, gusanos, troyanos. Kaspersky Endpoint Security analiza el módulo de descompresión de los archivos SFX (autoextraíbles).

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen utilizando compresores especiales. Los expertos de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

Exclusiones

Esta tabla contiene información sobre las exclusiones del análisis.

Recomendamos especificar rutas relativas en lugar de rutas absolutas. Esto permite excluir no solo los objetos del sistema de archivos, sino también los objetos sin archivos. Por ejemplo, `*\Program Files (x86)\Folder\Subfolder`.

Para excluir objetos de los análisis, puede usar los siguientes métodos:

- Especificar la ruta al archivo o la carpeta que desea excluir.
- Introducir el hash del objeto que desea excluir.

- Usar máscaras:
  - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
  - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la `Folder`, salvo en la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
  - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

    Puede utilizar máscaras en cualquier parte de la ruta de un archivo o carpeta. Por ejemplo, si desea que la cobertura del análisis incluya la carpeta descargas para todas las cuentas de usuario del equipo, ingrese la máscara `C:\Users\*\Downloads\`.

    Kaspersky Endpoint Security admite variables de entorno

    > Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de exclusiones usando la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

- Introduzca el nombre del objeto según la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`). Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, la aplicación excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

> Kaspersky Endpoint Security oculta la lista de exclusiones del análisis en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las exclusiones del análisis en la consola (símbolo de "candado cerrado") y las exclusiones del análisis locales están prohibidas (la casilla de verificación **Permitir el uso de exclusiones locales** se encuentra desactivada).

Aplicaciones de confianza

Esta tabla enumera las aplicaciones de confianza cuya actividad no supervisa Kaspersky Endpoint Security cuando está en funcionamiento.

Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

> Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

El componente Control de aplicaciones regula el inicio de cada una de las aplicaciones independientemente de si la aplicación está incluida en la tabla de aplicaciones de confianza.

> Kaspersky Endpoint Security oculta la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las aplicaciones de confianza en la consola (símbolo de "candado cerrado") y las aplicaciones de confianza locales están prohibidas (la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** se encuentra desactivada).

Fusionar valores al heredar *(disponible solo en la Consola de Kaspersky Security Center)*	Esto fusiona la lista de exclusiones de análisis y aplicaciones de confianza en las directivas principales y secundarias de Kaspersky Security Center. Para fusionar listas, la directiva secundaria debe configurarse para heredar la configuración de la directiva principal de Kaspersky Security Center. Si la casilla de verificación está seleccionada, los elementos de la lista de la directiva principal de Kaspersky Security Center se muestran en las directivas secundarias. De esta manera, puede, por ejemplo, crear una lista consolidada de aplicaciones de confianza para toda la organización. Los elementos de lista heredados de una directiva secundaria no se pueden eliminar ni editar. Los elementos de la lista de exclusiones de análisis y la lista de aplicaciones de confianza que se fusionan durante la herencia se pueden eliminar y editar solo en la directiva principal. Puede añadir, modificar o eliminar elementos de la lista en las directivas de nivel inferior. Si los elementos de las listas de la directiva principal y secundaria coinciden, estos elementos se muestran como el mismo elemento de la directiva principal. Si la casilla de verificación no está seleccionada, los elementos de las listas no se combinan al heredar la configuración de las directivas de Kaspersky Security Center. Esta funcionalidad también permite fusionar listas en perfiles de directivas. Para fusionar listas, en el perfil de mayor prioridad, active la herencia de la configuración de un perfil de menor prioridad. Para obtener más información sobre las prioridades de los perfiles de directivas, consulte la Ayuda de Kaspersky Security Center.
Permitir el uso de exclusiones locales/Permitir el uso de aplicaciones locales de confianza *(disponible solo en la Consola de Kaspersky Security Center)*	*Exclusiones locales y aplicaciones de confianza locales (zona de confianza local)*: lista definida por el usuario de objetos y aplicaciones en Kaspersky Endpoint Security para un equipo específico. Kaspersky Endpoint Security no supervisa objetos y aplicaciones de la zona de confianza local. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza, además de la zona de confianza general en una directiva. Si la casilla de verificación está seleccionada, un usuario puede crear una lista local de exclusiones de análisis y una lista local de aplicaciones de confianza. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo. Si la casilla de verificación está desmarcada, un usuario puede acceder solo a las listas generales de exclusiones de análisis y aplicaciones de confianza generadas en la directiva.
Telemetría de EDR (KATA) / NDR (KATA) *(disponible solo en la Consola de Kaspersky Security Center)*	Esta tabla contiene información sobre las exclusiones de telemetría de EDR.
Telemetría de KUMA *(disponible solo en la Consola de Kaspersky Security Center)*	Lista de eventos que se envían a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security funciona de las siguientes formas: • **Enviar todos los eventos**. En este modo, la aplicación envía todos los eventos del registro de Windows, excepto los eventos añadidos a las reglas de exclusión. • **Enviar solo eventos seleccionados**. En este modo, la aplicación envía solo los eventos añadidos en las reglas de inclusión.
Almacén de confianza de certificados del sistema	Si se selecciona uno de las tiendas de certificados de sistemas de confianza, Kaspersky Endpoint Security excluye de los análisis las aplicaciones firmadas con una firma digital de confianza. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al Grupo de **De confianza**. Si se selecciona **No usar**, Kaspersky Endpoint Security analiza las aplicaciones independientemente de si tienen o no una firma digital. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

Configuración de la aplicación

En este paso, configure los siguientes ajustes generales de la aplicación:

- Modo de funcionamiento
- Autoprotección
- Rendimiento
- Información de depuración
- Estado del equipo cuando la configuración está aplicada

Parámetro	Descripción
Ejecutar la aplicación al iniciar el equipo (recomendado)	Cuando se selecciona esta opción, Kaspersky Endpoint Security se inicia después de la carga del sistema operativo, lo que permite proteger el equipo durante la sesión completa. Cuando se desactiva esta opción, Kaspersky Endpoint Security no se inicia tras la carga del sistema operativo hasta que el usuario lo inicia de forma manual. La protección del equipo se desactiva y los datos del usuario pueden verse expuestos a amenazas.
Usar tecnología de Desinfección avanzada (requiere varios recursos informáticos)	Normalmente, Kaspersky Endpoint Security termina el software malicioso detectado antes de que el equipo se infecte. La Tecnología de desinfección avanzada protege el equipo del software malicioso ya activo (infección activa), minimizando así el riesgo de pérdida de datos y la propagación de la amenaza. Si esta tecnología está activada, cuando se detecta actividad maliciosa, Kaspersky Endpoint Security muestra una notificación emergente. En su notificación, Kaspersky Endpoint Security permite al usuario la opción de realizar la desinfección avanzada del equipo. Una vez que el usuario aprueba este procedimiento, Kaspersky Endpoint Security neutraliza la amenaza y, a continuación, reinicia el equipo. La tecnología de desinfección avanzada emplea un número considerable de recursos del equipo, lo que puede ralentizar el resto de las aplicaciones. Cuando la aplicación se encuentra en proceso de detectar una infección activa, es posible que algunas funcionalidades del sistema operativo no estén disponibles. La disponibilidad del sistema operativo se restablece tras la finalización de la Desinfección avanzada y el reinicio del equipo. Si Kaspersky Endpoint Security se instala en un equipo en el que se ejecuta Windows para servidores, Kaspersky Endpoint Security no muestra la notificación. Por lo tanto, no puede seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe activar la tecnología de Desinfección avanzada en la configuración de la aplicación y activar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis antimalware*. Luego, debe iniciar la tarea *Análisis antimalware*.
Usar Kaspersky Security Center como servidor proxy para la activación *(disponible solo en la Consola de Kaspersky Security Center)*	Si esta casilla se encuentra seleccionada, la aplicación utiliza el Servidor de administración de Kaspersky Security Center como servidor proxy para conectarse a los servidores de activación. Esto es necesario cuando utiliza un código de activación para activar la aplicación en un segmento aislado de la red sin acceso a Internet. Si activa la aplicación con un archivo de clave, el acceso a Internet no será necesario.
Activar Autoprotección	Si se activa esta función, Kaspersky Endpoint Security impide la modificación o eliminación de los archivos de la aplicación el disco duro, los procesos de memoria y las entradas en el Registro del sistema.
Bloquear administración externa de los servicios de la aplicación	Si se desactiva esta función, Kaspersky Endpoint Security no permite administrar los servicios de la aplicación mediante aplicaciones de terceros (como CMD). Cuando se intenta administrar los servicios de aplicaciones usando aplicaciones de terceros, aparece una notificación en la barra de tareas de Microsoft Windows, encima del icono de la aplicación (a menos que el usuario haya desactivado el servicio de notificaciones). Puede permitir la administración externa de los servicios de la aplicación solo en equipos que no admitan la tecnología AM-PPL o en equipos que tengan la tecnología desactivada.
Posponer tareas planificadas al funcionar con batería	Si esta casilla está marcada, el modo de ahorro de energía se activa cuando el equipo funciona con batería. Kaspersky Endpoint Security pospone las tareas planificadas. Las tareas de análisis y actualización podrán iniciarse manualmente cuando sea necesario. Cuando se activa el modo de ahorro de energía y el equipo funciona con la energía de la batería, las tareas siguientes no se ejecutan aunque estén planificadas: • *Análisis completo*. • *Análisis de áreas críticas*. • *Análisis personalizado*. • *Comprobación de integridad de la aplicación*. • *Análisis de IOC*. • *Actualización de las bases de datos y módulos de la aplicación* (solo parches) La aplicación omite las actualizaciones programadas de las bases de datos solo cuando el equipo portátil funciona con batería y el nivel de carga es inferior al 30 % (valor predeterminado). Puede cambiar el nivel mínimo de carga de la batería a partir del cual la aplicación comienza a omitir las actualizaciones programadas de las bases de datos antivirus editando el Registro. En todos los demás casos, Kaspersky Endpoint Security actualiza las bases de datos según lo programado, independientemente de si el equipo portátil está conectado o funciona con batería, o si la aplicación está en modo de ahorro de energía.

Parámetro	Descripción
Facilitar recursos para otras aplicaciones	El consumo de recursos informáticos de Kaspersky Endpoint Security al analizar el equipo puede aumentar la carga en los subsistemas de la CPU y el disco duro. Esto puede ralentizar otras aplicaciones. Para optimizar el rendimiento, Kaspersky Endpoint Security proporciona un *modo de transferencia de recursos a otras aplicaciones*. En este modo, el sistema operativo puede reducir la prioridad de los hilos de la tarea de análisis de Kaspersky Endpoint Security si la carga de la CPU es alta. Esto permite redistribuir recursos del sistema operativo a otras aplicaciones. Por tanto, las tareas de análisis recibirán menos tiempo de CPU. Como resultado, Kaspersky Endpoint Security tardará más en analizar el equipo. De forma predeterminada, la aplicación está configurada para ceder recursos a otras aplicaciones.
Limitar uso de CPU para tareas de análisis	Para optimizar el rendimiento de Kaspersky Endpoint Security, puede limitar el uso de la CPU por la tarea *Análisis antimalware*. Si la casilla de verificación está seleccionada, la carga media en todos los núcleos de CPU desde la tarea *Análisis antimalware* se aproxima al valor especificado. De forma predeterminada, la casilla de verificación está desactivada.
Activar escritura de volcado	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security escribe volcados cuando se producen fallos generales. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no escribe volcados. La aplicación también elimina los archivos de volcado existentes del disco duro del equipo.
Activar la protección de los archivos de volcado y de rastreo	Si se activa esta casilla, podrán acceder a los archivos de volcado el administrador del sistema, el administrador local y el usuario que haya habilitado la creación de dichos archivos. Solo el sistema y los administradores locales pueden acceder a los archivos de trazas. Si se desactiva, cualquier usuario puede acceder a los archivos de volcado y de trazas.
Estado del equipo cuando la configuración está aplicada *(disponible solo en la Consola de Kaspersky Security Center)*	Opciones para mostrar, en Web Console, los estados de los equipos cliente con Kaspersky Endpoint Security instalado cuando ocurran errores al aplicar una directiva o ejecutar una tarea. Los siguientes estados están disponibles *Aceptar*, *Advertencia* y *Crítico*.
Instalar actualizaciones sin reiniciar el equipo	Actualizar la aplicación sin reiniciar el equipo le permite garantizar un funcionamiento ininterrumpido de los servidores. La posibilidad de actualizar la aplicación sin reiniciar se incluye a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo. A partir de la versión 11.11.0 puede realizar las siguientes acciones sin reiniciar el equipo: • instalar parches • cambiar el conjunto de componentes de la aplicación • instalar Kaspersky Endpoint Security sobre Kaspersky Security for Windows Server El valor predeterminado de los parámetros varía en función del tipo de sistema operativo. Si la aplicación se instala en una estación de trabajo, la opción de actualización de la aplicación sin reinicio se deshabilita. Si la aplicación se instala en un servidor, la opción de actualización de la aplicación sin reinicio se habilita.
Compatibilidad con el software de administración remota *(disponible solo en la Consola de Kaspersky Security Center)*	Si el uso de Kaspersky Endpoint Security junto con las herramientas de administración remota (RAT) causa problemas, puede activar el modo de compatibilidad. Los problemas pueden estar relacionados con la incompatibilidad de las RAT con la funcionalidad Secure Desktop de la aplicación. Este objetivo de esta funcionalidad es confirmar acciones que pueden reducir el nivel de seguridad del equipo. Esta funcionalidad permite que una aplicación muestre un cuadro de diálogo de confirmación aislado de otros procesos. Esta funcionalidad utiliza permisos elevados para proteger la solicitud. De esta forma, solo el usuario puede confirmar la acción, y no el malware. Si se selecciona esta opción, se activa el modo de compatibilidad con las RAT. La aplicación muestra un cuadro de diálogo de confirmación sin esta funcionalidad. Esto puede reducir el nivel de seguridad del equipo. No recomendamos activar el modo de compatibilidad si Kaspersky Endpoint Security no está causando problemas con las RAT. Si se desmarca esta opción, el modo de compatibilidad con las RAT de desactiva. De forma predeterminada, la casilla de verificación está desactivada. Ejemplo: cuando se utiliza el navegador en modo RemoteApp, es posible que Kaspersky Endpoint Security no muestre una ventana de confirmación al visitar un sitio web con un certificado que no es de confianza porque RemoteApp no admite la funcionalidad de Escritorio seguro de la aplicación. Esto puede hacer que el navegador deje de responder. Para que el navegador funcione correctamente en el modo RemoteApp, debe activar el modo de compatibilidad. También puede intentar activar el modo de compatibilidad si tiene problemas con la funcionalidad de Escritorio seguro al utilizar otro software de terceros.

Informes y almacenamiento

Informes

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la ejecución de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se registra en informes.

Los informes se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Copia de seguridad

Copias de seguridad almacena copias de seguridad de los archivos que se modificaron o eliminaron durante la desinfección. Una *copia de seguridad* es una copia del archivo creada antes de que el archivo se desinfectara o se eliminara. Las copias de seguridad de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. El usuario cuya cuenta se usó para instalar la Kaspersky Endpoint Security tiene derechos de acceso limitado a esta carpeta.

Kaspersky Endpoint Security no ofrece la posibilidad de configurar permisos de acceso de usuario a copias de seguridad de los archivos.

Cuarentena

Cuarentena es un almacenamiento local especial en el equipo. El usuario puede poner en cuarentena archivos que considere peligrosos para el equipo. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la Cuarentena solo cuando se integra con soluciones de Kaspersky Detection and Response. En otros casos, Kaspersky Endpoint Security coloca el archivo relevante en Copia de seguridad. Para obtener información sobre cómo administrar la cuarentena como parte de las soluciones, consulte la Ayuda de Kaspersky Sandbox, la Ayuda de Kaspersky Endpoint Detection and Response Optimum, la Ayuda de Kaspersky Endpoint Detection and Response Expert, la Ayuda de Kaspersky Anti Targeted Attack Platform y la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises).

La cuarentena solo se puede configurar mediante Web Console. También puede usar Web Console para administrar objetos en cuarentena (restaurar, eliminar, añadir, etc.). Puede restaurar objetos localmente en el equipo mediante la línea de comandos.

Kaspersky Endpoint Security utiliza la cuenta del sistema (SYSTEM) para poner archivos en cuarentena.

Parámetro	Descripción
Eliminar informes tras (días)	Si la casilla de verificación está seleccionada, los informes se conservarán solo durante el tiempo definido como máximo. El período máximo predeterminado del almacenamiento de informes es de 30 días. Después de dicho período de tiempo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.
Limitar el tamaño del archivo del informe a (MB)	Si la casilla de verificación está seleccionada, el tamaño máximo del archivo de informes se limitará al valor definido. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Para evitar superar el tamaño máximo de archivo de informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo de informe cuando se alcance el tamaño máximo en el archivo de informe.
Eliminar objetos tras (días)	Si la casilla de verificación está seleccionada, los archivos se conservarán solo durante el tiempo definido como máximo. El período máximo predeterminado del almacenamiento de archivos es de 30 días. Cuando venza el período máximo de almacenamiento, Kaspersky Endpoint Security eliminará los archivos más antiguos de Copia de seguridad.
Limitar el tamaño de la copia de seguridad a (MB)	Si la casilla de verificación está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Cuando se alcanza el valor definido, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos para evitar que el límite se exceda.
Limitar el tamaño de Cuarentena	Si la casilla de verificación está seleccionada, el espacio de Cuarentena se limitará al tamaño definido como máximo. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Cuando la cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security envía el evento *No hay espacio suficiente en el almacenamiento de Cuarentena* a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación deja de colocar nuevos objetos en cuarentena. Debe vaciar manualmente la Cuarentena.
Notificar cuando se alcanza el almacenamiento de Cuarentena (%)	Valor umbral de la cuarentena. Por ejemplo, puede establecer el umbral de la cuarentena en 50 %. Cuando la cuarentena alcanza el umbral, Kaspersky Endpoint Security envía el evento correspondiente a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación continúa poniendo en cuarentena nuevos objetos.
Transferencia de datos al Servidor de administración *(disponible solo en Kaspersky Security Center)*	Categorías de eventos de los equipos cliente cuya información debe transmitirse al Servidor de administración. Puede desactivar la transferencia de algunos datos para optimizar el espacio en disco en el Servidor de administración. La aplicación envía eventos de las siguientes categorías: • **Acerca de los archivos en Cuarentena**. Puede ver la lista de archivos en cuarentena en la consola de Kaspersky Security Center, en la carpeta **Avanzado → Repositorios → Cuarentena**. Kaspersky Endpoint Security usa la Cuarentena solo cuando se integra con soluciones de Kaspersky Detection and Response. • **Acerca de los archivos en Copia de seguridad**. Puede ver la lista de archivos de Copia de seguridad en la consola de Kaspersky Security Center, en la carpeta **Avanzado → Repositorios → Copia de seguridad**. • **Acerca de los archivos no procesados**. Puede ver la lista de archivos sin procesar en la consola de Kaspersky Security Center, en la carpeta **Avanzado → Repositorios → Amenazas activas**. • **Acerca de dispositivos instalados**. Puede ver la lista de dispositivos conectados en la consola de Kaspersky Security Center en la carpeta **Avanzado → Repositorios → Hardware**. La lista de dispositivos también está disponible en las propiedades del equipo y en la directiva de Kaspersky Endpoint Security para Windows (sección **Control de dispositivos**). • **Acerca de aplicaciones iniciadas**. Puede ver la lista de archivos no procesados en la consola de Kaspersky Security Center en la carpeta **Avanzado → Administración de aplicaciones → Archivos ejecutables**. La lista de archivos ejecutables también está disponible en las propiedades del equipo. • **Acerca de los errores de cifrado de archivos**. Puede ver la lista de errores de cifrado de archivos en la consola de Kaspersky Security Center, en la carpeta **Avanzado → Protección y cifrado de datos → Eventos de cifrado**. La lista de errores también está disponible en las propiedades del equipo. • **Informe de estado de reglas de Control de anomalías adaptativo**. Puede ver el informe en la consola de Kaspersky Security Center, en el nodo **Servidor de administración** de la pestaña **Informes**. Este informe también está disponible en las propiedades de la directiva de Kaspersky Endpoint Security para Windows (sección **Control de anomalías adaptativo**). • **Informe de reglas de Control de anomalías adaptativo activado**. Puede ver el informe en la consola de Kaspersky Security Center, en el nodo **Servidor de administración** de la pestaña **Informes**. Este informe también está disponible en las propiedades de la directiva de Kaspersky Endpoint Security para Windows (sección **Control de anomalías adaptativo**). • **Acerca de una cadena de desarrollo de la amenaza**. Puede ver los detalles de la detección en Kaspersky Security Center Web Console en la sección **Supervisión → Alertas**. Las soluciones de Kaspersky Endpoint Detection and Response utilizan la información sobre la cadena de desarrollo de amenazas.

Configuración de red

Puede configurar los parámetros del servidor proxy utilizado para conectarse a Internet y actualizar las bases de datos antivirus, seleccionar el modo de vigilancia para los puertos de red y configurar un análisis de conexiones cifradas.

Parámetro	Descripción
Limitar el tráfico de las conexiones de uso medido	Si está seleccionada esta casilla de verificación, la aplicación reduce su propio tráfico de red cuando la conexión a Internet es limitada. Kaspersky Endpoint Security identifica la conexión a Internet móvil de alta velocidad como limitada e identifica la conexión wifi como ilimitada. Las redes con reconocimiento del coste funcionan en equipos con Windows 8 o posterior.
Insertar scripts en el tráfico web para interactuar con las páginas web	Si se activa la casilla de verificación, Kaspersky Endpoint Security inyecta un script de interacción con la página web en el tráfico web. Este script garantiza que el componente de Control web pueda funcionar correctamente. El script permite el registro de eventos de Control web. Sin este script, no se puede activar la supervisión de la actividad de Internet del usuario. Los expertos de Kaspersky recomiendan inyectar este script de interacción de la página web en el tráfico para garantizar el funcionamiento correcto de Control web.
Configuración del servidor proxy	Configuración del servidor proxy que los usuarios de equipos cliente usan para ingresar a internet. Kaspersky Endpoint Security utiliza estos parámetros para determinados componentes de protección, como los de actualización de bases de datos y módulos de la aplicación. Para la configuración automática del servidor proxy, Kaspersky Endpoint Security utiliza el protocolo WPAD (Web Proxy Auto-Discovery Protocol). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, la aplicación usa la dirección del servidor proxy especificada en la configuración del navegador Microsoft Internet Explorer.
No usar servidor proxy para direcciones locales	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security no utiliza un servidor proxy al realizar una actualización desde una carpeta compartida.
Configuración de autenticación del servidor proxy	Para autenticar la aplicación en el servidor proxy para el acceso a Internet, debe introducir las credenciales del usuario. Kaspersky Endpoint Security admite la autenticación automática en el servidor proxy. Si la autenticación automática falla, la aplicación le solicita que introduzca las credenciales. **No usar autenticación**. **Autenticación NTLM**. Autenticación de NTLM con la cuenta de usuario actual (predeterminada). **Autenticación NTLM con nombre de usuario y contraseña**. Autenticación de NTLM con credenciales especificadas manualmente. **Nombre de usuario y contraseña**. Autenticación con credenciales especificadas manualmente. **Autenticación automática**. **Autenticación Kerberos**. Autenticación de Kerberos con la cuenta de usuario actual. Para garantizar que la autenticación Kerberos funcione correctamente al usar registros CNAME para la dirección del servidor proxy, debe registrar un nombre principal de servicio (SPN) por cada registro CNAME. **Autenticación Kerberos con nombre de usuario y contraseña**. Autenticación de Kerberos con credenciales especificadas manualmente. Si está seleccionada la autenticación Kerberos, Kaspersky Endpoint Security usará Kerberos o NTLM para la autenticación, dependiendo de cómo esté configurado el servidor proxy.
Puertos vigilados	**Vigilar todos los puertos de red**. En este modo de supervisión de puertos de red, los componentes de protección (Protección frente a amenazas en archivos, Protección frente a amenazas web y Protección frente a amenazas en el correo) supervisan los flujos de datos que se transmiten a través de los puertos de red abiertos del equipo. **Vigilar solo los puertos de red seleccionados**. En este modo de supervisión de puertos de red, los componentes de protección controlan los puertos seleccionados del equipo y la actividad de red de las aplicaciones seleccionadas. La lista de puertos de red que normalmente se utilizan para transmitir correo electrónico y otras clases de tráfico se configura siguiendo las recomendaciones de los expertos de Kaspersky. **Vigilar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky**. Esto utiliza una lista de aplicaciones predefinidas cuyos puertos de red son supervisados por Kaspersky Endpoint Security. Por ejemplo, esta lista incluye Google Chrome, Adobe Reader, Java y otras aplicaciones. **Supervisar todos los puertos de las aplicaciones especificadas**. Esto utiliza una lista de aplicaciones cuyos puertos de red son supervisados por Kaspersky Endpoint Security.

Parámetro	Descripción
Análisis de conexiones cifradas	Kaspersky Endpoint Security analiza el tráfico de red cifrado que se transmite a través de los siguientes protocolos: • SSL 3.0 • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security admite los siguientes modos de análisis de conexión cifrada: • **No analizar las conexiones cifradas**. Kaspersky Endpoint Security no tendrá acceso al contenido de sitios web cuyas direcciones comiencen con `https://`. • **Analizar las conexiones cifradas cuando lo soliciten los componentes de protección**. Kaspersky Endpoint Security analizará el tráfico cifrado solo cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control web lo soliciten. • **Analizar conexiones cifradas siempre**. Kaspersky Endpoint Security analizará el tráfico de red cifrado incluso cuando los componentes de protección están desactivados. Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por aplicaciones de confianza para las que el análisis de tráfico está desactivado. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza solo en la interfaz de Kaspersky Endpoint Security. No puede ver la lista en la Consola de Kaspersky Security Center.
Certificados raíz de confianza	Lista de certificados raíz de confianza. Kaspersky Endpoint Security le permite instalar certificados raíz de confianza en equipos de usuarios si, por ejemplo, necesita desplegar un nuevo centro de certificados. La aplicación le permite añadir un certificado a un almacén de certificados especial de Kaspersky Endpoint Security. En este caso, el certificado se considera de confianza solo para la aplicación Kaspersky Endpoint Security. En otras palabras, el usuario puede acceder a un sitio web con el certificado nuevo en el navegador. Si otra aplicación intenta acceder al sitio web, es posible que se produzca un error de conexión debido a un problema de certificados. Para añadir un certificado al almacén de certificados del sistema, debe utilizar las directivas de grupo de Active Directory.
Visitando un dominio cuyo certificado no es de confianza	• **Permitir**. Cuando se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security permite que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para advertirle que acceder a ese dominio en particular no es recomendable e indicarle por qué. La página contiene un enlace para obtener acceso al recurso web solicitado. Si una aplicación o servicio de terceros establece una conexión con un dominio con un certificado que no es de confianza, Kaspersky Endpoint Security crea su propio certificado para analizar el tráfico. El certificado nuevo tiene el estado *No confiable*. Esto es necesario para advertir a la aplicación de terceros sobre la conexión no confiable porque la página HTML no se puede mostrar en este caso y la conexión se puede establecer en segundo plano. • **Bloquear**. Cuando se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security impide que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para explicarle por qué ese dominio en particular se ha bloqueado.
Visitando un dominio con un error de análisis de conexiones cifradas	• **Bloquear**. Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red. • **Permitir y añadir dominio a exclusiones**. Cuando se produce un error al analizar una conexión cifrada, Kaspersky Endpoint Security añade el dominio con el que se presentó el problema a la lista de dominios con errores de análisis y deja de controlar el tráfico de red cifrado que se genera al visitarlo. La lista de dominios con errores de análisis de conexiones cifradas solo puede consultarse a través de la interfaz local de la aplicación. Para borrar el contenido de la lista, deberá seleccionar **Bloquear**. Kaspersky Endpoint Security también genera un evento para el error de análisis de conexión cifrada.
Bloquear conexiones SSL 2.0	Cuando la casilla está marcada, la aplicación supervisa y bloquea las conexiones de red que se establecen con el protocolo SSL 2.0. Cuando la casilla está desmarcada, la aplicación no bloquea las conexiones de red que se establecen con el protocolo SSL 2.0. Sin embargo, la aplicación no supervisa el tráfico de red a través de este protocolo.
Bloquear conexiones SSL 3.0	Cuando la casilla está marcada, la aplicación bloquea las conexiones de red que se establecen con el protocolo SSL 3.0. Cuando la casilla está desmarcada, la aplicación no bloquea las conexiones de red que se establecen con el protocolo SSL 3.0. La aplicación supervisa el tráfico de red a través de este protocolo. Todos los componentes de la aplicación funcionan sin restricciones.
Bloquear conexiones TLS 1.0	Cuando la casilla está marcada, la aplicación bloquea las conexiones de red que se establecen con el protocolo TLS 1.0. Cuando la casilla está desmarcada, la aplicación no bloquea las conexiones de red que se establecen con el protocolo TLS 1.0. La aplicación supervisa el tráfico de red a través de este protocolo. Todos los componentes de la aplicación funcionan sin restricciones.

Parámetro	Descripción
Descifrar conexiones cifradas a sitios web que usen certificados de EV	Los certificados de EV (Extended Validation Certificate) confirman la autenticidad de los sitios web y mejoran la seguridad de la conexión. Cuando un sitio web cuente con un certificado de EV, verá un candado en la barra de direcciones del navegador. Es posible, además, que la barra de direcciones esté total o parcialmente sombreada en verde. Cuando esta casilla está marcada, la aplicación descifra y controla las conexiones cifradas con sitios web que usan un certificado de EV. Cuando esta casilla no está marcada, la aplicación no tiene acceso al contenido del tráfico HTTPS. Esto significa que la aplicación únicamente puede controlar el tráfico HTTPS sobre la base de la dirección del sitio web (por ejemplo, `https://bing.com`). Cuando visite un sitio web con certificado de EV por primera vez, la conexión cifrada se descifrará independientemente de que la casilla esté o no activada.
Configurar direcciones de confianza	Esto utiliza una lista de direcciones web que Kaspersky Endpoint Security omite del análisis de conexiones de red cifradas. En este caso, Kaspersky Endpoint Security no analiza el tráfico HTTPS de las direcciones web de confianza cuando los componentes Protección frente a amenazas web, Protección frente a amenazas en el correo y Control Web están haciendo su trabajo. Puede introducir un nombre de dominio o una dirección IP. Kaspersky Endpoint Security admite el carácter `*` para introducir una máscara en el nombre de dominio. Kaspersky Endpoint Security no es compatible con el símbolo `*` para direcciones IP. Puede seleccionar un rango de direcciones IP utilizando una máscara de subred (por ejemplo, 198.51.100.0/24). Ejemplos: • `domain.com`: el registro incluye las siguientes direcciones: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. El registro es exclusivo de subdominios (por ejemplo, `subdomain.domain.com`). • `subdomain.domain.com`: el registro incluye las siguientes direcciones: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. El registro es exclusivo del dominio `domain.com`. • `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro es exclusivo del dominio `domain.com`.
Configurar aplicaciones de confianza	En esta lista, se enumeran las aplicaciones de confianza cuya actividad no supervisa Kaspersky Endpoint Security durante su funcionamiento. Puede seleccionar los tipos de actividades que Kaspersky Endpoint Security no supervisará (por ejemplo, puede indicarle a la aplicación que no analice el tráfico de red). Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.
Para analizar conexiones cifradas en aplicaciones con su propia tienda de certificados, use *(disponible solo en la interfaz de Kaspersky Endpoint Security)*	Si esta casilla de verificación está marcada, la aplicación analiza el tráfico cifrado en el navegador Mozilla Firefox y el cliente de correo Thunderbird. Es posible que se bloquee el acceso a algunos sitios web a través del protocolo HTTPS. Para analizar el tráfico en el navegador Mozilla Firefox y el cliente de correo Thunderbird, debe activar el Análisis de conexiones cifradas. Si el Análisis de conexiones cifradas está desactivado, la aplicación no analiza el tráfico en el navegador Mozilla Firefox ni en el cliente de correo Thunderbird. La aplicación utiliza el certificado raíz de Kaspersky para descifrar y analizar el tráfico cifrado. Puede seleccionar la tienda de certificados que contendrá el certificado raíz de Kaspersky. • **El almacén de certificados de Windows (recomendado)**. El certificado raíz de Kaspersky se añade a esta tienda durante la instalación de Kaspersky Endpoint Security. • **Tienda de certificados propia**. Mozilla Firefox y Thunderbird utilizan sus propias tiendas de certificados. Si se selecciona la tienda de certificados de Mozilla, debe añadir manualmente el certificado raíz de Kaspersky a esta tienda a través de las propiedades del navegador.

Interfaz

Puede configurar los ajustes de la interfaz de la aplicación.

Parámetro	Descripción
Interacción con el usuario *(disponible solo en la Consola de Kaspersky Security Center)*	**Mostrar interfaz simplificada**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un icono en el área de notificación de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security en forma limitada a través del menú contextual de este icono. Kaspersky Endpoint Security también muestra únicamente notificaciones que requieren la acción del usuario sobre el icono de la aplicación. **Mostrar interfaz de usuario**. En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al icono ubicado en el área de notificaciones de Windows. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono. **Ocultar la sección del monitor de actividad de la aplicación**. En el equipo cliente, en la ventana principal de Kaspersky Endpoint Security, el botón **Supervisión de la Actividad de Aplicaciones** no está disponible. *Supervisión de la Actividad de Aplicaciones* es una herramienta diseñada para ver información sobre la actividad de las aplicaciones en el equipo de un usuario en tiempo real. **No mostrar interfaz de usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El icono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.
Acceso a las tareas locales	Si se selecciona la casilla de verificación, se muestran tareas locales en la interfaz local de Kaspersky Endpoint Security. Cuando no existen restricciones adicionales de directivas, el usuario puede configurar y ejecutar tareas. Sin embargo, el usuario no puede programar la configuración y la ejecución de las tareas. El usuario puede ejecutar tareas solo manualmente. Si esta casilla está desmarcada, las tareas locales se ocultan en la interfaz de la aplicación. De este modo, las tareas locales no se ejecutan según la planificación. Las tareas no se pueden iniciar ni configurar en la interfaz local de Kaspersky Endpoint Security, ni con la línea de comandos. Aun así, un usuario puede iniciar un análisis de un archivo o una carpeta eligiendo la opción **Buscar virus** en el menú contextual del archivo o de la carpeta. La tarea de análisis se inicia con los valores de configuración predeterminados de la tarea de análisis personalizado.
Ver tareas de grupo	Si se selecciona la casilla de verificación, se muestran tareas de grupo en la interfaz local de Kaspersky Endpoint Security. El usuario puede ver la lista de todas las tareas en la interfaz de la aplicación. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security muestra una lista de tareas vacía.
Gestionar tareas de grupo	Si se selecciona, los usuarios pueden iniciar y detener las tareas de grupo especificadas en la consola de Kaspersky Security Center. Los usuarios pueden iniciar y detener las tareas en la interfaz de la aplicación o en la interfaz de la aplicación simplificada. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no inicia las tareas planificadas automáticamente, o el administrador inicia las tareas manualmente en la consola de Kaspersky Security Center.
Configurar notificaciones	Tabla con la configuración de las notificaciones sobre eventos con distinto nivel de importancia que pueden producirse durante el funcionamiento de un componente, una tarea o toda una aplicación. Kaspersky Endpoint Security muestra notificaciones que informan de estos eventos en la pantalla, las envía por correo electrónico o las registra.
Configurar notificaciones de correo	Parámetros del servidor SMTP con el que se enviarán las notificaciones de los eventos registrados mientras la aplicación esté en funcionamiento. De forma predeterminada, Kaspersky Endpoint Security utiliza la configuración de notificaciones de correo electrónico de Kaspersky Security Center. Para obtener más información sobre la configuración de notificaciones de correo electrónico, consulte la Ayuda de Kaspersky Security Center. Si necesita configurar notificaciones de correo electrónico individuales, puede editar los siguientes ajustes: • **Dirección del remitente**. Dirección de correo electrónico del remitente. No se recomienda utilizar una dirección inexistente. • **Servidor SMTP**. Una o más direcciones de servidores de correo electrónico de su organización (por ejemplo, `mail.company.com`). Puede introducir una dirección IP (IPv4 o IPv6). Para autenticar al usuario en el servidor SMTP, ingrese las credenciales del remitente en los campos correspondientes. Para probar las notificaciones de correo electrónico, puede enviar un mensaje de prueba. • **Dirección de destino**. Direcciones de correo electrónico de los destinatarios a los que la aplicación enviará notificaciones. • **Modo de envío**. Modo de envío de notificaciones de correo electrónico. Kaspersky Endpoint Security puede enviar mensajes inmediatamente cuando ocurre un evento; alternativamente, puede seguir un horario preconfigurado.
Mostrar el estado de la aplicación en el área de notificaciones	Categorías de eventos de la aplicación que provocan un cambio (o) en el icono de Kaspersky Endpoint Security ubicado en el área de notificación de la barra de tareas de Microsoft Windows. Dichos eventos también dan lugar a una notificación emergente.
Notificaciones del estado de la base de datos antimalware local	Ajustes de las notificaciones sobre bases de datos de antivirus obsoletas utilizadas por la aplicación.

Parámetro	Descripción
Protección con contraseña	Cuando este interruptor está activado y el usuario intenta realizar una acción alcanzada por la función de protección con contraseña, Kaspersky Endpoint Security solicita la contraseña en cuestión. La cobertura de la protección con contraseña se compone de las acciones que se han prohibido (por ejemplo, la desactivación de los componentes de protección) y las cuentas de usuario para las que se han prohibido tales acciones. Cuando habilite la protección con contraseña, Kaspersky Endpoint Security le pedirá que establezca la contraseña para la cuenta de KLAdmin.
Soporte de usuario/Vínculos a recursos web *(disponible solo en la Consola de Kaspersky Security Center)*	Lista de enlaces a recursos web que contienen información sobre el Soporte técnico de Kaspersky Endpoint Security. Los enlaces añadidos se muestran en la ventana **Soporte** de la interfaz local de Kaspersky Endpoint Security en lugar de los enlaces predeterminados.
Soporte de usuario/Descripción *(disponible solo en la Consola de Kaspersky Security Center)*	Mensaje que se muestra en la ventana **Soporte** de la interfaz local de Kaspersky Endpoint Security.

Administrar configuración

Puede guardar la configuración actual de Kaspersky Endpoint Security en un archivo y usarla para configurar rápidamente la aplicación en un equipo diferente. También puede utilizar un archivo de configuración al implementar la aplicación a través de Kaspersky Security Center con un paquete de instalación. Puede restaurar la configuración predeterminada en cualquier momento.

Los ajustes de administración de la configuración de la aplicación solo están disponibles en la interfaz de Kaspersky Endpoint Security.

Ajustes de gestión de la configuración de la aplicación

Configuración	Descripción
Importar	Extraer la configuración de la aplicación de un archivo en formato CFG y aplicarla.
Exportar	Guardar la configuración actual de la aplicación a un archivo en formato CFG.
Restaurar	Puede restaurar la configuración de la aplicación recomendada por Kaspersky en cualquier momento. Cuando se restablece la configuración, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección.

Actualización de las bases de datos y módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antivirus y de la base de código) y la función de KSN pueden dejar de estar disponibles en la aplicación en el territorio de EE. UU.

Las actualizaciones regulares requieren una licencia efectiva. Si no hay ninguna licencia actual, solamente podrá realizar una actualización una vez.

Su equipo debe estar conectado a Internet para descargar satisfactoriamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. De forma predeterminada, los parámetros de conexión a Internet se determinan automáticamente. Si utiliza un servidor proxy, debe ajustar la configuración del servidor proxy.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTPS.

Mientras se lleva a cabo la actualización, se descargan e instalan los siguientes objetos en su equipo:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se proporciona por medio de bases de datos que contienen firmas de virus y otras amenazas, así como información sobre la forma de neutralizarlas. Los componentes de protección emplean esta información a la hora de buscar y neutralizar archivos infectados en el equipo. Las bases de datos se actualizan constantemente con registros de nuevas amenazas y métodos para combatirlas. Por tanto, es recomendable que actualice la base de datos con regularidad.

  Además de las bases de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de protección interceptar el tráfico de la red.

- Módulos de la aplicación. Aparte de las bases de datos de Kaspersky Endpoint Security, también puede actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación sirve para solucionar vulnerabilidades en Kaspersky Endpoint Security, añade nuevas funciones o mejora las existentes.

Durante una actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con los de la versión actualizada en el origen de actualizaciones. Si los módulos de la aplicación y las bases de datos actuales son diferentes de sus respectivas versiones actualizadas, la parte de las actualizaciones que falte se instala en su equipo.

Si las bases de datos no están actualizadas, puede que el tamaño del paquete de actualización sea considerable, lo que provocaría un tráfico de internet adicional (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en la ventana principal de la aplicación o en la información sobre herramientas que ve cuando pasa el cursor sobre el icono de la aplicación en el área de notificación.

La información sobre los resultados de la actualización y sobre todos los eventos se producen durante la ejecución de la tarea de actualización se registra en el informe de Kaspersky Endpoint Security.

Si la aplicación funciona en modo Light Agent, hay consideraciones especiales que afectan a la actualización de las bases de datos y los módulos de la aplicación.

Configuración de actualización de base de datos y módulo de aplicación

Parámetro	Descripción
Programación de la actualización de bases de datos	**Automáticamente**. En este modo, la aplicación comprueba el origen de actualizaciones con cierta frecuencia en busca de nuevos paquetes de actualización. La frecuencia de las comprobaciones para ver si hay paquetes de actualización aumenta durante los brotes de virus y disminuye cuando no hay brotes. Tras detectar un paquete de actualización nuevo, Kaspersky Endpoint Security lo descarga e instala las actualizaciones en su equipo. **Manual**. Este modo de ejecución de la tarea de actualización permite iniciar la tarea de actualización de forma manual. **Según programación**. En este modo de ejecución de la tarea de actualización, Kaspersky Endpoint Security ejecuta la tarea de actualización en función de la programación especificada. Si está seleccionado este modo de ejecución de la tarea de actualización, también puede iniciar la tarea de actualización de Kaspersky Endpoint Security manualmente.
Ejecutar tareas no realizadas	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security iniciará la tarea omitida lo antes posible. La tarea se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programado de la tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas omitidas, las ejecuta de manera aleatoria dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no iniciará las tareas omitidas. En lugar de ello, lleva a cabo la siguiente tarea de acuerdo con la planificación actual.
Orígenes de actualizaciones	Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security. Las fuentes de las actualizaciones incluyen el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky y carpetas locales y en red. Si no hay servidores de actualización de Kaspersky disponibles, Kaspersky Endpoint Security puede usar dominios alternativos para actualizar sus bases de datos y módulos de software de la aplicación. Para obtener información detallada, consulte la Base de conocimientos de soporte técnico. La lista predeterminada de orígenes de actualizaciones incluye los servidores de actualizaciones de Kaspersky Security Center y Kaspersky. Puede agregar a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones. Kaspersky Endpoint Security no es compatible con las actualizaciones de los servidores HTTPS a menos que sean servidores de actualizaciones de Kaspersky. Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno después de otro, empieza desde el inicio de la lista y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible. De forma predeterminada, Kaspersky Endpoint Security utiliza el servidor de Kaspersky Security Center como la primera fuente de actualización. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una política al equipo, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de la tarea local *Actualización de las bases de datos y módulos de la aplicación*, porque es posible que la aplicación no tenga acceso al servidor de Kaspersky Security Center. Si la aplicación se está ejecutando en modo Light Agent, se selecciona una carpeta en la SVM como origen de actualizaciones.
Ejecutar actualizaciones de bases de datos como	De forma predeterminada, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta se ha utilizado para iniciar la sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security se podría actualizar desde un origen de actualizaciones al que el usuario no pueda acceder debido a la falta de los permisos necesarios (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o un origen de actualizaciones para el que no se haya configurado la autenticación del servidor proxy. En la configuración de la aplicación, puede especificar un usuario que tenga esos permisos e iniciar la tarea de actualización de Kaspersky Endpoint Security con la cuenta de ese usuario.

Parámetro	Descripción
Descargar actualizaciones de los módulos de la aplicación	Descarga de actualizaciones del módulo de la aplicación con actualizaciones de la base de datos de la aplicación. Si se selecciona la casilla de verificación, Kaspersky Endpoint Security informa al usuario sobre actualizaciones disponibles de los módulos de la aplicación e incluye actualizaciones de estos en el paquete de actualización mientras ejecuta la tarea. La manera en la que se aplican las actualizaciones de los módulos de la aplicación está determinada por la configuración siguiente: • **Instalar actualizaciones críticas y aprobadas**. Si se selecciona esta opción, cuando las actualizaciones de los módulos de la aplicación están disponibles, Kaspersky Endpoint Security instala automáticamente las actualizaciones críticas y todas las demás únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. • **Instalar solo actualizaciones aprobadas**. Si se selecciona esta opción, cuando están disponibles las actualizaciones de los módulos de la aplicación, Kaspersky Endpoint Security las instala únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada. Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no informa al usuario sobre actualizaciones disponibles de los módulos de la aplicación ni incluye actualizaciones de estos en el paquete de actualización mientras ejecuta la tarea. Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia de usuario final, la aplicación instala las actualizaciones después de que se hayan aceptado dichos términos. Esta casilla está marcada de forma predeterminada.
Copiar las actualizaciones a la carpeta	Si se selecciona esta casilla, Kaspersky Endpoint Security copia el paquete de actualización en la carpeta compartida especificada bajo la casilla. Después, el resto de los equipos de su LAN pueden acceder al paquete de actualización a través de esta carpeta compartida. Reduce el tráfico de Internet dado que el paquete de actualización se descarga únicamente una vez. La carpeta especificada por defecto es `C:\ProgramData\Kaspersky Lab\KES.14.2\Update distribution\`.
Servidor proxy para actualizaciones *(disponible solo en la interfaz de Kaspersky Endpoint Security)*	Configuración del servidor proxy para el acceso a Internet de los usuarios de los equipos de clientes para actualizar los módulos de la aplicación y las bases de datos. Para la configuración automática del servidor proxy, Kaspersky Endpoint Security utiliza el protocolo WPAD (Web Proxy Auto-Discovery Protocol). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, Kaspersky Endpoint Security usa la dirección especificada en la configuración del navegador Microsoft Internet Explorer.
No usar servidor proxy para direcciones locales *(disponible solo en la interfaz de Kaspersky Endpoint Security)*	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security no utiliza un servidor proxy al realizar una actualización desde una carpeta compartida.

Apéndice 2. Grupos de confianza de aplicaciones

Kaspersky Endpoint Security clasifica todas las aplicaciones que se inician en el equipo en grupos de confianza. Dicha clasificación se realiza en grupos de confianza en función del nivel de peligro que las aplicaciones presentan para el sistema operativo.

Los grupos de confianza son los siguientes:

- **De confianza**. Este grupo incluye aplicaciones para las que se cumplen una o varias de las siguientes condiciones:
  - Aplicaciones firmadas digitalmente por proveedores de confianza.
  - Aplicaciones registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto la aplicación en el grupo *De confianza*.

No hay operaciones prohibidas para dichas aplicaciones.

- **Restricción mínima**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - Aplicaciones no firmadas digitalmente por proveedores de confianza.
  - Aplicaciones no registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto la aplicación en el grupo *Restricción mínima*.

  Dichas aplicaciones están sujetas a restricciones mínimas de acceso a los recursos del sistema operativo.
- **Restricción máxima**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - Aplicaciones no firmadas digitalmente por proveedores de confianza.
  - Aplicaciones no registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto la aplicación en el grupo *Restricción máxima*.

  Dichas aplicaciones están sujetas a un nivel alto de restricción en el acceso a los recursos del sistema operativo.
- **No fiable**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - Aplicaciones no firmadas digitalmente por proveedores de confianza.
  - Aplicaciones no registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto la aplicación en el grupo *No fiable*.

  Para estas aplicaciones, todas las operaciones están bloqueadas.

Apéndice 3. Extensiones de archivo para el análisis rápido de unidades extraíbles

com: archivo ejecutable de una aplicación no superior a 64 KB

exe: archivo ejecutable o archivo comprimido autoextraíble

sys: archivo del sistema de Microsoft Windows

prg: texto de programas como dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin: archivo binario

bat: archivo de lotes

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para DOS), OS/2

dpl: biblioteca comprimida de Borland Delphi

dll: biblioteca de enlaces dinámicos

scr: pantalla de presentación en Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto Microsoft OLE (Object Linking and Embedding)

tsp: programa ejecutable en modo de tiempo fraccionado

drv: controlador de dispositivo

vxd: controlador de dispositivo virtual de Microsoft Windows

pif: archivo de información de programa

lnk: archivo de acceso directo de Microsoft Windows

reg: archivo clave para el Registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de instalación para Microsoft Windows, Windows NT y ciertas aplicaciones

cla: clase Java

vbs: script Visual Basic®

vbe: extensión de vídeo del BIOS

js, jse: texto de origen JavaScript

htm: documento hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta: programa hipertexto para Microsoft Internet Explorer®

asp: secuencia de comandos Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script PHP integrado en archivos HTML

wsh: archivo de configuración de Microsoft Windows Script Host

wsf: script Microsoft Windows

the: papel tapiz del escritorio de Microsoft Windows 95

hlp: archivo de Ayuda de Microsoft Windows

msg: mensaje de correo de Microsoft Mail

plg: mensaje de correo

mbx: mensajes de correo de Microsoft Office Outlook guardado

doc*: documentos de Microsoft Office Word, como doc (Microsoft Office Word), docx (Microsoft Office Word 2007 con compatibilidad con XML) y docm (Microsoft Office Word 2007 con compatibilidad para macros)

dot*: plantilla de documento de Microsoft Office Word, como: dot para plantillas de documento de Microsoft Office Word; dotx para plantillas de documento Microsoft Office Word 2007, y dotm para plantilla de documento Microsoft Office Word 2007 con soporte para macros

fpm: programa de bases de datos, archivo de inicio para Microsoft Visual FoxPro

rtf: documento en formato de texto enriquecido (Rich Text Format)

shs: fragmento de identificador de objeto de recorte de Shell de Windows

dwg: base de datos de dibujos de AutoCAD®

msi: paquete de instalación de Microsoft Windows Installer

otm: proyecto VBA para Microsoft Office Outlook

pdf: documento Adobe Acrobat

swf: objeto empaquetado Shockwave® Flash

jpg, jpeg: formato gráfico para imágenes comprimidas

emf: formato de metadatos ampliado

ico: archivo de icono

ov?: Archivos ejecutables de Microsoft Office Word

xl*: documentos de Microsoft Office Excel y archivos como: xla, la extensión para Microsoft Office Excel; xlc para diagramas; xlt para plantillas de documentos; xlsx para libros de trabajo de Microsoft Office Excel 2007; xltm para libros de trabajo de Microsoft Office Excel 2007 con compatibilidad para macros; xlsb para libros de trabajo de Microsoft Office Excel 2007 en formato binario (no XML); xltx para plantillas de Microsoft Office Excel 2007; xlsm para plantillas de Microsoft Office Excel 2007 con compatibilidad para macros, y xlam para complementos de Microsoft Office Excel 2007 con compatibilidad para macros

pp*: documentos y archivos de Microsoft Office PowerPoint®, como: pps para diapositivas de Microsoft Office PowerPoint; ppt para presentaciones; pptx para presentaciones de Microsoft Office PowerPoint 2007; pptm para presentaciones de Microsoft Office PowerPoint 2007 con compatibilidad para macros; potx para plantillas de presentación de Microsoft Office PowerPoint 2007; potm para plantillas de presentación de Microsoft Office PowerPoint 2007 con compatibilidad para macros; ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007; ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 con compatibilidad para macros, y ppam para complementos de Microsoft Office PowerPoint 2007 con compatibilidad para macros

md*: documentos y archivos de Microsoft Office Access® como mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: diapositivas Microsoft PowerPoint 2007

sldm: diapositivas Microsoft PowerPoint 2007 con soporte para macros

thmx: tema Microsoft Office 2007

Apéndice 4. Tipos de archivo para el filtrado de adjuntos Protección frente a amenazas en el correo

Recuerde que el formato real de un archivo puede no corresponder al formato indicado por su extensión.

Si activa el filtro de archivos adjuntos a mensajes de correo electrónico, el componente Protección frente a amenazas en el correo podría eliminar o cambiar el nombre de los archivos con las siguientes extensiones:

com: archivo ejecutable de una aplicación no superior a 64 KB

exe: archivo ejecutable o archivo comprimido autoextraíble

sys: archivo del sistema de Microsoft Windows

prg: texto de programas como dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin: archivo binario

bat: archivo de lotes

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para DOS), OS/2

dpl: biblioteca comprimida de Borland Delphi

dll: biblioteca de enlaces dinámicos

scr: pantalla de presentación en Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto Microsoft OLE (Object Linking and Embedding)

tsp: programa ejecutable en modo de tiempo fraccionado

drv: controlador de dispositivo

vxd: controlador de dispositivo virtual de Microsoft Windows

pif: archivo de información de programa

lnk: archivo de acceso directo de Microsoft Windows

reg: archivo clave para el Registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de instalación para Microsoft Windows, Windows NT y ciertas aplicaciones

cla: clase Java

vbs: script Visual Basic®

vbe: extensión de vídeo del BIOS

js, jse: texto de origen JavaScript

htm: documento hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta: programa hipertexto para Microsoft Internet Explorer®

asp: secuencia de comandos Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script PHP integrado en archivos HTML

wsh: archivo de configuración de Microsoft Windows Script Host

wsf: script Microsoft Windows

the: papel tapiz del escritorio de Microsoft Windows 95

hlp: archivo de Ayuda de Microsoft Windows

msg: mensaje de correo de Microsoft Mail

plg: mensaje de correo

mbx: mensajes de correo de Microsoft Office Outlook guardado

doc*: documentos de Microsoft Office Word, como doc (Microsoft Office Word), docx (Microsoft Office Word 2007 con compatibilidad con XML) y docm (Microsoft Office Word 2007 con compatibilidad para macros)

dot*: plantilla de documento de Microsoft Office Word, como: dot para plantillas de documento de Microsoft Office Word; dotx para plantillas de documento Microsoft Office Word 2007, y dotm para plantilla de documento Microsoft Office Word 2007 con soporte para macros

fpm: programa de bases de datos, archivo de inicio para Microsoft Visual FoxPro

rtf: documento en formato de texto enriquecido (Rich Text Format)

shs: fragmento de identificador de objeto de recorte de Shell de Windows

dwg: base de datos de dibujos de AutoCAD®

msi: paquete de instalación de Microsoft Windows Installer

otm: proyecto VBA para Microsoft Office Outlook

pdf: documento Adobe Acrobat

swf: objeto empaquetado Shockwave® Flash

jpg, jpeg: formato gráfico para imágenes comprimidas

emf: formato de metadatos ampliado

ico: archivo de icono

ov?: Archivos ejecutables de Microsoft Office Word

xl*: documentos de Microsoft Office Excel y archivos como: xla, la extensión para Microsoft Office Excel; xlc para diagramas; xlt para plantillas de documentos; xlsx para libros de trabajo de Microsoft Office Excel 2007; xltm para libros de trabajo de Microsoft Office Excel 2007 con compatibilidad para macros; xlsb para libros de trabajo de Microsoft Office Excel 2007 en formato binario (no XML); xltx para plantillas de Microsoft Office Excel 2007; xlsm para plantillas de Microsoft Office Excel 2007 con compatibilidad para macros, y xlam para complementos de Microsoft Office Excel 2007 con compatibilidad para macros

pp*: documentos y archivos de Microsoft Office PowerPoint®, como: pps para diapositivas de Microsoft Office PowerPoint; ppt para presentaciones; pptx para presentaciones de Microsoft Office PowerPoint 2007; pptm para presentaciones de Microsoft Office PowerPoint 2007 con compatibilidad para macros; potx para plantillas de presentación de Microsoft Office PowerPoint 2007; potm para plantillas de presentación de Microsoft Office PowerPoint 2007 con compatibilidad para macros; ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007; ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 con compatibilidad para macros, y ppam para complementos de Microsoft Office PowerPoint 2007 con compatibilidad para macros

md*: documentos y archivos de Microsoft Office Access® como mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: diapositivas Microsoft PowerPoint 2007

sldm: diapositivas Microsoft PowerPoint 2007 con soporte para macros

thmx: tema Microsoft Office 2007

Apéndice 5. Configuración de red para la interacción con servicios externos

Kaspersky Endpoint Security y Kaspersky Security Center utilizan un canal de comunicación cifrado con TLS (Transport Layer Security) para trabajar con servicios externos de Kaspersky.

Kaspersky Endpoint Security utiliza la siguiente configuración de red para interactuar con servicios externos.

Configuración de red

Dirección	Descripción
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocolo: `HTTPS` Puerto: `443`	Activando la aplicación.

Dirección	Descripción

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTPS`
Puerto: `443`
	Actualizando las bases de datos y módulos de la aplicación.

`downloads.upd.kaspersky.com` Protocolo: `HTTPS` Puerto: `443`	• Actualizando las bases de datos y módulos de la aplicación. • Verificando el acceso a los servidores de Kaspersky. Si el acceso a los servidores con los DNS del sistema no es posible, la aplicación utilizará DNS públicos. Esto es necesario para asegurarse de que las bases de datos antivirus estén actualizadas y para mantener el nivel de seguridad para el equipo. Kaspersky Endpoint Security utiliza la siguiente lista de servidores DNS públicos en el siguiente orden: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Las solicitudes emitidas por la aplicación pueden contener direcciones de dominios y direcciones IP públicas del usuario, ya que la aplicación establece una conexión TCP/UDP con el servidor DNS. Esta información es necesaria, por ejemplo, para validar el certificado de un recurso web al utilizar HTTPS. Si Kaspersky Endpoint Security utiliza un servidor DNS público, el procesamiento de datos se rige por la directiva de privacidad del servicio correspondiente. Si desea evitar que Kaspersky Endpoint Security utilice un servidor DNS público, póngase en contacto con el Soporte técnico para acceder a un parche privado.
`touch.kaspersky.com` Protocolo: `HTTP`	• Recibiendo el tiempo de confianza para revisar el periodo de validez del certificado (conexión TLS). • Advertencia sobre el acceso denegado a un recurso web en el navegador cuando Protección frente a amenazas web está en ejecución.

Dirección	Descripción

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTP`
Puerto: `80`
	Actualizando las bases de datos y módulos de la aplicación.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocolo: `HTTPS`
Puerto: `443`
	Uso de Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocolo: `KSN`
Puerto: `443`, `1443`
	Uso de Kaspersky Security Network.

`click.kaspersky.com`
`redirect.kaspersky.com`
Protocolo: `HTTPS`
Puerto: `443`
	Haga clic en los enlaces de la interfaz.

Configuración, empleado para el cifrado

Dirección	Descripción

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocolo: `HTTP`
Puerto: `80`
	Infraestructura de clave pública (PKI).

Apéndice 6. Eventos de aplicación

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la finalización de cada tarea de análisis antimalware, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se almacenan en el registro de eventos de Kaspersky Security Center y en el registro de eventos de Windows.

Kaspersky Endpoint Security genera eventos de los siguientes tipos: eventos generales y eventos específicos. Los eventos específicos son creados únicamente por Kaspersky Endpoint Security para Windows. Los eventos específicos tienen una id. simple, como `000000cb`. Los eventos específicos contienen los siguientes parámetros requeridos:

- `GNRL_EA_DESCRIPTION` es el contenido del evento.
- `GNRL_EA_ID` es el ID de servicio del evento.
- `GNRL_EA_SEVERITY` es el estado del evento. `1` – *Información*, `2` – *Advertencia*, `3` – *Fallo operativo*, `4` – *Crítico*.
- `EVENT_TYPE_DISPLAY_NAME` es el título del evento.
- `TASK_DISPLAY_NAME` es el nombre del componente de la aplicación que inició el evento.

Los eventos generales pueden ser creados por Kaspersky Endpoint Security para Windows así como por otras aplicaciones de Kaspersky (por ejemplo, Kaspersky Security for Windows Server). Los eventos generales tienen una ID. más compleja, como `GNRL_EV_VIRUS_FOUND`. Además de la configuración requerida, los eventos generales contienen una configuración avanzada.

Cuánto tiempo se almacenan los eventos en el servidor

Crítico

La licencia ha caducado

Estado	!
Componente	Auditoría del sistema
ID del evento de Windows	`201`
ID del evento de Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Licencia a punto de caducar

Estado	!
Componente	Auditoría del sistema
ID del evento de Windows	`203`

ID del evento de Kaspersky Security Center	000000cb
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Faltan las bases de datos o están dañadas

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	206
ID del evento de Kaspersky Security Center	000000ce
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Las bases de datos están muy desactualizadas

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	207
ID del evento de Kaspersky Security Center	000000cf
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Autoejecución de la aplicación desactivada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	209
ID del evento de Kaspersky Security Center	000000d1
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de activación

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	229
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado una amenaza activa. Se debe iniciar la desinfección avanzada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	231
ID del evento de Kaspersky Security Center	000000e7

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Servidores de KSN no disponibles

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	2023
ID del evento de Kaspersky Security Center	000007e7
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No hay espacio suficiente en el almacenamiento de Cuarentena

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	343
ID del evento de Kaspersky Security Center	00000157
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto no restaurado de Cuarentena

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	346
ID del evento de Kaspersky Security Center	0000015a
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto no eliminado de Cuarentena

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	348
ID del evento de Kaspersky Security Center	0000015c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La aplicación estableció una conexión a un sitio web con un certificado no confiable

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	57
ID del evento de Kaspersky Security Center	00000039

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error en la verificación de una conexión cifrada. El dominio se añade a la lista de exclusiones

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	`60`
ID del evento de Kaspersky Security Center	`0000003c`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto malicioso detectado (bases de datos locales)

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Prevención de intrusiones en el host Detección de comportamiento Anti-Cryptor Prevención de exploits Análisis antimalware
ID del evento de Windows	`302`
ID del evento de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el hash del objeto (SHA256). • `GNRL_EA_PARAM_2` es el nombre del objeto. Si se detecta el cifrado externo de carpetas compartidas, la aplicación muestra la ruta al archivo de destino. • `GNRL_EA_PARAM_5` es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_8` es el tipo de amenaza (tipo ?). • `GNRL_EA_PARAM_9` es información adicional sobre el objeto detectado: Componente de la aplicación (`engine` ?). Tecnología de detección de amenazas (`method` ?). Amenaza detectada por Kaspersky Private Security Network (`blacklist`): `true` o `false`. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto malicioso detectado (KSN)

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Prevención de intrusiones en el host Detección de comportamiento Anti-Cryptor Prevención de exploits Análisis antimalware
ID del evento de Windows	`302`
ID del evento de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el hash del objeto (SHA256). • `GNRL_EA_PARAM_2` es el nombre del objeto. • `GNRL_EA_PARAM_5` es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_8` es el tipo de amenaza (tipo ?). • `GNRL_EA_PARAM_9` es información adicional sobre el objeto detectado: Componente de la aplicación (`engine` ?). Tecnología de detección de amenazas (`method` ?). Amenaza detectada por Kaspersky Private Security Network (`blacklist`): `true` o `false`. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede desinfectar

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas en el correo Prevención de intrusiones en el host Detección de comportamiento Anti-Cryptor Análisis antimalware
ID del evento de Windows	`312`
ID del evento de Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el hash del objeto (SHA256). • `GNRL_EA_PARAM_2` es el nombre del objeto. • `GNRL_EA_PARAM_5` es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_8` es el tipo de amenaza (tipo ?). • `GNRL_EA_PARAM_9` es información adicional sobre el objeto detectado: Componente de la aplicación (`engine` ?). Tecnología de detección de amenazas (`method` ?). Amenaza detectada por Kaspersky Private Security Network (`blacklist`): `true` o `false`. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede eliminar

Estado	⚠
Componente	Protección frente a amenazas en archivos Prevención de intrusiones en el host Detección de comportamiento Anti-Cryptor Análisis antimalware
ID del evento de Windows	313
ID del evento de Kaspersky Security Center	00000139
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de procesamiento

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Prevención de intrusiones en el host Protección AMSI Análisis antimalware
ID del evento de Windows	317
ID del evento de Kaspersky Security Center	0000013d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Proceso finalizado

Estado	⚠
Componente	Protección frente a amenazas en archivos Prevención de intrusiones en el host Detección de comportamiento Análisis antimalware
ID del evento de Windows	452
ID del evento de Kaspersky Security Center	000001c4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede finalizar el proceso

Estado	⚠
Componente	Protección frente a amenazas en archivos Prevención de intrusiones en el host Detección de comportamiento Análisis antimalware
ID del evento de Windows	453
ID del evento de Kaspersky Security Center	000001c5
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Vínculo peligroso bloqueado

Estado	ⓘ
Componente	Protección frente a amenazas web
ID del evento de Windows	362
ID del evento de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Parámetros de eventos	• GNRL_EA_PARAM_2 es la ruta al objeto. • GNRL_EA_PARAM_5 es el nombre del objeto según la clasificación de Kaspersky. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por KSN privada (blacklist): true o false.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Vínculo peligroso abierto

Estado	ⓘ
Componente	Protección frente a amenazas web
ID del evento de Windows	363
ID del evento de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Parámetros de eventos	• GNRL_EA_PARAM_2 es la ruta al objeto. • GNRL_EA_PARAM_5 es el nombre del objeto según la clasificación de Kaspersky. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por KSN privada (blacklist): true o false.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado un vínculo peligroso abierto anteriormente

Estado	ⓘ
Componente	Protección frente a amenazas web
ID del evento de Windows	1201
ID del evento de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Parámetros de eventos	• GNRL_EA_PARAM_2 es la ruta al objeto. • GNRL_EA_PARAM_5 es el nombre del objeto según la clasificación de Kaspersky. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por KSN privada (blacklist): true o false.

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acción del proceso bloqueada

Estado	ⓘ
Componente	Control de anomalías adaptativo
ID del evento de Windows	`2200`
ID del evento de Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el nombre de la regla de Control de anomalías adaptativo. • `GNRL_EA_PARAM_2` es el ID de la regla heurística. • `GNRL_EA_PARAM_3` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_4` es el proceso de origen. • `GNRL_EA_PARAM_5` es el objeto de origen. • `GNRL_EA_PARAM_6` es el proceso de destino. • `GNRL_EA_PARAM_7` es el objeto de destino. • `GNRL_EA_PARAM_8` es información adicional sobre el objeto detectado: Sumas de comprobación del proceso/objeto de origen y del proceso/objeto de destino. Proceso bloqueado (`verdict_type`): `true` o `false`. ID de seguridad del usuario (SID).
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Teclado no autorizado

Estado	ⓘ
Componente	Prevención de ataques de BadUSB
ID del evento de Windows	`2051`
ID del evento de Kaspersky Security Center	`00000803`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Solicitud AMSI bloqueada

Estado	ⓘ
Componente	Protección AMSI
ID del evento de Windows	`2200`
ID del evento de Kaspersky Security Center	`00000898`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Actividad de red bloqueada

Estado	ⓘ
Componente	Firewall
ID del evento de Windows	`602`
ID del evento de Kaspersky Security Center	`00000329`

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Ataque de red detectado

Estado	⚠
Componente	Protección frente a amenazas en la red
ID del evento de Windows	`651`
ID del evento de Kaspersky Security Center	`GNRL_EV_ATTACK_DETECTED`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el nombre del ataque. • `GNRL_EA_PARAM_2` es el protocolo. • `GNRL_EA_PARAM_3` es la dirección IP del equipo que actúa como origen del ataque de red. La dirección IP se indica en el orden de bytes del host. Por ejemplo, `2886729929` para `172.16.0.201`. • `GNRL_EA_PARAM_4` es el número de puerto. • `GNRL_EA_PARAM_5` es una dirección IPv6, por ejemplo, `12B012B012B012B012B012B012B012B0`. • `GNRL_EA_PARAM_6` es la dirección IP del equipo al que está dirigido el ataque de red. La dirección IP se indica en el orden de bytes del host. Por ejemplo, `2886729929` para `172.16.0.201`.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Inicio de la aplicación prohibido

Estado	⚠
Componente	Control de aplicaciones
ID del evento de Windows	`702`
ID del evento de Kaspersky Security Center	`GNRL_EV_APPLICATION_LAUNCH_DENIED`
Parámetros de eventos	• `GNRL_EA_PARAM_2` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_3` es el identificador de categoría que se creó manualmente. • `GNRL_EA_PARAM_4` es el identificador de la categoría de la aplicación. • `GNRL_EA_PARAM_5` es información sobre la firma digital de la aplicación. • `GNRL_EA_PARAM_6` es el nombre del archivo ejecutable de la aplicación (por ejemplo, chrome.exe). • `GNRL_EA_PARAM_7` es la ruta al archivo ejecutable. • `GNRL_EA_PARAM_8` es el hash del objeto (SHA256). • `GNRL_EA_PARAM_9` es la versión de la aplicación que el usuario está intentando ejecutar.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se inició un proceso prohibido antes del arranque de Kaspersky Endpoint Security

Estado	⚠
Componente	Control de aplicaciones
ID del evento de Windows	`710`
ID del evento de Kaspersky Security Center	`000002c6`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso denegado (bases de datos locales)

Estado	⚠
Componente	Control Web
ID del evento de Windows	752
ID del evento de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parámetros de eventos	• GNRL_EA_PARAM_1 es la URL. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 es el nombre de la regla de Control Web.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso denegado (KSN)

Estado	⚠
Componente	Control Web
ID del evento de Windows	752
ID del evento de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parámetros de eventos	• GNRL_EA_PARAM_1 es la URL. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 es el nombre de la regla de Control Web.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Operación con el dispositivo prohibida

Estado	⚠
Componente	Control de dispositivos
ID del evento de Windows	802
ID del evento de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parámetros de eventos	• GNRL_EA_PARAM_1 es la id. del hardware (HWID). • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión de red bloqueada

Estado	⚠
Componente	Control de dispositivos
ID del evento de Windows	809
ID del evento de Kaspersky Security Center	00000329
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se prohíbe realizar operaciones con el dispositivo hasta que se inicie Kaspersky Endpoint Security

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	816
ID del evento de Kaspersky Security Center	00000330
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se prohíbe conectar el dispositivo hasta que se inicie Kaspersky Endpoint Security

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	817
ID del evento de Kaspersky Security Center	00000331
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al actualizar el componente

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	1011
ID del evento de Kaspersky Security Center	000003f3
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al distribuir las actualizaciones de componentes

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	1012
ID del evento de Kaspersky Security Center	000003f4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error de actualización local

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	1014
ID del evento de Kaspersky Security Center	000003f6
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error de actualización de red

Estado	⊗
Componente	Actualización
ID del evento de Windows	1015
ID del evento de Kaspersky Security Center	000003f7
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

No se puede iniciar dos tareas a la vez

Estado	⊗
Componente	Actualización
ID del evento de Windows	1017
ID del evento de Kaspersky Security Center	000003f9
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al verificar las bases de datos y módulos de la aplicación

Estado	⊗
Componente	Actualización
ID del evento de Windows	1018
ID del evento de Kaspersky Security Center	000003fa
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error en la interacción con Kaspersky Security Center

Estado	⊗
Componente	Actualización
ID del evento de Windows	1019
ID del evento de Kaspersky Security Center	000003fb
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se han actualizado todos los componentes

Estado	⊗
Componente	Actualización
ID del evento de Windows	1021
ID del evento de Kaspersky Security Center	000003fd
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Actualización completada correctamente. Error de la distribución de actualizaciones

Estado	⚠
Componente	Actualización
ID del evento de Windows	1023
ID del evento de Kaspersky Security Center	000003ff
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error interno de tarea

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	101
ID del evento de Kaspersky Security Center	00000065
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error al instalar parche

Estado	⚠
Componente	Actualización
ID del evento de Windows	2153
ID del evento de Kaspersky Security Center	00000869
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al revertir parche

Estado	⚠
Componente	Actualización
ID del evento de Windows	2156
ID del evento de Kaspersky Security Center	0000086c
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al implementar las reglas de cifrado o descifrado de archivos

Estado	⚠
Componente	Cifrado de datos
ID del evento de Windows	904
ID del evento de Kaspersky Security Center	00000388
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error en el cifrado o descifrado de archivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	912
ID del evento de Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Parámetros de eventos	• GNRL_EA_PARAM_1 es la ruta al archivo. • GNRL_EA_PARAM_2 es el motivo del error. • GNRL_EA_PARAM_3 es el tipo de dispositivo.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso al archivo bloqueado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	940
ID del evento de Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Parámetros de eventos	• GNRL_EA_PARAM_1 es el objeto de destino. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 el nombre del archivo ejecutable de la aplicación (por ejemplo, chrome.exe) que intenta acceder al archivo.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error al activar el modo portátil

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	951
ID del evento de Kaspersky Security Center	000003b7
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al desactivar el modo portátil

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	953
ID del evento de Kaspersky Security Center	000003b9
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al crear el paquete cifrado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	931
ID del evento de Kaspersky Security Center	000003a3
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al cifrar/descifrar dispositivo

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1305
ID del evento de Kaspersky Security Center	00000519
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se ha podido cargar el módulo de cifrado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1311
ID del evento de Kaspersky Security Center	0000051f
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La tarea de administración de cuentas del Agente de autenticación ha finalizado con un error

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1340
ID del evento de Kaspersky Security Center	0000053c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La directiva no se puede aplicar

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	1312
ID del evento de Kaspersky Security Center	00000520
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al actualizar FDE

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1342
ID del evento de Kaspersky Security Center	0000053e
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al revertir actualización de FDE (para obtener más información, consulte la ayuda en línea de Kaspersky Endpoint Security para Windows)

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1344
ID del evento de Kaspersky Security Center	00000540
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Servidor de Kaspersky Anti Targeted Attack Platform no disponible

Estado	ⓘ
Componente	Endpoint Sensor
ID del evento de Windows	2100
ID del evento de Kaspersky Security Center	00000834
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se ha podido eliminar el objeto

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2252
ID del evento de Kaspersky Security Center	000008cc
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto no está en cuarentena (Sandbox)

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2603
ID del evento de Kaspersky Security Center	00000a2b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Ha ocurrido un error interno

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2607
ID del evento de Kaspersky Security Center	00000a2f
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado del servidor de Sandbox no válido

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2613
ID del evento de Kaspersky Security Center	00000a35
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El nodo Sandbox no está disponible

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2614
ID del evento de Kaspersky Security Center	00000a36
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al procesar el objeto en Sandbox

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2617
ID del evento de Kaspersky Security Center	00000a39
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se superó la carga máxima a Sandbox

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2618
ID del evento de Kaspersky Security Center	00000a3a
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

IOC encontrado

Estado	⚠
Componente	Endpoint Detection and Response
ID del evento de Windows	2651
ID del evento de Kaspersky Security Center	00000a5b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se produjo un error al verificar la licencia de Sandbox

Estado	⚠
Componente	Sandbox
ID del evento de Windows	2620
ID del evento de Kaspersky Security Center	00000a3c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al enviar la tarea de análisis a Sandbox por parte de un usuario

Estado	⚠
Componente	Sandbox
ID del evento de Windows	2623
ID del evento de Kaspersky Security Center	00000a3e
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al crear la tarea de Sandbox

Estado	⚠
Componente	Sandbox
ID del evento de Windows	2621
ID del evento de Kaspersky Security Center	00000a3d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha bloqueado el inicio del objeto

Estado	⚠
Componente	Endpoint Detection and Response
ID del evento de Windows	2553
ID del evento de Kaspersky Security Center	000009f9
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha bloqueado el inicio del proceso

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2551
ID del evento de Kaspersky Security Center	000009f7
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Ejecución de script bloqueada

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2559
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto no está en cuarentena (Endpoint Detection and Response)

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2556
ID del evento de Kaspersky Security Center	000009fc
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El inicio del proceso no está bloqueado

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2561
ID del evento de Kaspersky Security Center	00000a01
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto no está bloqueado

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2562
ID del evento de Kaspersky Security Center	00000a02
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La ejecución de script no está bloqueada

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2563
ID del evento de Kaspersky Security Center	00000a03
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al cambiar los componentes de la aplicación

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	1401
ID del evento de Kaspersky Security Center	00000579
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Hay patrones de un posible ataque de fuerza bruta en el sistema

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2800
ID del evento de Kaspersky Security Center	00000af0
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Hay patrones de un posible abuso del Registro de eventos de Windows

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2801
ID del evento de Kaspersky Security Center	00000af1
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se han detectado acciones atípicas en nombre de un nuevo servicio instalado

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2802
ID del evento de Kaspersky Security Center	00000af2
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado un inicio de sesión atípico que usa credenciales explícitas

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2803
ID del evento de Kaspersky Security Center	00000af3
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Hay patrones de un posible ataque de PAC de Kerberos (MS14-068) en el sistema

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2804
ID del evento de Kaspersky Security Center	00000af4
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se han detectado cambios sospechosos en el grupo de administradores integrado con privilegios

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2805
ID del evento de Kaspersky Security Center	00000af5
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado una actividad atípica durante una sesión de inicio de sesión de red

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2806
ID del evento de Kaspersky Security Center	00000af6
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Regla de inspección de registro activada

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2807
ID del evento de Kaspersky Security Center	00000af7
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Un evento atípico tiene lugar con demasiada frecuencia. Agregación de evento iniciada

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2808
ID del evento de Kaspersky Security Center	00000af8
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe sobre un evento atípico del periodo de agregación

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2809
ID del evento de Kaspersky Security Center	00000af9
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectar con el servidor de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID del evento de Windows	2850
ID del evento de Kaspersky Security Center	00000b22
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID del evento de Windows	2851
ID del evento de Kaspersky Security Center	00000b23
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID del evento de Windows	2852
ID del evento de Kaspersky Security Center	00000b24
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectar con el servidor de respuesta de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2858
ID del evento de Kaspersky Security Center	00000b22
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de respuesta de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2859
ID del evento de Kaspersky Security Center	00000b23
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de respuesta de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2860
ID del evento de Kaspersky Security Center	00000b24
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de conexión al servidor de recopilación de telemetría de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2854
ID del evento de Kaspersky Security Center	00000b22
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de recopilación de telemetría de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2855
ID del evento de Kaspersky Security Center	00000b23

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de recopilación de telemetría de EDR Expert

Estado	⚠
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	`2856`
ID del evento de Kaspersky Security Center	`00000b24`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectar con el servidor NDR

Estado	⚠
Componente	Network Detection and Response (KATA)
ID del evento de Windows	`3080`
ID del evento de Kaspersky Security Center	`00000c08`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor NDR

Estado	⚠
Componente	Network Detection and Response (KATA)
ID del evento de Windows	`3081`
ID del evento de Kaspersky Security Center	`00000c09`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor NDR

Estado	⚠
Componente	Network Detection and Response (KATA)
ID del evento de Windows	`3082`
ID del evento de Kaspersky Security Center	`00000c0a`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El dispositivo está conectado a un servidor de administración no fiable. Póngase en contacto con el administrador

Estado	⚠
Componente	Protección de la conexión al servidor de administración
ID del evento de Windows	`3301`

ID del evento de Kaspersky Security Center	00000ce5
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado la modificación de un archivo o una carpeta

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2950
ID del evento de Kaspersky Security Center	00000b86
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

El objeto cambia con demasiada frecuencia. Agregación de eventos iniciada

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2955
ID del evento de Kaspersky Security Center	00000b8b
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informar sobre la modificación del objeto durante el periodo de agregación

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2953
ID del evento de Kaspersky Security Center	00000b89
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2956
ID del evento de Kaspersky Security Center	00000b8c
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Se detectó el cambio de registro

Estado	/ /
Componente	Control de integridad del sistema
ID del evento de Windows	2951
ID del evento de Kaspersky Security Center	00000b87
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Se ha detectado una conexión/desconexión de dispositivos

Estado	/ /
Componente	Control de integridad del sistema
ID del evento de Windows	2952
ID del evento de Kaspersky Security Center	00000b88
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

La cobertura de la supervisión incluye objetos incorrectos

Estado	/ /
Componente	Control de integridad del sistema
ID del evento de Windows	2903
ID del evento de Kaspersky Security Center	00000b89
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Demasiados intentos de realizar las operaciones restringidas con el objeto. Se ha iniciado la agregación de eventos

Estado	
Componente	Control de integridad del sistema
ID del evento de Windows	2963
ID del evento de Kaspersky Security Center	00000b93

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó una operación con los archivos de la cobertura de supervisión

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2959
ID del evento de Kaspersky Security Center	00000b8f
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Modificación de registro bloqueada

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2960
ID del evento de Kaspersky Security Center	00000b90
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Error de procesamiento

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2954
ID del evento de Kaspersky Security Center	00000b8a
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de integridad del sistema: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2964
ID del evento de Kaspersky Security Center	00000b94
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de aplicaciones: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas

Estado	ⓘ
Componente	Control de aplicaciones
ID del evento de Windows	711
ID del evento de Kaspersky Security Center	000002c7
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de dispositivos: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	810
ID del evento de Kaspersky Security Center	0000032a
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control Web: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas

Estado	ⓘ
Componente	Control Web
ID del evento de Windows	757
ID del evento de Kaspersky Security Center	000002f5
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de anomalías adaptativo: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas

Estado	ⓘ
Componente	Control de anomalías adaptativo
ID del evento de Windows	504
ID del evento de Kaspersky Security Center	000001f8
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Inspección de registros: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas

Estado	ⓘ
Componente	Inspección de registros
ID del evento de Windows	2810
ID del evento de Kaspersky Security Center	00000afa

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

SVM no disponible

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3151
ID del evento de Kaspersky Security Center	00000c4f
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto malicioso detectado. La desinfección avanzada debería iniciarse en una plantilla de máquina virtual

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3182
ID del evento de Kaspersky Security Center	00000c6e
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La conexión de red establecida en el protocolo obsoleto se bloqueó

Estado	⚠
Componente	Protección
ID del evento de Windows	75
ID del evento de Kaspersky Security Center	0000004b
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de conexión al servidor KUMA

Estado	⚠
Componente	Integración con KUMA
ID del evento de Windows	2854
ID del evento de Kaspersky Security Center	00000b26
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor KUMA

Estado	⚠
Componente	Integración con KUMA
ID del evento de Windows	2855
ID del evento de Kaspersky Security Center	00000b27

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor KUMA

Estado	⚠
Componente	Integración con KUMA
ID del evento de Windows	2856
ID del evento de Kaspersky Security Center	00000b28
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de conexión al servidor SIEM

Estado	⚠
Componente	Integración con KUMA
ID del evento de Windows	3250
ID del evento de Kaspersky Security Center	00000cb2
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor SIEM

Estado	⚠
Componente	Integración con KUMA
ID del evento de Windows	3251
ID del evento de Kaspersky Security Center	00000cb3
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor SIEM

Estado	⚠
Componente	Integración con KUMA
ID del evento de Windows	3252
ID del evento de Kaspersky Security Center	00000cb4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Fallo operativo

La tarea no se puede llevar a cabo

Estado	⊗
Componente	Auditoría del sistema
ID del evento de Windows	212
ID del evento de Kaspersky Security Center	000000d4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La configuración de la tarea no es válida y no se ha aplicado

Estado	⊗
Componente	Auditoría del sistema
ID del evento de Windows	707
ID del evento de Kaspersky Security Center	000002c3
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Advertencia

La aplicación falló durante una sesión anterior

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	237
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La licencia caduca pronto

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	204
ID del evento de Kaspersky Security Center	000000cc
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Las bases de datos están desactualizadas

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	208
ID del evento de Kaspersky Security Center	000000d0

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Las actualizaciones automáticas están desactivadas

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	210
ID del evento de Kaspersky Security Center	000000d2
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Autoprotección desactivada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	211
ID del evento de Kaspersky Security Center	000000d3
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Componentes de protección desactivados

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	214
ID del evento de Kaspersky Security Center	000000d6
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El equipo se está ejecutando en modo seguro

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	215
ID del evento de Kaspersky Security Center	000000d7
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Hay archivos no procesados

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	216
ID del evento de Kaspersky Security Center	000000d8

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Directiva de grupo aplicada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	219
ID del evento de Kaspersky Security Center	000000db
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Tarea detenida

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	222
ID del evento de Kaspersky Security Center	000000de
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para completar la actualización, salga de la aplicación y vuelva a abrirla

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	224
ID del evento de Kaspersky Security Center	0000057b
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Es necesario reiniciar el equipo

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	225
ID del evento de Kaspersky Security Center	000000e1
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La licencia permite usar componentes que no se han instalado

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	226
ID del evento de Kaspersky Security Center	000000e2

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Desinfección avanzada iniciada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	232
ID del evento de Kaspersky Security Center	000000e8
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Desinfección avanzada completada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	233
ID del evento de Kaspersky Security Center	000000e9
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Clave de reserva incorrecta

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	230
ID del evento de Kaspersky Security Center	000000e6
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La suscripción caducará pronto

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	240
ID del evento de Kaspersky Security Center	000000f0
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Bloqueado

Estado	⚠
Componente	Detección de comportamiento Anti-Cryptor Prevención de exploits Protección frente a amenazas web
ID del evento de Windows	331

ID del evento de Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el hash del objeto (SHA256). • GNRL_EA_PARAM_2 es el nombre del objeto. Si se detecta el cifrado externo de carpetas compartidas, la aplicación muestra la ruta al archivo de destino. • GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por Kaspersky Private Security Network (blacklist): true o false. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La configuración del sistema operativo no permite controlar el acceso a redes wifi

Estado	⚠
Componente	Control de dispositivos
ID del evento de Windows	249
ID del evento de Kaspersky Security Center	000000f9
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto no restaurado de Copia de seguridad

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	336
ID del evento de Kaspersky Security Center	00000150
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha detectado actividad de red sospechosa

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	2001
ID del evento de Kaspersky Security Center	000007d1
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión cifrada terminada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	250
ID del evento de Kaspersky Security Center	000007d3
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La participación en KSN está desactivada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	2021
ID del evento de Kaspersky Security Center	000007e5
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El procesamiento de algunas funciones del SO está desactivado

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	245
ID del evento de Kaspersky Security Center	000000f5
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El almacenamiento de Cuarentena ya casi no tiene espacio libre

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	344
ID del evento de Kaspersky Security Center	00000158
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión de red bloqueada

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	809
ID del evento de Kaspersky Security Center	00000abe
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede crear una copia de seguridad

Estado	⚠
Componente	Protección frente a amenazas en archivos Detección de comportamiento Anti-Cryptor Prevención de intrusiones en el host Análisis antimalware
ID del evento de Windows	310
ID del evento de Kaspersky Security Center	00000136
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto no procesado

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas en el correo Prevención de intrusiones en el host Protección AMSI Análisis antimalware
ID del evento de Windows	314
ID del evento de Kaspersky Security Center	0000013a
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto cifrado

Estado	⚠
Componente	Prevención de intrusiones en el host
ID del evento de Windows	320
ID del evento de Kaspersky Security Center	00000140
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto dañado

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Prevención de intrusiones en el host Análisis antimalware
ID del evento de Windows	321
ID del evento de Kaspersky Security Center	00000141
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales (bases locales)

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Prevención de intrusiones en el host Protección AMSI Detección de comportamiento Anti-Cryptor Anti-Cryptor Análisis antimalware
ID del evento de Windows	`303`
ID del evento de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el hash del objeto (SHA256). • `GNRL_EA_PARAM_2` es el nombre del objeto. • `GNRL_EA_PARAM_5` es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_8` es el tipo de amenaza (tipo ?).
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales (KSN)

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Prevención de intrusiones en el host Protección AMSI Detección de comportamiento Anti-Cryptor Anti-Cryptor Análisis antimalware
ID del evento de Windows	`303`
ID del evento de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el hash del objeto (SHA256). • `GNRL_EA_PARAM_2` es el nombre del objeto. • `GNRL_EA_PARAM_5` es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_8` es el tipo de amenaza (tipo ?).
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas en el correo Prevención de intrusiones en el host Prevención de exploits Detección de comportamiento Anti-Cryptor Análisis antimalware

ID del evento de Windows	307
ID del evento de Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el hash del objeto (SHA256). • GNRL_EA_PARAM_2 es el nombre del objeto. • GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por Kaspersky Private Security Network (blacklist): true o false. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto desinfectado

Estado	⚠
Componente	Protección frente a amenazas en archivos Protección frente a amenazas en el correo Prevención de intrusiones en el host Análisis antimalware
ID del evento de Windows	306
ID del evento de Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el hash del objeto (SHA256). • GNRL_EA_PARAM_2 es el nombre del objeto. • GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por Kaspersky Private Security Network (blacklist): true o false. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto se desinfectará al reiniciar

Estado	⚠
Componente	Prevención de intrusiones en el host Protección frente a amenazas en archivos Análisis antimalware
ID del evento de Windows	324
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El objeto se eliminará al reiniciar

Estado	⚠
Componente	Detección de comportamiento Anti-Cryptor Prevención de exploits Prevención de intrusiones en el host Protección frente a amenazas en archivos Análisis antimalware
ID del evento de Windows	323
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto eliminado según la configuración

Estado	⚠
Componente	Protección frente a amenazas en el correo
ID del evento de Windows	342
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Reversión completada

Estado	⚠
Componente	Protección frente a amenazas en archivos Detección de comportamiento Anti-Cryptor Prevención de exploits Análisis antimalware
ID del evento de Windows	455
ID del evento de Kaspersky Security Center	000001c7
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al eliminar la versión anterior de la aplicación

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	246
ID del evento de Kaspersky Security Center	000000f6
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha bloqueado la descarga del objeto

Estado	⚠
Componente	Protección frente a amenazas web

ID del evento de Windows	341
ID del evento de Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el hash del objeto (SHA256). • GNRL_EA_PARAM_2 es el nombre del objeto. • GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por Kaspersky Private Security Network (blacklist): true o false. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de autorización del teclado

Estado	⚠
Componente	Prevención de ataques de BadUSB
ID del evento de Windows	2052
ID del evento de Kaspersky Security Center	00000804
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El resultado del análisis del objeto se ha enviado a una aplicación de terceros

Estado	⚠
Componente	Protección AMSI
ID del evento de Windows	1512
ID del evento de Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el hash del objeto (SHA256). • GNRL_EA_PARAM_2 es el nombre del objeto. • GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_8 es el tipo de amenaza (tipo ?). • GNRL_EA_PARAM_9 es información adicional sobre el objeto detectado: Componente de la aplicación (engine ?). Tecnología de detección de amenazas (method ?). Amenaza detectada por Kaspersky Private Security Network (blacklist): true o false. Versión de EDR. Identificador de amenazas en EDR. Hash MD5 del objeto.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Configuración de tarea aplicada correctamente

Estado	⚠
Componente	Control de aplicaciones
ID del evento de Windows	708
ID del evento de Kaspersky Security Center	000002c4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Advertencia acerca de contenido indeseado (bases de datos locales)

Estado	⚠
Componente	Control Web
ID del evento de Windows	708
ID del evento de Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parámetros de eventos	• GNRL_EA_PARAM_1 es la URL. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 es el nombre de la regla de Control Web.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Advertencia acerca de contenido indeseado (KSN)

Estado	⚠
Componente	Control Web
ID del evento de Windows	708
ID del evento de Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parámetros de eventos	• GNRL_EA_PARAM_1 es la URL. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 es el nombre de la regla de Control Web.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha accedido a contenido indeseado tras una advertencia

Estado	⚠
Componente	Control Web
ID del evento de Windows	754
ID del evento de Kaspersky Security Center	000002f2
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Acceso temporal al dispositivo activado

Estado	⚠
Componente	Control de dispositivos
ID del evento de Windows	803
ID del evento de Kaspersky Security Center	000002f2

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Operación cancelada por el usuario

Estado	⚠
Componente	Actualización
ID del evento de Windows	1016
ID del evento de Kaspersky Security Center	000003f8
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El usuario ha optado por no implementar la directiva de cifrado

Estado	⚠
Componente	Cifrado de datos
ID del evento de Windows	1306
ID del evento de Kaspersky Security Center	0000051a
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha interrumpido la implementación de las reglas de cifrado o descifrado de archivos

Estado	⚠
Componente	Cifrado de datos
ID del evento de Windows	903
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha interrumpido el cifrado o descifrado de archivos

Estado	⚠
Componente	Cifrado de datos
ID del evento de Windows	914
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha interrumpido el cifrado o descifrado de dispositivos

Estado	⚠
Componente	Cifrado de datos
ID del evento de Windows	1303
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

No se han podido instalar ni actualizar los controladores de Cifrado de disco de Kaspersky en la imagen de WinRE

Estado	⚠
Componente	Cifrado de datos
ID del evento de Windows	1345
ID del evento de Kaspersky Security Center	00000541
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al comprobar la firma del módulo

Estado	⚠
Componente	Comprobación de la integridad del sistema
ID del evento de Windows	2002
ID del evento de Kaspersky Security Center	000007d2
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha bloqueado el inicio de la aplicación

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2105
ID del evento de Kaspersky Security Center	00000839
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha bloqueado la apertura del documento

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2106
ID del evento de Kaspersky Security Center	0000083a
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El proceso ha sido finalizado por el administrador del servidor de Kaspersky Anti Targeted Attack Platform

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2112
ID del evento de Kaspersky Security Center	00000840

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La aplicación ha sido finalizada por el administrador del servidor de Kaspersky Anti Targeted Attack Platform

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2113
ID del evento de Kaspersky Security Center	00000841
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El archivo o la secuencia ha sido eliminado por el administrador del servidor de Kaspersky Anti Targeted Attack Platform

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2111
ID del evento de Kaspersky Security Center	0000083f
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador ha restaurado el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2110
ID del evento de Kaspersky Security Center	0000083e
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador ha puesto el archivo en cuarentena en el servidor de Kaspersky Anti Targeted Attack Platform

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2109
ID del evento de Kaspersky Security Center	0000083d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La actividad de red de las aplicaciones de terceros se ha bloqueado

Estado	⚠
Componente	Endpoint Sensor

ID del evento de Windows	2107
ID del evento de Kaspersky Security Center	0000083b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha desbloqueado la actividad de red de todas las aplicaciones de terceros

Estado	⚠
Componente	Endpoint Sensor
ID del evento de Windows	2108
ID del evento de Kaspersky Security Center	0000083c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto se borrará tras el reinicio (Sandbox)

Estado	⚠
Componente	Sandbox
ID del evento de Windows	2605
ID del evento de Kaspersky Security Center	00000a2d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El tamaño total de las tareas de análisis superó el límite

Estado	⚠
Componente	Sandbox
ID del evento de Windows	2612
ID del evento de Kaspersky Security Center	00000a34
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha permitido el inicio del objeto, el evento está registrado

Estado	⚠
Componente	Endpoint Detection and Response
ID del evento de Windows	2553
ID del evento de Kaspersky Security Center	000009fa
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha permitido el inicio del proceso, el evento está registrado

Estado	⚠
Componente	Endpoint Detection and Response

ID del evento de Windows	2554
ID del evento de Kaspersky Security Center	000009f8
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto se borrará tras el reinicio (Endpoint Detection and Response)

Estado	⚠
Componente	Endpoint Detection and Response
ID del evento de Windows	2558
ID del evento de Kaspersky Security Center	000009fe
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Aislamiento de red

Estado	⚠
Componente	Endpoint Detection and Response
ID del evento de Windows	2700
ID del evento de Kaspersky Security Center	00000a8c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Finalización del aislamiento de red

Estado	⚠
Componente	Endpoint Detection and Response
ID del evento de Windows	2701
ID del evento de Kaspersky Security Center	00000a8d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se debe reiniciar para completar la tarea

Estado	⚠
Componente	Auditoría del sistema
ID del evento de Windows	225
ID del evento de Kaspersky Security Center	0000057b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión a un sitio web con un certificado no confiable establecida por decisión del usuario

Estado	⚠
Componente	Network Detection and Response (KATA)

ID del evento de Windows	70
ID del evento de Kaspersky Security Center	00000046
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Mensaje al administrador por bloqueo del inicio de la aplicación

Estado	⚠
Componente	Control de aplicaciones
ID del evento de Windows	503
ID del evento de Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Parámetros de eventos	• GNRL_EA_DESCRIPTION es el mensaje al usuario. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_6 es el nombre del archivo ejecutable de la aplicación (por ejemplo, chrome.exe). • GNRL_EA_PARAM_7 es la ruta al archivo ejecutable. • GNRL_EA_PARAM_8 es el hash del objeto (SHA256). • GNRL_EA_PARAM_9 es la versión de la aplicación que el usuario está intentando ejecutar.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje al administrador por bloqueo del acceso al dispositivo

Estado	⚠
Componente	Control de dispositivos
ID del evento de Windows	804
ID del evento de Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Parámetros de eventos	• c_er_descr es el mensaje al usuario. • GNRL_EA_PARAM_1 es la id. del hardware (HWID). • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje al administrador por bloqueo del acceso a la página web

Estado	⚠
Componente	Control Web
ID del evento de Windows	755
ID del evento de Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Parámetros de eventos	• GNRL_EA_DESCRIPTION es el mensaje al usuario. • GNRL_EA_PARAM_1 es la URL. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión del dispositivo bloqueada

Estado	⚠
Componente	Control de dispositivos
ID del evento de Windows	`807`
ID del evento de Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUG_DENIED`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es la id. del hardware (HWID). • `GNRL_EA_PARAM_2` es el nombre del usuario de la sesión.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje al administrador por bloqueo de la actividad de aplicaciones

Estado	⚠
Componente	Control de anomalías adaptativo
ID del evento de Windows	`503`
ID del evento de Kaspersky Security Center	`GNRL_EV_ADSEC_USER_REQUEST`
Parámetros de eventos	• `GNRL_EA_DESCRIPTION` es el mensaje al usuario. • `GNRL_EA_PARAM_1` es el nombre de la regla de Control de anomalías adaptativo. • `GNRL_EA_PARAM_2` es el ID de la regla heurística. • `GNRL_EA_PARAM_3` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_4` es el proceso de origen. • `GNRL_EA_PARAM_5` es el objeto de origen. • `GNRL_EA_PARAM_6` es el proceso de destino. • `GNRL_EA_PARAM_7` es el objeto de destino. • `GNRL_EA_PARAM_8` es información adicional sobre el objeto detectado: Hashes del proceso/objeto de origen y del proceso/objeto de destino. Proceso bloqueado (`verdict_type`): `true` o `false`. ID de seguridad del usuario (SID).
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El inicio de la aplicación cliente de servicios en la nube está bloqueado

Estado	⚠
Componente	Cloud Discovery
ID del evento de Windows	`2212`
ID del evento de Kaspersky Security Center	`000008a4`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El acceso al servicio en la nube está bloqueado

Estado	⚠
Componente	Cloud Discovery
ID del evento de Windows	`2213`
ID del evento de Kaspersky Security Center	`000008a5`

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado la modificación de un archivo o una carpeta

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2950
ID del evento de Kaspersky Security Center	00000b86
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

El objeto cambia con demasiada frecuencia. Agregación de eventos iniciada

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2955
ID del evento de Kaspersky Security Center	00000b8b
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informar sobre la modificación del objeto durante el periodo de agregación

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2956
ID del evento de Kaspersky Security Center	00000b8c
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Se detectó el cambio de registro

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2951
ID del evento de Kaspersky Security Center	00000b87
Registro de eventos de Windows (predeterminado)	–

Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Se ha detectado una conexión/desconexión de dispositivos

Estado	ⓘ / ⚠ / ⓔ
Componente	Control de integridad del sistema
ID del evento de Windows	2952
ID del evento de Kaspersky Security Center	00000b88
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

La cobertura de la supervisión incluye objetos incorrectos

Estado	ⓘ / ⚠ / ⓔ
Componente	Control de integridad del sistema
ID del evento de Windows	2903
ID del evento de Kaspersky Security Center	00000b89
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

La operación prohibida se permitió en el modo de prueba

Estado	⚠
Componente	Control de integridad del sistema
ID del evento de Windows	2961
ID del evento de Kaspersky Security Center	00000b91
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No es posible conectar con el servidor de integración durante más de 30 minutos. Compruebe el estado del servidor de integración y la configuración de red

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3102

ID del evento de Kaspersky Security Center	00000c1e
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede conectar con el servidor de integración durante más de 6 horas. Compruebe el estado del servidor de integración y la configuración de red

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3103
ID del evento de Kaspersky Security Center	00000c1f
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede conectar al servidor de integración. Compruebe el estado y la configuración de red del mismo

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3101
ID del evento de Kaspersky Security Center	00000c1d
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Es necesario actualizar la plantilla de la máquina virtual

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3181
ID del evento de Kaspersky Security Center	00000c6d
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La licencia Standard ha finalizado. La aplicación se está ejecutando con la licencia Enterprise

Estado	⚠
Componente	Light Agent
ID del evento de Windows	3171
ID del evento de Kaspersky Security Center	00000c64
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Estado	⚠
Componente	Monitor de integridad de archivos
ID del evento de Windows	2901
ID del evento de Kaspersky Security Center	00000b55

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Estado	⚠
Componente	Monitor de integridad de archivos
ID del evento de Windows	2900
ID del evento de Kaspersky Security Center	00000b54
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje de información

Aplicación iniciada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	235
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Aplicación detenida

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	236
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La Autoprotección restringió el acceso al recurso protegido

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	213
ID del evento de Kaspersky Security Center	000000d5
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe borrado

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	217

ID del evento de Kaspersky Security Center	000000d9
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Directiva de grupo desactivada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	220
ID del evento de Kaspersky Security Center	000000dc
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Configuración de la aplicación modificada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	218
ID del evento de Kaspersky Security Center	000000da
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Tarea iniciada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	221
ID del evento de Kaspersky Security Center	000000dd
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Tarea terminada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	223
ID del evento de Kaspersky Security Center	000000df
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Todos los componentes de la aplicación definidos por la licencia se han instalado y se ejecutan en modo normal

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	227

ID del evento de Kaspersky Security Center	000000e3
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La configuración de suscripción ha cambiado

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	238
ID del evento de Kaspersky Security Center	000000ee
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha renovado la suscripción

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	239
ID del evento de Kaspersky Security Center	000000ef
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto restaurado de Copia de seguridad

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	335
ID del evento de Kaspersky Security Center	0000014f
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Introducción del nombre de usuario y la contraseña

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	2000
ID del evento de Kaspersky Security Center	000007d0
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La participación en KSN está activada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	2020

ID del evento de Kaspersky Security Center	000007e4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Servidores de KSN disponibles

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	2022
ID del evento de Kaspersky Security Center	000007e6
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La aplicación funciona y procesa datos según las leyes correspondientes, y usa la infraestructura adecuada

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	2024
ID del evento de Kaspersky Security Center	000007e8
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto restaurado de Cuarentena

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	345
ID del evento de Kaspersky Security Center	00000159
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado de Cuarentena

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	347
ID del evento de Kaspersky Security Center	0000015b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha creado una copia de seguridad del objeto

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas en el correo Detección de comportamiento Anti-Cryptor Prevención de intrusiones en el host Sandbox Análisis antimalware
ID del evento de Windows	`308`
ID del evento de Kaspersky Security Center	`00000134`
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Sobrescrito por una copia desinfectada anteriormente

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Prevención de intrusiones en el host Análisis antimalware
ID del evento de Windows	`327`
ID del evento de Kaspersky Security Center	`00000147`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo protegido por contraseña detectado

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Prevención de intrusiones en el host Análisis antimalware
ID del evento de Windows	`322`
ID del evento de Kaspersky Security Center	`GNRL_EV_PASSWD_ARCHIVE_FOUND`
Parámetros de eventos	• `GNRL_EA_PARAM_2` es el nombre del objeto. • `GNRL_EA_PARAM_3` es la fecha de creación del objeto (opcional). • `GNRL_EA_PARAM_7` es el nombre del usuario de la sesión. • `GNRL_EA_PARAM_9` es información adicional sobre el objeto detectado: Componente de la aplicación (`engine`). Tecnología de detección de amenazas (`method`). Amenaza detectada por KSN privada (denylist): verdadero o falso.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Información sobre el objeto detectado

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Prevención de intrusiones en el host Análisis antimalware

ID del evento de Windows	332
ID del evento de Kaspersky Security Center	0000014c
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto está en la lista de permitidos de Kaspersky Private Security Network

Estado	ⓘ
Componente	Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Prevención de intrusiones en el host Análisis antimalware
ID del evento de Windows	340
ID del evento de Kaspersky Security Center	00000154
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto renombrado

Estado	ⓘ
Componente	Protección frente a amenazas en el correo Prevención de exploits Detección de comportamiento Anti-Cryptor Análisis antimalware
ID del evento de Windows	329
ID del evento de Kaspersky Security Center	00000149
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto procesado

Estado	ⓘ
Componente	Prevención de intrusiones en el host Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Análisis antimalware
ID del evento de Windows	301
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto omitido

Estado	ⓘ
Componente	Prevención de intrusiones en el host Protección frente a amenazas en archivos Protección AMSI Análisis antimalware

ID del evento de Windows	315
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo detectado

Estado	ⓘ
Componente	Prevención de intrusiones en el host Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Análisis antimalware
ID del evento de Windows	318
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto comprimido detectado

Estado	ⓘ
Componente	Prevención de intrusiones en el host Protección frente a amenazas en archivos Protección frente a amenazas web Protección frente a amenazas en el correo Protección AMSI Análisis antimalware
ID del evento de Windows	319
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Vínculo procesado

Estado	ⓘ
Componente	Protección frente a amenazas web
ID del evento de Windows	361
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Inicio de la aplicación permitido

Estado	ⓘ
Componente	Control de aplicaciones
ID del evento de Windows	701
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Origen de actualizaciones seleccionado

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	1001
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Servidor proxy seleccionado

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	1002
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El vínculo está en la lista de permitidos de Kaspersky Private Security Network

Estado	ⓘ
Componente	Protección frente a amenazas web
ID del evento de Windows	370
ID del evento de Kaspersky Security Center	00000172
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Aplicación colocada en el grupo de confianza

Estado	ⓘ
Componente	Prevención de intrusiones en el host
ID del evento de Windows	401
ID del evento de Kaspersky Security Center	00000191
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Aplicación colocada en grupo restringido

Estado	ⓘ
Componente	Prevención de intrusiones en el host
ID del evento de Windows	402
ID del evento de Kaspersky Security Center	00000192

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Prevención de intrusiones en el host accionada

Estado	ⓘ
Componente	Prevención de intrusiones en el host
ID del evento de Windows	403
ID del evento de Kaspersky Security Center	00000193
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Archivo restaurado

Estado	ⓘ
Componente	Detección de comportamiento Anti-Cryptor Prevención de exploits Prevención de intrusiones en el host
ID del evento de Windows	457
ID del evento de Kaspersky Security Center	000001c9
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Valor del registro restaurado

Estado	ⓘ
Componente	Detección de comportamiento Prevención de exploits
ID del evento de Windows	458
ID del evento de Kaspersky Security Center	000001ca
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Valor del registro eliminado

Estado	ⓘ
Componente	Detección de comportamiento Prevención de exploits
ID del evento de Windows	459
ID del evento de Kaspersky Security Center	000001cb
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Acción del proceso omitida

Estado	ⓘ
Componente	Control de anomalías adaptativo

ID del evento de Windows	2201
ID del evento de Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Parámetros de eventos	• GNRL_EA_PARAM_1 es el nombre de la regla de Control de anomalías adaptativo. • GNRL_EA_PARAM_2 es el ID de la regla heurística. • GNRL_EA_PARAM_3 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_4 es el proceso de origen. • GNRL_EA_PARAM_5 es el objeto de origen. • GNRL_EA_PARAM_6 es el proceso de destino. • GNRL_EA_PARAM_7 es el objeto de destino. • GNRL_EA_PARAM_8 es información adicional sobre el objeto detectado: Hashes del proceso/objeto de origen y del proceso/objeto de destino. Proceso bloqueado (verdict_type): true o false. ID de seguridad del usuario (SID).
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Teclado autorizado

Estado	ⓘ
Componente	Prevención de ataques de BadUSB
ID del evento de Windows	2050
ID del evento de Kaspersky Security Center	00000802
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Actividad de red permitida

Estado	ⓘ
Componente	Firewall
ID del evento de Windows	601
ID del evento de Kaspersky Security Center	00000259
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Inicio de la aplicación prohibido en el modo de prueba

Estado	ⓘ
Componente	Control de aplicaciones
ID del evento de Windows	703
ID del evento de Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Parámetros de eventos	• GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 es el identificador de categoría que se creó manualmente. • GNRL_EA_PARAM_4 es el identificador de seguridad de la cuenta (SID). • GNRL_EA_PARAM_5 es información sobre la firma digital de la aplicación. • GNRL_EA_PARAM_6 es el nombre del archivo ejecutable de la aplicación (por ejemplo, chrome.exe). • GNRL_EA_PARAM_7 es la ruta al archivo ejecutable. • GNRL_EA_PARAM_8 es el hash del objeto (SHA256). • GNRL_EA_PARAM_9 es la versión de la aplicación que el usuario está intentando ejecutar.

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Inicio de la aplicación permitido en el modo de prueba

Estado	ⓘ
Componente	Control de aplicaciones
ID del evento de Windows	704
ID del evento de Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Parámetros de eventos	• GNRL_EA_PARAM_2 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_3 es el identificador de categoría que se creó manualmente. • GNRL_EA_PARAM_4 es el identificador de seguridad de la cuenta (SID). • GNRL_EA_PARAM_5 es información sobre la firma digital de la aplicación.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha abierto una página permitida

Estado	ⓘ
Componente	Control Web
ID del evento de Windows	751
ID del evento de Kaspersky Security Center	000002f4
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Operación con el dispositivo permitida

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	801
ID del evento de Kaspersky Security Center	00000321
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Operación de archivo realizada

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	808
ID del evento de Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Parámetros de eventos	• GNRL_EA_PARAM_1 es la operación de archivo (escribir o borrar). • GNRL_EA_PARAM_2 es la ruta al archivo. • GNRL_EA_PARAM_3 es el nombre del dispositivo. • GNRL_EA_PARAM_4 es el nombre del usuario de la sesión. • GNRL_EA_PARAM_5 es la id. del hardware (HWID).

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

No hay actualizaciones disponibles

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1020`
ID del evento de Kaspersky Security Center	`000003fc`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Distribución de actualizaciones completada correctamente

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1022`
ID del evento de Kaspersky Security Center	`000003fe`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Descargando archivos

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1003`
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo descargado

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1004`
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo instalado

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1005`
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo actualizado

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1006`
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo revertido debido a un error de actualización

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1007`
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Actualizando archivos

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1008`
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Distribuyendo actualizaciones

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1009`
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Revirtiendo archivos

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	`1010`
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Creando la lista de archivos para descargar

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	1013
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Descargando parches

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	2150
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Instalando parche

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	2151
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Parche instalado

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	2152
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Revirtiendo parche

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	2154
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Parche revertido

Estado	ⓘ
Componente	Actualización
ID del evento de Windows	2155
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha iniciado la implementación de las reglas de cifrado o descifrado de archivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	901
ID del evento de Kaspersky Security Center	00000385
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha completado la implementación de las reglas de cifrado o descifrado de archivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	902
ID del evento de Kaspersky Security Center	00000386
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha reanudado la implementación de las reglas de cifrado o descifrado de archivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	905
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha iniciado el cifrado o descifrado de archivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	910
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha completado el cifrado o descifrado de archivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	911
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El archivo no se ha cifrado porque es una exclusión

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	913
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Modo portátil activado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	950
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Modo portátil desactivado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	952
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha iniciado el cifrado o descifrado de dispositivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1301
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha completado el cifrado o descifrado de dispositivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1302
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha reanudado el cifrado o descifrado de dispositivos

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1304
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El dispositivo no está cifrado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1307
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El proceso de cifrado o descifrado de dispositivos se ha cambiado al modo activo

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1308
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El proceso de cifrado o descifrado de dispositivos se ha cambiado al modo pasivo

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1309
ID del evento de Kaspersky Security Center	–

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha cargado el módulo de cifrado

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1310
ID del evento de Kaspersky Security Center	0000051e
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Nueva cuenta del Agente de autenticación creada

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1330
ID del evento de Kaspersky Security Center	00000532
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cuenta del Agente de autenticación eliminada

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1331
ID del evento de Kaspersky Security Center	00000533
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Contraseña de la cuenta del Agente de autenticación cambiada

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1332
ID del evento de Kaspersky Security Center	00000534
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Inicio de sesión del Agente de autenticación correcto

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1333
ID del evento de Kaspersky Security Center	00000535

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Intento de inicio de sesión del Agente de autenticación fallido

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1334
ID del evento de Kaspersky Security Center	00000536
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha accedido al disco duro con el procedimiento de solicitud de acceso a dispositivos cifrados

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1335
ID del evento de Kaspersky Security Center	00000537
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Intento fallido de acceder al disco duro con el procedimiento de solicitud de acceso a dispositivos cifrados

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1336
ID del evento de Kaspersky Security Center	00000538
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La cuenta no se ha añadido. Esta cuenta ya existe

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1337
ID del evento de Kaspersky Security Center	00000539
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La cuenta no se ha modificado. Esta cuenta no existe

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1338
ID del evento de Kaspersky Security Center	0000053a

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La cuenta no se ha eliminado. Esta cuenta no existe

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1339
ID del evento de Kaspersky Security Center	0000053b
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Actualización de FDE correcta

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1341
ID del evento de Kaspersky Security Center	0000053d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Deshacer actualización de FDE correcta

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1343
ID del evento de Kaspersky Security Center	0000053f
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se han podido desinstalar los controladores de Cifrado de disco de Kaspersky de la imagen de WinRE

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1346
ID del evento de Kaspersky Security Center	00000542
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se cambió la clave de recuperación de BitLocker

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1370
ID del evento de Kaspersky Security Center	0000055a

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha modificado el PIN o la contraseña de BitLocker

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1371
ID del evento de Kaspersky Security Center	0000055b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La clave de recuperación de BitLocker se guardó en una unidad extraíble

Estado	ⓘ
Componente	Cifrado de datos
ID del evento de Windows	1372
ID del evento de Kaspersky Security Center	0000055c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El procesamiento de tareas del servidor de Kaspersky Anti Targeted Attack Platform está inactivo

Estado	ⓘ
Componente	Endpoint Sensor
ID del evento de Windows	2103
ID del evento de Kaspersky Security Center	00000837
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El componente Endpoint Sensor se ha conectado al servidor

Estado	ⓘ
Componente	Endpoint Sensor
ID del evento de Windows	2101
ID del evento de Kaspersky Security Center	00000835
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha recuperado la conexión con el servidor de Kaspersky Anti Targeted Attack Platform

Estado	ⓘ
Componente	Endpoint Sensor
ID del evento de Windows	2102
ID del evento de Kaspersky Security Center	00000836

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El procesamiento de tareas del servidor de Kaspersky Anti Targeted Attack Platform está activo

Estado	ⓘ
Componente	Endpoint Sensor
ID del evento de Windows	2104
ID del evento de Kaspersky Security Center	00000838
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado

Estado	ⓘ
Componente	Eliminación de datos
ID del evento de Windows	2251
ID del evento de Kaspersky Security Center	000008cb
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Estadísticas de la tarea de eliminación

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID del evento de Windows	2853
ID del evento de Kaspersky Security Center	00000b25
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Estado	ⓘ
Componente	Eliminación de datos
ID del evento de Windows	2253
ID del evento de Kaspersky Security Center	000008cd
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto en cuarentena (Sandbox)

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2602
ID del evento de Kaspersky Security Center	00000a2a
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado (Sandbox)

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2604
ID del evento de Kaspersky Security Center	00000a2c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se ha iniciado el análisis de IOC

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2652
ID del evento de Kaspersky Security Center	00000a5c
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha completado el análisis de IOC

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2653
ID del evento de Kaspersky Security Center	00000a5d
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto en cuarentena (Endpoint Detection and Response)

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2555
ID del evento de Kaspersky Security Center	000009fb
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado (Endpoint Detection and Response)

Estado	ⓘ
Componente	Endpoint Detection and Response
ID del evento de Windows	2557
ID del evento de Kaspersky Security Center	000009fd
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Los componentes de la aplicación se han cambiado correctamente

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	1402
ID del evento de Kaspersky Security Center	0000057a
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2606
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2609
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2610
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	2616
ID del evento de Kaspersky Security Center	–
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El servidor de administración al que está conectado su dispositivo está definido como de confianza

Estado	ⓘ
Componente	Protección de la conexión al servidor de administración
ID del evento de Windows	3300
ID del evento de Kaspersky Security Center	00000ce4

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El dispositivo está conectado a un nuevo servidor de administración de confianza

Estado	ⓘ
Componente	Protección de la conexión al servidor de administración
ID del evento de Windows	`3302`
ID del evento de Kaspersky Security Center	`00000ce6`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El servidor de administración al que está conectado su dispositivo ya no está definido como de confianza

Estado	ⓘ
Componente	Protección de la conexión al servidor de administración
ID del evento de Windows	`3303`
ID del evento de Kaspersky Security Center	`00000ce7`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Detección asíncrona de Sandbox

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	`2619`
ID del evento de Kaspersky Security Center	`GNRL_EV_APP_INCIDENT_OCCURED`
Parámetros de eventos	• `GNRL_EA_PARAM_1` son los parámetros de los componentes de Sandbox. • `GNRL_EA_PARAM_2` es la ruta al objeto. • `GNRL_EA_PARAM_3` es la id. del incidente. • `GNRL_EA_PARAM_4` es el hash del objeto (SHA256).
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Un usuario ha enviado la tarea de análisis a Sandbox correctamente

Estado	ⓘ
Componente	Sandbox
ID del evento de Windows	`2622`
ID del evento de Kaspersky Security Center	`00000a3e`
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El dispositivo está conectado

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	805
ID del evento de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Parámetros de eventos	• GNRL_EA_PARAM_1 es la id. del hardware (HWID). • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El dispositivo está desconectado

Estado	ⓘ
Componente	Control de dispositivos
ID del evento de Windows	806
ID del evento de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Parámetros de eventos	• GNRL_EA_PARAM_1 es la id. del hardware (HWID). • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión correcta al servidor de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID del evento de Windows	2853
ID del evento de Kaspersky Security Center	00000b25
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión correcta al servidor de respuesta de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2853
ID del evento de Kaspersky Security Center	00000b25
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión correcta al servidor de recopilación de telemetría de EDR Expert

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID del evento de Windows	2857
ID del evento de Kaspersky Security Center	00000b26

Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión correcta al servidor NDR

Estado	ⓘ
Componente	Network Detection and Response (KATA)
ID del evento de Windows	3083
ID del evento de Kaspersky Security Center	00000c0b
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se permite iniciar la aplicación cliente del servicio en la nube

Estado	ⓘ
Componente	Cloud Discovery
ID del evento de Windows	2210
ID del evento de Kaspersky Security Center	000008a2
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se permite acceder al servicio en la nube

Estado	ⓘ
Componente	Cloud Discovery
ID del evento de Windows	2211
ID del evento de Kaspersky Security Center	000008a3
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso al área protegida

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	2004
ID del evento de Kaspersky Security Center	000007d4
Registro de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha detectado la modificación de un archivo o una carpeta

Estado	ⓘ / ⚠ / ⓔ
Componente	Control de integridad del sistema
ID del evento de Windows	2950
ID del evento de Kaspersky Security Center	00000b86
Registro de eventos de Windows (predeterminado)	–

Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

El objeto cambia con demasiada frecuencia. Agregación de eventos iniciada

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2955
ID del evento de Kaspersky Security Center	00000b8b
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informar sobre la modificación del objeto durante el periodo de agregación

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2956
ID del evento de Kaspersky Security Center	00000b8c
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Se detectó el cambio de registro

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2951
ID del evento de Kaspersky Security Center	00000b87
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Se ha detectado una conexión/desconexión de dispositivos

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2952
ID del evento de Kaspersky Security Center	00000b88

Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

La cobertura de la supervisión incluye objetos incorrectos

Estado	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2903
ID del evento de Kaspersky Security Center	00000b89
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Línea de base creada

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2957
ID del evento de Kaspersky Security Center	00000b8d
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Línea de base actualizada

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2958
ID del evento de Kaspersky Security Center	00000b8e
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El usuario de confianza realiza una operación

Estado	ⓘ
Componente	Control de integridad del sistema
ID del evento de Windows	2962
ID del evento de Kaspersky Security Center	00000b92
Registro de eventos de Windows (predeterminado)	–

Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención de este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Supervisión de la integridad del sistema: *Se ha detectado la modificación de un archivo o una carpeta*.

Conectado a SVM

Estado	ⓘ
Componente	Light Agent
ID del evento de Windows	3152
ID del evento de Kaspersky Security Center	00000c50
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se creó una nueva contraseña temporal

Estado	ⓘ
Componente	Auditoría del sistema
ID del evento de Windows	265
ID del evento de Kaspersky Security Center	00000109
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conectado al servidor de integración

Estado	ⓘ
Componente	Light Agent
ID del evento de Windows	3105
ID del evento de Kaspersky Security Center	00000c21
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Restaurando conexión con el servidor de integración

Estado	ⓘ
Componente	Light Agent
ID del evento de Windows	3104
ID del evento de Kaspersky Security Center	00000c20
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión correcta al servidor KUMA

Estado	ⓘ
Componente	Integración con KUMA

ID del evento de Windows	2857
ID del evento de Kaspersky Security Center	00000b29
Registro de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Apéndice 7. Extensiones de archivos compatibles con la Prevención de ejecución

Kaspersky Endpoint Security es compatible con la prevención de la apertura de archivos en formato Office en ciertas aplicaciones. La información acerca de las extensiones de archivos y aplicaciones compatibles se enumera en la siguiente tabla.

Extensiones de archivos compatibles con la Prevención de ejecución

Nombre de aplicación	Archivo ejecutable	Extensión del archivo
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Nombre de aplicación	Archivo ejecutable	Extensión del archivo
Adobe Acrobat	acrord32.exe	pdf
Lector de PDF de Foxit	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Navegador Tor	tor.exe	

Apéndice 8. Intérpretes de script admitidos para la Prevención de ejecución

La Prevención de ejecución es compatible con los siguientes intérpretes de script:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

La Prevención de ejecución admite el funcionamiento con aplicaciones de Java en el entorno de tiempo de ejecución de Java (procesos de java.exe y javaw.exe).

Apéndice 9. Cobertura de análisis de IOC en el registro (RegistryItem)

Cuando añade el tipo de datos **Registro de Windows: RegistryItem** a la cobertura de análisis de IOC, Kaspersky Endpoint Security analiza las siguientes claves de registro de forma predeterminada:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Apéndice 10. Requisitos de los archivos de IOC

Al crear tareas de análisis de IOC, considere los siguientes requerimientos y limitaciones de los archivos de IOC:

- La aplicación es compatible con archivos IOC con extensiones IOC y XML en el estándar abierto OpenIOC versiones 1.0 y 1.1 para describir indicadores de compromiso.
- Después de cargar archivos de IOC, puede editar manualmente los archivos en el editor integrado directamente en las propiedades de la tarea. Kaspersky Endpoint Security admite la edición de archivos de IOC que cumplen con el estándar OpenIOC 1.1. No es posible modificar el contenido de los archivos IOC que cumplan con la versión 1.0 de OpenIOC.
- Si, al crear una tarea de *Análisis de IOC* en la línea de comandos, carga archivos de IOC y algunos no son compatibles, la aplicación utiliza solo los archivos de IOC compatibles cuando se ejecuta la tarea. Si, al crear una tare *Análisis de IOC* en la línea de comandos, ninguno de los archivo de IOC que carga resultan ser compatibles, la tarea puede ejecutarse de todos modos. Sin embargo, no detectará ningún indicador de riesgo. No es posible cargar archivos de IOC no compatibles a través de Web Console o Cloud Console.

- Los errores semánticos y los términos y etiquetas de IOC no compatibles en archivos de IOC no hacen que falle la ejecución de la tarea. En dichas secciones de archivos de IOC, la aplicación no detecta una coincidencia.
- Los identificadores de todos los archivos de IOC utilizados en una sola tarea de análisis de IOC deben ser únicos. Si hay archivos de IOC con el mismo identificador, esto puede afectar los resultados de la ejecución de la tarea.
- Un solo archivo de IOC no debe superar los 2 MB de tamaño. Usar archivos más grandes hará que las tareas de análisis de IOC finalicen con un error. El tamaño total de todos los archivos agregados a la colección IOC no debe superar los 10 MB. Si el tamaño total de todos los archivos supera los 10 MB, debe dividir la colección de IOC y crear varias tareas *Análisis de IOC*.
- Se recomienda crear un archivo de IOC por amenaza. Esto facilita el análisis de los resultados de la tarea *Análisis de IOC*.

El archivo que puede descargar al hacer clic en el enlace a continuación contiene una tabla con la lista completa de términos de IOC del estándar de OpenIOC.

DESCARGAR EL ARCHIVO IOC_TERMS.XLSX

Las funcionalidades y limitaciones en la compatibilidad de la aplicación con el estándar OpenIOC se enumeran en la siguiente tabla.

Funcionalidades y limitaciones en la compatibilidad con OpenIOC versiones 1.0 y 1.1.

Condiciones compatibles	OpenIOC 1.0:
	
	`is`
	`isnot` (como una excepción del grupo)
	`contains`
	`containsnot` (como una excepción del grupo)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Para los términos de correo electrónico / *, solo se admiten las condiciones `contains` y `is`. Para que el análisis IOC retrospectivo funcione correctamente, al utilizar la condición `is`, las direcciones de correo electrónico en los archivos IOC se deben especificar en el siguiente formato: `"name@example.org" <SMTP:name@example.org>`. Al ejecutar la tarea *Análisis de IOC* normalmente, es suficiente especificar la dirección de correo electrónico en el siguiente formato: `name@example.org`.

Atributos de la condición compatibles	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operadores compatibles	`AND` `OR`
Tipos de datos compatibles	`"date"`: fecha (condiciones aplicables: `is`, `greater-than`, `less-than`) `"int"`: ´número entero (condiciones aplicables `is`, `greater-than`, `less-than`) `"string"`: serie (condiciones aplicables: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duración en segundos (condiciones aplicables: `is`, `greater-than`, `less-than`)

Funcionalidades de interpretación de tipos de datos	Los tipos de datos `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` y `"base64Binary"` se interpretan como series.
	
	La aplicación es compatible con la interpretación de la configuración de `Content` para los tipos de datos `int` y `date` cuando se establecen en forma de intervalos:
	
	OpenIOC 1.0:
	Usar el operador `TO` en el campo `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Usar las condiciones `greater-than` y `less-than`
	Usar el operador `TO` en el campo `Content`
	La aplicación admite la interpretación de los tipos de datos `date` y `duration` si los indicadores se establecen en formato `ISO 8601, Zulu time zone, UTC`.

Apéndice 11. API para respuesta ante amenazas de EDR

Kaspersky Endpoint Security 12.9 para Windows presenta soporte con acciones de Respuesta ante amenazas de EDR (EDR responses) usando Kaspersky Security Center OpenAPI. Es decir, puede llamar a métodos de OpenAPI para automatizar la respuesta a amenazas de EDR usando Python. Puede llamar a estos métodos cuando se integran con soluciones SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, la solución de Kaspersky SIEM, es compatible con la OpenAPI de Respuesta ante amenazas de EDR a partir de la versión 3.4.1. Para ver scripts de ejemplo, consulte la documentación de KUMA.

Para realizar acciones de Respuesta ante amenazas de EDR, debe crear una solicitud y enviarla mediante KSC Open API (`AddIncident`). Una vez que se procesa la solicitud, se crea una tarea especial en la consola de Kaspersky Security Center.

Para crear tareas al responder ante amenazas de EDR, debe establecer una conexión en segundo plano entre el Servidor de administración y Kaspersky Security Center Web Console. El servicio de conexión en segundo plano está disponible en Kaspersky Security Center Windows 14.2 o posterior y en Kaspersky Security Center Linux 15.2 o posterior. No se admiten otras consolas, incluidas las consolas de las soluciones Kaspersky Detection and Response.

Para la Respuesta ante amenazas de EDR, debe especificar parámetros de solicitud básicos; por ejemplo, en formato JSON:

- `task` es el tipo de tarea (consulte a continuación).
- `targetHost` es el ID del equipo en el que se debe ejecutar el script. Argumento requerido. El script obtiene este argumento del evento.
- `responseEventIncidentArea` es el nombre de la aplicación que ejecutó el script (por ejemplo, `KUMA`). Este parámetro se añade al nombre de la tarea creada.

Para configurar la Respuesta ante amenazas de EDR, debe especificar la configuración de la tarea en formato JSON en el parámetro `"KLINCDT_BODY": json.dumps(data)`. Como resultado, la aplicación crea el `[Response][KUMA] <task type> - <Date> <Time> - <ID>` en la consola de Kaspersky Security Center.

Conexión a Kaspersky Security Center OpenAPI

Como parte de EDR Threat Response, la aplicación crea tareas especiales en la consola de Kaspersky Security Center. La creación de estas tareas requiere establecer una conexión entre el equipo y Kaspersky Security Center. Para lograr esto, los parámetros de conexión de Kaspersky Security Center deben especificarse en la solicitud.

En Kaspersky XDR versión 2.1, el método para autorizar solicitudes ha cambiado. Kaspersky XDR utiliza tokens PAT en lugar de la autenticación de nombre de usuario y contraseña. Por lo tanto, no es posible ejecutar scripts en Kaspersky XDR. Para obtener más información sobre la autorización de solicitudes, consulte la Ayuda de Kaspersky XDR.

Parámetros de conexión de Kaspersky Security Center

Parámetro	Tipo	Descripción
`kscHost`	`string`	Dirección del Servidor de administración de Kaspersky Security Center. Parámetro requerido.
`kscPort`	`int`	Puerto de conexión al Servidor de administración. Parámetro requerido.
`kscCert`	`string`	Ruta a un archivo de certificado para conectar al Servidor de administración de Kaspersky Security Center. De forma predeterminada, el parámetro está establecido en `False`.
`kscUser`	`string`	Nombre de la cuenta de usuario. Parámetro requerido.
`kscPassword`	`string`	Contraseña de la cuenta de usuario. Parámetro requerido.

Ejemplo

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Los datos de la cuenta de usuario no están protegidos; por tanto, debe dedicar un usuario independiente que se utilizará solo para realizar estas acciones.

Obtener archivo – getFile

Configuración de la tarea Obtener archivo

Parámetro	Tipo	Descripción
`md5hash`	`string`	Hash MD5 del archivo que desea obtener.
`sha256hash`	`string`	Hash SHA256 del archivo que desea obtener.
`path`	`string`	Ruta al archivo que desea obtener.

Ejemplo

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Eliminar archivo – deleteFile

Configuración de la tarea Eliminar archivo

Parámetro	Tipo	Descripción
`md5hash`	`string`	Hash MD5 del archivo que desea eliminar.
`sha256hash`	`string`	Hash SHA256 del archivo que desea eliminar.
`path`	`string`	Ruta al archivo que desea eliminar.
`searchInSubfolders?`	`boolean`	Busca el archivo que desea eliminar en subcarpetas.

Ejemplo

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Mover archivo a Cuarentena – quarantineFile

Configuración de la tarea Mover archivo a Cuarentena

Parámetro	Tipo	Descripción
md5hash	string	Hash MD5 del archivo que desea poner en cuarentena.
sha256hash	string	Hash SHA256 del archivo que desea poner en cuarentena.
path	string	Ruta al archivo que desea poner en cuarentena.

Ejemplo

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Análisis de IOC – iocScan

Configuración de la tarea Análisis de IOC

Parámetro	Tipo	Descripción
ioc	string	Ruta al archivo ZIP con un archivo de IOC que desee usar para el análisis.
isolateHost	boolean	Aísle el equipo de la red cuando se detecte un indicador de peligro para evitar que la amenaza se propague.
scanCriticalAreas	boolean	Ejecute la tarea *Análisis de áreas críticas* cuando se detecte un indicador de compromiso.
quarantineObject	boolean	Elimine el objeto malicioso cuando se detecte un indicador de compromiso. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.

Ejemplo

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Iniciar proceso – startProcess

Configuración de la tarea Iniciar proceso

Parámetro	Tipo	Descripción
executablePath	string	Ruta al archivo ejecutable que se utiliza para iniciar el proceso.
arguments?	string	Argumentos de línea de comandos adicionales para iniciar el proceso.
workingFolder?	string	Ruta a la carpeta de trabajo del proceso.

Ejemplo

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Terminar proceso – terminateProcess

Configuración de la tarea Terminar proceso

Parámetro	Tipo	Descripción
md5hash	string	Hash MD5 del archivo cuyo proceso desea finalizar.
sha256hash	string	Hash SHA256 del archivo cuyo proceso desea finalizar.
path	string	Ruta al archivo que desea eliminar.
caseSensitive	boolean	Distinción de mayúsculas y minúsculas al buscar el archivo.

Ejemplo

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Aislamiento de equipos de la red – isolateHost

Configuración del aislamiento de equipos de la red

Parámetro	Tipo	Descripción
`action`	`string`	Modo de funcionamiento de aislamiento de la red.

Ejemplo

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Prevención de ejecución – preventExecution

Configuración de prevención de ejecución

Parámetro	Tipo	Descripción
`hash`	`string`	Hash MD5 del archivo cuya ejecución desea evitar.
`path`	`string`	Ruta al archivo cuya ejecución desea evitar.
`caseSensitive`	`boolean`	Distinción de mayúsculas y minúsculas al buscar el archivo.

Ejemplo

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Análisis antimalware – onDemandScan

Configuración de la tarea Análisis antimalware

Parámetro	Tipo	Descripción
`path`	`string`	Lista delimitada por espacios de archivos y carpetas para análisis personalizado.
`recursive`	`boolean`	Modo de análisis recursivo.

Parámetro	Tipo	Descripción
type	number	Cobertura del análisis.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Ejemplo

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Apéndice 12. Cuentas de usuario en las reglas de los componentes de la aplicación

Para configurar algunos componentes de la aplicación, debe añadir reglas especiales. Por ejemplo, para Control web, debe añadir una regla con una lista de direcciones web que desea que la aplicación bloquee. En las reglas de componentes de la aplicación, también puede configurar una programación para el componente o seleccionar usuarios a los que la aplicación debe aplicar la regla.

Se deben añadir reglas para configurar los siguientes componentes de la aplicación:

- Control de aplicaciones.
- Control web.
- Control de dispositivos.
- Inspección de registros.
- Control de anomalías adaptativo.
- Control de integridad del sistema.

A partir de Kaspersky Endpoint Security para Windows 12.5, puede seleccionar usuarios no solo desde Active Directory, sino también desde la lista de usuarios en Kaspersky Security Center. También puede introducir los datos de la cuenta de usuario de forma manual. Esto significa que puede añadir usuarios de las siguientes formas:

- Active Directory (recomendado)
- Lista de usuarios en Kaspersky Security Center
- Cuenta de usuario local

Para utilizar correctamente todos los métodos de selección de usuarios, debe actualizar la aplicación Kaspersky Endpoint Security y el complemento de administración a la versión 12.5 o superior.

Kaspersky recomienda utilizar cuentas de usuario locales solo en casos especiales cuando no es posible utilizar cuentas de usuario de dominio. Para obtener detalles sobre los riesgos de seguridad del uso de cuentas locales, consulte la Base de conocimientos de Microsoft. Usted es totalmente responsable de la seguridad de un equipo si se utilizan cuentas de usuario locales; en particular, esto incluye la responsabilidad de controlar y restringir el acceso a la configuración de Kaspersky Endpoint Security.

La aplicación utiliza el SID (Identificador de seguridad) de los usuarios para identificarlos. Al utilizar cuentas de usuario de Active Directory o de la lista de usuarios de Kaspersky Security Center, la aplicación determina el SID en el Servidor de administración. Esto significa que la aplicación no representa una carga adicional para el equipo al momento de identificar a un usuario. Si agregó más de 1000 cuentas de usuario locales a una regla de aplicación, las aplicaciones se comunicarán con el controlador de dominio para identificar al usuario. Esto significa que la carga en el equipo aumenta. Para optimizar el impacto en el rendimiento del equipo, recomendamos utilizar cuentas de usuario de Active Directory o de la lista de usuarios de Kaspersky Security Center.

La aplicación utiliza nombres de NetBIOS para la identificación de cuentas de usuario añadidas manualmente en los formatos `<username>` y `<hostname>\<username>`. Un nombre de NetBIOS puede tener hasta 16 bytes (15 caracteres) de longitud. Si el nombre del equipo tiene más de 15 caracteres, la aplicación no puede identificar al usuario. Luego, la aplicación deshabilita la regla y genera un error; por ejemplo, *Control Web: los usuarios cuya identificación de seguridad (SID) no coincida no pueden activar reglas*. Para que la regla funcione, debe acortar manualmente el nombre del equipo. Puede agregar cuentas de usuario desde Active Directory o Kaspersky Security Center. En este caso, la aplicación acorta automáticamente el nombre del equipo.

Kaspersky Endpoint Security también admite usuarios y grupos integrados (como el grupo "Todos") en las reglas. Debido a cómo se determina el SID de un usuario, la aplicación permite usar solo cuentas de usuario integradas añadidas desde Active Directory o la lista de usuarios en Kaspersky Security Center. Las reglas en las que se añade una cuenta de usuario integrada localmente no funcionan.

Información legal

Provisión de datos

Esta sección contiene información sobre los datos que la aplicación Kaspersky Endpoint Security puede almacenar en el dispositivo y transmitir automáticamente a Kaspersky durante su funcionamiento.

La información recibida cuenta con protección de Kaspersky de acuerdo con la ley, los requisitos y las normativas aplicables de Kaspersky. Los datos se transmiten a través de canales de comunicación cifrados.

Provisión de datos según el Contrato de licencia de usuario final

Si se aplica un código de activación para activar Kaspersky Endpoint Security, acepta que la siguiente información se transmitirá a Kaspersky en forma periódica y automática con el fin de que se verifique el uso correcto de la aplicación:

- tipo, versión y localización de Kaspersky Endpoint Security;
- versiones de las actualizaciones instaladas para Kaspersky Endpoint Security;
- ID del equipo e ID de la instalación específica de Kaspersky Endpoint Security en el equipo;
- el número de serie del certificado e identificador de la clave de licencia activa;
- tipo, versión y velocidad de bits del sistema operativo, y nombre del entorno virtual (si Kaspersky Endpoint Security está instalado en un entorno virtual);
- ID de solicitud única para los servicios del Titular de los derechos;
- ID de los componentes de Kaspersky Endpoint Security que están activos cuando se transmite la información.

Kaspersky también puede usar esta información para generar estadísticas sobre la difusión y el uso del software de Kaspersky.

Al usar un código de activación, acepta transmitir automáticamente los datos indicados anteriormente. Si no acepta transmitir esta información a Kaspersky, debe usar un archivo clave para activar Kaspersky Endpoint Security.

Al aceptar las condiciones del Contrato de licencia de usuario final, acepta transmitir automáticamente la siguiente información:

- Al actualizar Kaspersky Endpoint Security:
  - versión de Kaspersky Endpoint Security;
  - ID de Kaspersky Endpoint Security;
  - clave activa;

- ID exclusivo de la ejecución de la tarea de actualización;
- ID exclusivo de la instalación de Kaspersky Endpoint Security.

- Al seguir los enlaces desde la interfaz de Kaspersky Endpoint Security:
  - versión de Kaspersky Endpoint Security;
  - versión del sistema operativo;
  - fecha de activación de Kaspersky Endpoint Security;
  - fecha de caducidad de la licencia;
  - fecha de creación de la clave;
  - fecha de instalación de Kaspersky Endpoint Security;
  - ID de Kaspersky Endpoint Security;
  - ID de la vulnerabilidad detectada en el sistema operativo;
  - ID de la última actualización instalado para Kaspersky Endpoint Security;
  - hash del archivo detectado como amenaza y el nombre de esta amenaza según la clasificación de Kaspersky;
  - categoría del error de activación de Kaspersky Endpoint Security;
  - código del error de activación de Kaspersky Endpoint Security;
  - número de días antes del vencimiento de la clave;
  - número de días que han pasado desde que se añadió la clave;
  - número de días que han pasado desde que se caducó la licencia;
  - número de equipos en los que se aplica la licencia actual;
  - clave activa;
  - período de validez de la licencia de Kaspersky Endpoint Security;
  - estado actual de la licencia;
  - tipo de licencia actual;
  - tipo de aplicación;
  - ID exclusivo de la ejecución de la tarea de actualización;
  - ID exclusivo de la instalación de Kaspersky Endpoint Security en el equipo;
  - idioma de la interfaz de Kaspersky Endpoint Security.

La información recibida cuenta con protección de Kaspersky de acuerdo con la ley, los requisitos y las normativas aplicables de Kaspersky. Los datos se transmiten a través de canales de comunicación cifrados.

Puede leer el Contrato de licencia de usuario final y visitar el sitio web de Kaspersky para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn_<ID de idioma>.txt con el texto del Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network se incluyen en el kit de distribución de la aplicación.

Provisión de datos al usar Kaspersky Security Network

El conjunto de datos que Kaspersky Endpoint Security envía a Kaspersky depende del tipo de licencia y de la configuración de uso de Kaspersky Security Network.

Uso de KSN bajo licencia en no más de 4 equipos

Al aceptar la Declaración de Kaspersky Security Network, acepta transmitir automáticamente la siguiente información:

- información sobre las actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida, código de error de la actualización de la configuración;
- información sobre los archivos y las direcciones URL que deben escanearse: las sumas de comprobación del archivo escaneado (MD5, SHA2-256, SHA1) y el patrón del archivo (MD5), el tamaño del patrón, el tipo de amenaza detectada y su nombre de acuerdo con la clasificación del Titular de los derechos; el identificador de las bases de datos antivirus, la dirección URL en la que se solicita la reputación, así como la dirección URL de referencia, el identificador del protocolo de conexión y el número del puerto utilizado;
- ID de la tarea de análisis que detectó la amenaza;
- información sobre los certificados digitales que se usaron y que se necesitaba para verificar su autenticidad: las sumas de comprobación (SHA256) del certificado que se usó para firmar el objeto analizado y la clave pública del certificado;
- identificador del componente de software que realiza el análisis;
- identificadores de las bases de datos antivirus y de los registros de estas bases de datos antivirus;
- información sobre la activación del Software en el equipo: encabezado del ticket firmado por el servicio de activación (identificador del centro de activación regional, suma de control del código de activación, suma de control del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket, estado de la licencia, fecha y hora de inicio y fin de la validez del ticket, identificador único de la licencia, versión de la licencia), identificador del certificado utilizado para firmar el encabezado del ticket, suma de control (MD5) del archivo clave;
- Información sobre el Titular de los derechos del Software: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

Uso de KSN bajo licencia en 5 o más equipos

Al aceptar la Declaración de Kaspersky Security Network, acepta transmitir automáticamente la siguiente información:

Si se selecciona la casilla de verificación **Kaspersky Security Network** y se desactiva la casilla **Activar el modo ampliado de KSN**, la aplicación envía la siguiente información:

- información sobre las actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida, código de error de la actualización de la configuración;
- información sobre los archivos y las direcciones URL que deben escanearse: las sumas de comprobación del archivo escaneado (MD5, SHA2-256, SHA1) y el patrón del archivo (MD5), el tamaño del patrón, el tipo de amenaza detectada y su nombre de acuerdo con la clasificación del Titular de los derechos; el identificador de las bases de datos antivirus, la dirección URL en la que se solicita la reputación, así como la dirección URL de referencia, el identificador del protocolo de conexión y el número del puerto utilizado;
- ID de la tarea de análisis que detectó la amenaza;
- información sobre los certificados digitales que se usaron y que se necesitaba para verificar su autenticidad: las sumas de comprobación (SHA256) del certificado que se usó para firmar el objeto analizado y la clave pública del certificado;
- identificador del componente de software que realiza el análisis;
- identificadores de las bases de datos antivirus y de los registros de estas bases de datos antivirus;
- información sobre la activación del Software en el equipo: encabezado del ticket firmado por el servicio de activación (identificador del centro de activación regional, suma de control del código de activación, suma de control del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket, estado de la licencia, fecha y hora de inicio y fin de la validez del ticket, identificador único de la licencia, versión de la licencia), identificador del certificado utilizado para firmar el encabezado del ticket, suma de control (MD5) del archivo clave;
- Información sobre el Titular de los derechos del Software: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

Si se selecciona **Activar el modo ampliado de KSN** además de la casilla **Kaspersky Security Network**, la aplicación también enviará la información indicada a continuación, además de la enumerada arriba:

- información sobre los resultados de la categorización de los recursos web solicitados, lo que contiene la URL procesada y la dirección IP del host, la versión del componente del Software que realizó la categorización, el método de categorización y el conjunto de categorías que definió el recurso web;
- información sobre el software instalado en el equipo: nombres de las aplicaciones de software y de los proveedores de software, claves de registro y sus valores, información sobre los archivos de los componentes de software instalados (sumas de comprobación [MD5, SHA2-256, SHA1], nombre, ruta al archivo en el equipo, tamaño, versión y firma digital);
- información sobre el estado de la protección antivirus del equipo: las versiones y las marcas de tiempo de lanzamiento de las bases de datos antivirus que se utilizan, el ID de la tarea y el ID del Software que realiza el análisis;

- información sobre los archivos descargados por el Usuario final: la dirección URL y la dirección IP de la descarga y dirección URL de la página que se visitó antes de la página de descarga, el identificador del protocolo de descarga y el número de puerto de conexión, el estado de las direcciones URL como maliciosas o no, los atributos de archivo, el tamaño y las sumas de comprobación (MD5, SHA2-256, SHA1), información sobre el proceso que ha descargado el archivo (sumas de comprobación [MD5, SHA2-256, SHA1], la fecha y la hora de creación/compilación, el estado de reproducción automática, los atributos, los nombres de compresores, información sobre las firmas, el indicador de archivo ejecutable, el identificador de formato y el tipo de cuenta utilizada para iniciar el proceso), información sobre el archivo del proceso (nombre, ruta de archivo y tamaño), el nombre del archivo y su ruta en el equipo, la firma digital del archivo y la fecha y la hora de su generación, la dirección URL donde se produjo la detección, el número de script en la página que parece sospechosa o dañina e información sobre las peticiones HTTP generadas y la respuesta a las mismas;

- información sobre las aplicaciones que se ejecutan y sus módulos: los datos sobre procesos que se ejecutan en el sistema (el identificador del proceso [PID], el nombre del proceso; la información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, el indicio de programa o proceso de confianza, la ruta de acceso completa a los archivos del proceso y sus sumas de comprobación (MD5, SHA2-256, SHA1), y la línea de comandos de inicio; el nivel de integridad del proceso; una descripción del producto al que pertenece el proceso [el nombre del producto y la información sobre el editor], así como los certificados digitales utilizados y la información necesaria para verificar su autenticidad o la información acerca de la ausencia de la firma digital de un archivo); información sobre los módulos cargados en los procesos (sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación [MD5, SHA2-256, SHA1], las rutas de acceso a estos en el equipo); información sobre el encabezado del archivo PE, los nombres de los empaquetadores (si el archivo estaba empaquetado);

- información sobre todos los objetos y actividades potencialmente maliciosos: nombre del objeto detectado y ruta completa al objeto en el equipo, sumas de comprobación de los archivos procesados (MD5, SHA2-256, SHA1), fecha y hora de detección, nombres y tamaños de los archivos infectados y rutas a estos archivos, código de plantilla de la ruta, indicador de si el objeto es un contenedor o no, indicador de archivo ejecutable, nombre del compresor (si el archivo estaba comprimido), código del tipo de archivo, ID del formato de archivo, lista de acciones realizadas por el malware y decisión tomada por el software y el usuario en respuesta, identificadores de las bases de datos antivirus y de los registros en estas bases de datos antivirus usados para tomar la decisión, indicador de objeto potencialmente malicioso, nombre de la amenaza detectada según la clasificación del titular de los derechos, nivel de peligro, estado y método de detección, razón por la que se incluyó en el contexto analizado y número de secuencia del archivo en el contexto, sumas de comprobación (MD5, SHA2-256, SHA1), nombre y atributos del archivo ejecutable de la aplicación a través del que se transmitió el mensaje o enlace infectado, direcciones IP despersonalizadas (IPv4 e IPv6) del host del objeto bloqueado, entropía del archivo, indicador de archivo autoejecutable, hora en que el archivo se detectó por primera vez en el sistema, número de veces que se ha ejecutado el archivo desde que se enviaron las últimas estadísticas, información sobre el nombre, sumas de comprobación (MD5, SHA2-256, SHA1) y tamaño del cliente de correo a través del que se recibió el objeto malicioso, ID de la tarea de software que realizó el análisis, indicador de si se comprobaron la reputación del archivo y la firma o no, resultado de procesamiento del archivo, suma de comprobación (MD5) del patrón obtenido para el objeto, tamaño del patrón en bytes y especificaciones técnicas de las tecnologías de detección aplicadas;

- información sobre los objetos analizados: el grupo de confianza asignado en el que se ubicó el archivo o desde el que se ubicó; el motivo por el que el archivo se ubicó en esa categoría; el identificador de la categoría; la información sobre el origen de las categorías y la versión de la base de datos de la categoría; la marca de certificado de confianza del archivo; el nombre del proveedor del archivo; la versión del archivo; el nombre y la versión de la aplicación de software que contiene el archivo;

- información sobre las vulnerabilidades detectadas: el identificador de la vulnerabilidad en la base de datos de vulnerabilidades, la clase de riesgo de la vulnerabilidad;

- información acerca de la emulación del archivo ejecutable: el tamaño del archivo y sus sumas de comprobación (MD5, SHA2-256, SHA1); la versión del componente de la emulación, la profundidad de la emulación, el conjunto de propiedades de los bloques lógicos y las funciones situadas dentro de estos bloques que se obtuvieron durante la emulación; los datos provenientes de los encabezados de PE del archivo ejecutable;

- las direcciones IP del equipo atacante (IPv4 e IPv6), el número del puerto del equipo al que se dirige el ataque de red, el identificador del protocolo del paquete IP que contiene el ataque, el objetivo del ataque (nombre de la organización, sitio web), la marca de la reacción ante el ataque, la ponderación del ataque y el nivel de confianza;

- información sobre ataques asociados a recursos de red falsificados, y las direcciones IP (IPv4 e IPv6) y DNS de los sitios web visitados;

- direcciones IP (IPv4 o IPv6) y DNS del recurso web solicitado; la información sobre el archivo y el cliente web que accede al recurso web; información sobre el archivo y el cliente web que accede al recurso web; el nombre, el tamaño y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo, ruta completa al archivo y código de plantilla de la ruta, el resultado de la comprobación de la firma digital y su estado de conformidad con KSN;

- información sobre reversión de acciones de malware: los datos del archivo cuya actividad se ha revertido (el nombre del archivo, ruta entera al archivo, su tamaño y sumas de comprobación (MD5, SHA2-256, SHA1)), datos de acciones correctas y fallidas a eliminar, renombra y copia archivos y restaura los valores en el registro (los nombres de las claves de registro y sus valores), e información sobre los archivos del sistema modificados por el malware, antes y después de la reversión.

- información sobre las exclusiones establecidas para el componente de Control de anomalías adaptativo: la identificación y el estado de la regla que se ejecutó, la acción llevada a cabo por el Software cuando se ejecutó la regla, el tipo de cuenta de usuario con la cual el proceso o el hilo lleva a cabo una actividad sospechosa, información sobre el proceso que realizó o recibió la actividad sospechosa (identificación de la secuencia o nombre del archivo del proceso, ruta de acceso completa al archivo del proceso, código del patrón de la ruta, sumas de comprobación [MD5, SHA2-256, SHA1] del archivo del proceso); información sobre el objeto que llevó a cabo las actividades sospechosas, así como sobre el objeto que quedó sujeto a acciones sospechosas (nombre de la clave de registro o nombre del archivo, ruta completa al archivo, código del patrón de la ruta, y sumas de comprobación [MD5, SHA2-256, SHA1] del archivo);

- Información sobre los módulos de software cargados: nombre, tamaño y sumas de comprobación (MD5, SHA2-256, SHA1) del archivo del módulo, la ruta completa hacia el archivo y código de la plantilla de la ruta, configuración de la firma digital del archivo del módulo, fecha y hora de la creación de la firma, nombre del asunto y organización que firmó el archivo del módulo, ID del proceso en el cual se cargó el módulo, nombre del proveedor del módulo y número de secuencia del módulo en la cola que carga.

- información sobre la calidad de la interacción del Software con los servicios KSN: fecha y hora de comienzo y finalización del periodo en el que se generaron las estadísticas, información sobre la calidad de las solicitudes y conexión con cada uno de los servicios KSN utilizados (identificador del servicio KSN, cantidad de solicitudes exitosas, cantidad de solicitudes con respuestas del caché, cantidad de solicitudes no exitosas (problemas de red, KSN desactivado en la configuración del Software, ruta incorrecta), intervalo de tiempo de las solicitudes exitosas, intervalo de tiempo de las solicitudes canceladas, intervalo de tiempo de las solicitudes con límite de tiempo excedido, cantidad de conexiones a KSN tomadas del caché, cantidad de conexiones exitosas a KSN, cantidad de conexiones no exitosas a KSN, cantidad de transacciones exitosas, cantidad de transacciones no exitosas, intervalo de tiempo de las conexiones exitosas a KSN, intervalo de tiempo de las conexiones no exitosas a KSN, intervalo de tiempo de las transacciones exitosas, intervalo de tiempo de las transacciones no exitosas);

- si se detecta un objeto posiblemente malicioso, se debe proporcionar información sobre los datos en la memoria de los procesos: los elementos de la jerarquía de los objetos del sistema (ObjectManager), los datos de la memoria UEFI BIOS, los nombres de las claves del registro y sus valores;

- información sobre los eventos en los registros de los sistemas: la marca de tiempo del evento, el nombre del registro en el que se encontró el evento, el tipo y la categoría del evento, el nombre de la fuente del evento y su descripción;

- información sobre las conexiones de red: la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo desde el que se inició el proceso de apertura del puerto, la ruta de acceso al archivo del proceso y su firma digital, las direcciones IP locales y remotas, la cantidad de puertos de conexión local y remota, el estado de conexión, y la marca de tiempo de apertura del puerto;

- información sobre la fecha de instalación y activación del Software en el equipo: el ID del socio que vendió la licencia, el número de serie de la licencia, el encabezado firmado del ticket del servicio de activación (el ID de un centro de activación regional, el suma de control del código de activación, las suma de comprobación del ticket, la fecha de creación del ticket, el ID único del ticket, la versión del ticket, el estado de la licencia, la fecha y hora de inicio/finalización del ticket, el ID único de la licencia, la versión de la licencia), el ID del certificado utilizado para firmar el encabezado del ticket, la suma de comprobación (MD5) del archivo clave, el ID único de la instalación del software en el equipo, el tipo y el ID de la aplicación que se actualiza, el ID del tarea de actualización;

- información sobre el conjunto de todas las actualizaciones instaladas y el conjunto de las últimas actualizaciones instaladas o eliminadas, el tipo de evento que ocasionó que se enviara la información de actualización, el tiempo transcurrido desde la instalación de la última actualización, y la información sobre las bases de datos antivirus instaladas;

- información sobre el funcionamiento del software en el equipo: datos de uso de la CPU, datos de uso de memoria (Bytes Privados, grupo no paginado, grupo paginado), número de amenazas activas en el proceso de software y amenazas pendientes y el tiempo de funcionamiento del software antes del error.

- cantidad de volcados de software y volcados del sistema (BSOD) desde que se instaló el Software y a partir del momento de la última actualización, identificador y la versión del módulo del Software en la que se produjo el error, la pila de memoria del proceso del Software e información sobre las bases de datos antivirus en el momento en que se generó el error;

- datos acerca del volcado del sistema (BSOD): la marca que refleja su aparición en el equipo, el nombre del controlador que provocó el BSOD, la dirección y la pila de memoria del controlador, la marca que refleja la duración de la sesión del SO antes de que ocurriera el BSOD, la pila de memoria de los controladores que se bloquearon, el tipo de volcado de la memoria almacenada, la marca de la sesión del SO antes de que el BSOD se prolongara por más de 10 minutos, el identificador único del volcado y la marca de tiempo del BSOD;

- información sobre los errores o problemas de rendimiento que tuvieron lugar durante la operación de los componentes del Software: identificación del estado del Software, tipo de error, código y causa, así como el horario en el que ocurrió el error, identificador del componente, módulo y proceso del producto en el que tuvo lugar el error, identificador de la tarea o categoría de actualización en el que tuvo lugar el error, registros de los controladores que utiliza el Software (código de error, nombre del módulo, nombre del archivo de origen y línea en la que ocurrió el error);

- información sobre las actualizaciones de bases de datos de antivirus y componentes del Software: nombre, fecha y horario de los archivos de índice descargados durante la última actualización y en descarga en la actualización vigente;

- información sobre la terminación anormal de la operación del Software: marca de tiempo de la creación del volcado, su tipo, tipo de evento que provocó la terminación anormal del funcionamiento del Software (cierre inesperado, error en la aplicación de terceros), fecha y horario del cierre inesperado;

- información sobre la compatibilidad de los controladores del Software con el hardware y el Software: información sobre las propiedades del sistema operativo que limitan la funcionalidad de los componentes del Software (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), tipo de Software de descarga instalado (UEFI, BIOS), identificador de módulo de plataforma segura (TPM), versión de especificación de TPM, información sobre el CPU instalado en el equipo, modo operativo y parámetros de la Integridad del Código y la Protección de Dispositivos, modo de funcionamiento de los controladores y motivo para utilizar el modo actual, versión de los controladores del Software, estado de soporte de virtualización del software y del hardware del equipo;

- información acerca de las aplicaciones externas que generaron el error: su nombre, la versión y la ubicación; el código de error y la información sobre este, proveniente del registro de aplicaciones del sistema; la dirección de la aparición del error y la pila de la memoria de la aplicación externa; la marca que representa la aparición del error en el componente del Software; el período durante el cual funcionó la aplicación externa antes de que se produjera el error; las sumas de comprobación (MD5, SHA2-256, SHA1) de la imagen del proceso de la aplicación en el cual ocurrió el error; la ruta de acceso a la imagen del proceso de la aplicación y el código del patrón de la ruta de acceso; la información del registro del sistema, con una descripción del error asociado a la aplicación; la información sobre el módulo de la aplicación en la que se produjo el error (el identificador de la excepción, la ubicación del error en la memoria como un desplazamiento del módulo de la aplicación, el nombre y la versión del módulo, el identificador del error de la aplicación en el complemento del Titular de los derechos y la pila de memoria del error, y la duración de la sesión de aplicación antes de que se produjera el error);

- versión del componente de actualización del Software y la cantidad de errores que ocurrieron en este componente durante la ejecución de tareas de actualización durante su ciclo de vida, el identificador de los tipos de tareas de actualización, la cantidad de intentos fallidos que realizó el componente de actualización a fin de completar las tareas correspondientes;

- información sobre el funcionamiento de los componentes de monitoreo del sistema del Software: versiones completas de los componentes, fecha y hora en que se iniciaron los componentes, código del evento que desbordó la cola de eventos y la cantidad de dichos eventos, cantidad total de eventos de desborde de la cola, información sobre el archivo del proceso del iniciador del evento (nombre de archivo y su ruta en el equipo, código de plantilla de la ruta del archivo, sumas de comprobación (MD5, SHA2-256, SHA1) del proceso asociado con el archivo, versión del archivo), identificador de la intercepción del evento que tuvo lugar, versión completa del filtro de intercepción, identificador del tipo de evento interceptado, tamaño de la cola del evento y la cantidad de eventos entre el primer evento de la cola y el evento actual, cantidad de eventos vencidos en la cola, información sobre el archivo del proceso del iniciador del evento actual (nombre del archivo y su ruta en el equipo, código de patrón de la ruta del archivo, sumas de comprobación (MD5, SHA2-256, SHA1) del proceso asociado con el archivo), duración del procesamiento del evento, duración máxima del procesamiento del evento, probabilidad del envío de estadísticas, información sobre los eventos del sistema operativo respecto de los cuales se excedió el límite de tiempo de procesamiento (fecha y hora del evento, cantidad de inicializaciones reiteradas de las base de datos de antivirus, fecha y hora de la inicialización repetida por última vez de las base de datos de antivirus después de su actualización, tiempo de demora de procesamiento del evento para cada uno de los componentes de monitoreo del sistema, cantidad de eventos en cola, cantidad de eventos procesados, cantidad de eventos demorados del tipo actual, tiempo de demora total para los eventos del tipo actual, tiempo de demora total para todos los eventos);

- información de la herramienta de seguimiento de eventos de Windows (Event Tracing for Windows, ETW) en caso de que se presenten problemas de rendimiento con el Software, proveedores de eventos SysConfig/SysConfigEx/WinSATAssessment de Microsoft: información sobre el equipo (modelo, fabricante, factor de forma del alojamiento, versión), información sobre las métricas de rendimiento de Windows (evaluaciones WinSAT, índice de rendimiento de Windows), nombre de dominio, información sobre los procesadores físicos y lógicos (cantidad de procesadores físicos y lógicos, fabricante, modelo, nivel de revisión, cantidad de núcleos, frecuencia del reloj, CPUID, características del caché, indicadores de modos e instrucciones compatibles), información sobre los módulos RAM (tipo, factor de forma, fabricante, modelo, capacidad, granularidad de la distribución de la memoria), información sobre las interfaces de red (direcciones IP y MAC, nombre; descripción; configuración de las interfaces de red, desglose de la cantidad y del tamaño de los paquetes de red por tipo, velocidad del intercambio de la red, desglose de la cantidad de errores de red por tipo), configuración del controlador IDE, direcciones IP de los servidores DNS, información sobre la tarjeta de video (modelo, descripción, fabricante, compatibilidad, capacidad de memoria de video, permiso de la pantalla, cantidad de bits por píxel, versión BIOS), información sobre los dispositivos "enchufar y reproducir" (nombre, descripción, identificador del dispositivo [PnP, ACPI], información sobre los discos y dispositivos de almacenamiento (cantidad de discos o unidades flash, fabricante, modelo, capacidad de disco, cantidad de cilindros, cantidad de pistas por cilindro, cantidad de sectores por pista, capacidad del sector, características del caché, número secuencial, cantidad de particiones, configuración del controlador SCSI), información sobre los discos lógicos (número secuencial, capacidad de partición, capacidad de volumen, letra del volumen, tipo de partición, tipo del sistema de archivos, cantidad de clústeres, tamaño del clúster, cantidad de sectores por clúster, cantidad de clústeres vacíos y ocupados, carta de volumen reiniciable, dirección de desplazamiento de la partición en relación con el inicio del disco), información sobre la placa madre BIOS (fabricante, fecha de lanzamiento, versión), información sobre la placa madre (fabricante, modelo, tipo), información sobre la memoria física (capacidad compartida y libre), información sobre los servicios del sistema operativo (nombre, descripción, estado, etiqueta, información sobre los procesos [nombre y PID]), parámetros de consumo de energía para el equipo, configuración del controlador de interrupción, ruta a las carpetas del sistema de Windows (Windows y System32), información sobre el sistema operativo (versión, edición, fecha de lanzamiento, nombre, tipo, fecha de instalación), tamaño del archivo de página, información sobre monitores (cantidad, fabricante, permiso de pantalla, capacidad de resolución, tipo), información sobre el controlador de la tarjeta de video (fabricante, fecha de lanzamiento, versión);

- información sobre ETW, proveedores de eventos EventTrace/EventMetadata de Microsoft: información sobre la secuencia de eventos del sistema (tipo, horario, fecha, zona horaria), metadatos sobre el archivo con resultados de rastreo (nombre, estructura, parámetros de rastreo, desglose de la cantidad de operaciones de pista por tipo), información sobre el sistema operativo (nombre, tipo, versión, edición, fecha de lanzamiento, hora de inicio);

- información de ETW, proveedores de eventos de Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power de Microsoft: información sobre los procesos iniciados y completos (nombre, PID, parámetros de inicio, línea de comando, código de retorno, parámetros de administración de la energía, horario de inicio y compleción, tipo de token de acceso, SID, SessionID, cantidad de descriptores instalados), información sobre los cambios en las prioridades del hilo (TID, prioridad, horario), información sobre las operaciones de disco del proceso (tipo, horario, capacidad, cantidad), historial de cambios en la estructura y capacidad de procesos de memoria utilizable;

- información de ETW, proveedores de eventos StackWalk/Perfinfo de Microsoft; información sobre los contadores de rendimiento (rendimiento de secciones de código individual, secuencia de llamadas de función, PID, TID, direcciones y atributos de ISR y DPC);

- información de ETW, proveedor de eventos KernelTraceControl-ImageID de Microsoft: información sobre los archivos ejecutables y las bibliotecas dinámicas (nombre, tamaño de la imagen, ruta completa), información sobre archivos PDB (nombre, identificador), datos de recursos VERSIONINFO para los archivos ejecutables (nombre, descripción, creador, ubicación, versión e identificador de la aplicación, versión del archivo e identificador);

- información de ETW; proveedores de eventos Filelo/Disklo/Image/Windows Kernel Disk de Microsoft: información sobre el archivo y las operaciones del disco (tipo, capacidad, horario de inicio, horario de compleción, duración, estado de compleción, PID, TID, direcciones de llamada de la función del controlador, Paquete de Solicitud de E/S (IRP), atributos de objeto de archivo de Windows), información sobre los archivos que forman parte de operaciones de archivo y disco (nombre, versión, tamaño, ruta completa, atributos, desplazamiento, suma de comprobación de la imagen, acciones abiertas y de acceso);

- información de ETW, proveedor de eventos PageFault de Microsoft: información sobre los errores de acceso de la página de memoria (dirección, horario, capacidad, PID, TID, atributos del objeto de archivo de Windows, parámetros de distribución de la memoria);

- información de ETW, proveedor de eventos de hilo de Microsoft: información sobre la creación/compleción del hilo, información sobre hilos iniciados (PID, TID, tamaño de la pila, prioridades y asignación de recursos del CPU, recursos de E/S, páginas de memoria entre hilos, dirección de la pila, dirección de la función init, dirección del Thread Environment Block [TEB], etiqueta de servicios de Windows);

- información de ETW, proveedor de eventos Microsoft Windows Kernel Memory de Microsoft: información sobre las operaciones de administración de la memoria (estado de compleción, hora, cantidad, PID), estructura de asignación de la memoria (tipo, capacidad, SessionID, PID);

- información sobre el funcionamiento del Software en caso de problemas de rendimiento: identificador de la instalación del Software, tipo y valor de caída en el rendimiento, información sobre la secuencia de eventos en el Software (hora, zona horaria, tipo, estado de compleción, identificador del componente de Software, identificador del escenario operativo del Software, TID, PID, direcciones de llamada de funciones), información sobre las conexiones de red a verificarse (URL, dirección de la conexión, tamaño del paquete de red), información sobre los archivos PDB (nombre, identificador, tamaño de imagen del archivo ejecutable), información sobre los archivos a verificarse (nombre, ruta completa; suma de comprobación), parámetros de monitoreo del rendimiento del Software;

- información sobre el último reinicio fallido del SO: la cantidad de reinicios fallidos desde la instalación del SO, datos sobre el volcado del sistema (el código y los parámetros del error; el nombre, la versión y la suma de comprobación [CRC32] del módulo que generó el error en el funcionamiento del SO; la ubicación del error como un desplazamiento en el módulo; las sumas de comprobación [MD5, SHA2-256, SHA1] del volcado del sistema);

- información para verificar la autenticidad de los certificados digitales que se utilizan para firmar archivos: la huella digital del certificado, el algoritmo de la suma de comprobación, la clave pública y el número de serie del certificado, el nombre del emisor del certificado, el resultado de la validación del certificado y el identificador de la base de datos del certificado;

- información sobre el proceso que ejecuta el ataque a la autoprotección del software: el nombre y el tamaño del archivo del proceso, sus sumas de comprobación (MD5, SHA2-256, SHA1), la ruta completa al archivo del proceso y el código de plantilla de la ruta del archivo, las marcas de fecha de creación y compilación, indicador de archivo ejecutable, atributos del archivo de proceso, información sobre el certificado utilizado para firmar el archivo del proceso, código de la cuenta utilizada para iniciar el proceso, identificador de operaciones realizadas para acceder al proceso, tipo de recurso sobre el que se realiza la operación (proceso, archivo, objeto de registro, función de búsqueda FindWindow), nombre del recurso sobre el que se realiza la operación, indicador del éxito de la operación, estado del archivo del proceso y su firma según KSN;

- información sobre el Software del Titular de los derechos: versión completa, tipo, ubicación y estado de funcionamiento del Software utilizado, versiones de los componentes del Software instalados y su estado de funcionamiento, información sobre las actualizaciones de Software instaladas, el valor del filtro TARGET, la versión del protocolo utilizado para conectarse a los servicios del Titular de los derechos;

- información sobre el hardware instalado en el equipo: el tipo, el nombre, el nombre del modelo, la versión del firmware, los parámetros de los dispositivos integrados y conectados, el identificador único del Equipo con el Software instalado;

- información sobre las versiones del sistema operativo y las actualizaciones instaladas, el tamaño de las palabras, la edición y los parámetros del modo de ejecución del SO, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del SO, fecha y horario de inicio del SO;
- archivos ejecutables y no ejecutables, total o parcialmente;
- porciones de la RAM del equipo;
- sectores involucrados en el proceso de arranque del sistema operativo;
- paquetes de datos de tráfico de red;
- páginas web y correos electrónicos que contienen objetos sospechosos y maliciosos;
- descripción de las clases e instancias de clases del repositorio WMI;
- informes de actividad de la aplicación:
  - el nombre, tamaño y versión del archivo que se envía, su descripción y sumas de comprobación (MD5, SHA2-256, SHA1), identificador de formato de archivo, el nombre del proveedor del archivo, el nombre del producto al que pertenece el archivo, ruta completa al archivo en el equipo, código de plantilla de la ruta, la creación y modificación de las marcas de tiempo del archivo;
  - fecha/hora de inicio y finalización del período de validez del certificado (si el archivo tiene una firma digital), la fecha y la hora de la firma, el nombre del emisor del certificado, información sobre el titular del certificado, la huella dactilar, la clave pública del certificado y los algoritmos correspondientes y el número de serie del certificado;
  - el nombre de la cuenta desde la que se ejecuta el proceso;
  - sumas de comprobación (MD5, SHA2-256, SHA1) del nombre del equipo en la que se ejecuta el proceso;
  - títulos de las ventanas de proceso;
  - Identificador de las bases de datos antivirus, nombre de la amenaza detectada según la clasificación del Titular de los derechos;
  - datos sobre la licencia instalada, su identificador, tipo y fecha de caducidad;
  - hora local del equipo en el momento de la provisión de información;
  - nombres y rutas de los archivos a los que accedió el proceso;
  - nombres de claves de registro y sus valores a los que accedió el proceso;
  - Direcciones URL e IP a las que accedió el proceso;
  - Direcciones URL e IP desde las que se descargó el archivo en ejecución.

Provisión de datos al usar soluciones de Detection and Response

En equipos con Kaspersky Endpoint Security instalado, los datos preparados para el envío automático a los servidores de Kaspersky Endpoint Detection and Response, Kaspersky Sandbox y Kaspersky Anti Targeted Attack Platform se almacenan. Los archivos se almacenan en los equipos de forma simple, no encriptada.

El conjunto específico de datos depende de la solución en la que se utilice Kaspersky Endpoint Security.

Kaspersky Endpoint Detection and Response

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

Datos recibidos como resultado la ejecución de la tarea Análisis de IOC (tarea estándar)

Kaspersky Endpoint Security envía automáticamente datos sobre los resultados de la ejecución de la tarea *Análisis de IOC* a Kaspersky Security Center.

Los datos de los resultados de la ejecución de la tarea *Análisis de IOC* pueden contener la siguiente información:

- Dirección IP de la tabla ARP
- Dirección física de la tabla ARP
- Tipo y nombre del registro de DNS
- Dirección IP del equipo protegido
- Dirección física (dirección MAC) del equipo protegido
- Identificador en la entrada del registro de eventos
- Nombre del origen de los datos del registro
- Nombre de registro
- Hora del evento
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo (ruta incluida)
- Tamaño del archivo
- Dirección IP remota y puerto al que se estableció la conexión durante el análisis
- Dirección IP del adaptador local
- Puerto abierto en el adaptador local
- Protocolo como un número (de acuerdo con el estándar IANA)
- Nombre del proceso
- Argumentos del proceso

- Ruta al archivo de proceso
- Identificador de Windows (PID) del proceso
- Identificador de Windows (PID) del proceso principal
- Cuenta de usuario que inició el proceso
- Fecha y hora en que se inició el proceso
- Nombre del servicio
- Descripción del servicio
- Ruta y nombre del servicio DLL (para svchost)
- Ruta y nombre del archivo ejecutable del servicio
- Identificador de Windows (PID) del servicio
- Tipo de servicio (por ejemplo, un controlador o adaptador de kernel)
- Estado del servicio
- Modo de lanzamiento del servicio
- Nombre de la cuenta de usuario.
- Nombre del volumen
- Letra del volumen
- Tipo de volumen
- Valor del registro de Windows
- Valor de colmena de registro
- Ruta de la clave de registro (sin nombre de colmena ni de valor)
- Configuración del registro
- Sistema (entorno)
- Nombre y versión del sistema operativo instalado en el equipo
- Nombre de red del equipo protegido
- Dominio o grupo al que pertenece el equipo protegido
- Nombre del navegador
- Versión del navegador
- Hora en que se accedió por última vez al recurso web

- URL de la solicitud HTTP
- Nombre de la cuenta utilizada para la solicitud HTTP
- Nombre de archivo del proceso que realizó la solicitud HTTP
- Ruta completa al archivo del proceso que realizó la solicitud HTTP
- Identificador de Windows (PID) del proceso que realizó la solicitud HTTP
- Referencia HTTP (URL de origen de la solicitud HTTP)
- URI del recurso solicitado a través de HTTP
- Información sobre el agente de usuario HTTP (la aplicación que realizó la solicitud HTTP)
- Tiempo de ejecución de la solicitud HTTP
- Identificador único del proceso que realizó la consulta de HTTP

Datos para crear una cadena de desarrollo de la amenaza

De forma predeterminada, los datos para crear una cadena de desarrollo de la amenaza se almacenan durante siete días. Los datos se envían automáticamente a Kaspersky Security Center.

Los datos para crear una cadena de desarrollo de la amenaza pueden contener la siguiente información:

- Fecha y hora del incidente
- Nombre de detección
- Modo de análisis
- Estado de la última acción relacionada con la detección
- Motivo por el que falló el procesamiento de la detección
- Tipo de objeto detectado
- Nombre del objeto detectado
- Estado de amenaza después de que se procese el objeto
- Razón por la que falló la ejecución de acciones en el objeto
- Acciones realizadas para revertir acciones maliciosas
- Información sobre el objeto procesado:
  - Identificador único del proceso
  - Identificador único del proceso principal

- Identificador único del archivo de proceso
- Identificador de proceso de Windows (PID)
- Línea de comando del proceso
- Cuenta de usuario que inició el proceso
- Código de la sesión de inicio de sesión en la que se está ejecutando el proceso
- Tipo de sesión en la que se está ejecutando el proceso
- Nivel de integridad del proceso que se está procesando
- Membresía de la cuenta de usuario que inició el proceso en los grupos locales y de dominio con privilegios
- Identificador del objeto procesado
- Nombre completo del objeto procesado
- Identificador del dispositivo protegido
- Nombre completo del objeto (nombre de archivo local o dirección web del archivo descargado)
- Hash MD5 o SHA256 del objeto procesado
- Tipo de objeto procesado
- Fecha de creación del objeto procesado
- Fecha en que se modificó por última vez el objeto procesado
- Tamaño del objeto procesado
- Atributos del objeto procesado
- Organización que firmó el objeto procesado
- Resultado de la verificación del certificado digital del objeto procesado
- Identificador de seguridad (SID) del objeto procesado
- Identificador de zona horaria del objeto procesado
- Dirección web de la descarga del objeto procesado (solo para archivos en disco)
- Nombre de la aplicación que descargó el archivo
- Hashes MD5 y SHA256 de la aplicación que descargó el archivo
- Nombre de la aplicación que modificó por última vez el archivo
- Hashes MD5 y SHA256 de la aplicación que modificó por última vez el archivo
- Número de inicios de objetos procesados

- Fecha y hora en que se inició por primera vez el objeto
- Identificadores únicos del archivo
- Nombre completo del archivo (nombre del archivo local o dirección web del archivo descargado)
- Ruta a la variable del registro de Windows procesada
- Nombre de la variable del registro de Windows procesada
- Valor de la variable del registro de Windows procesada
- Tipo de la variable del registro de Windows procesada
- Indicador de la membresía de la clave de registro procesada en el punto de ejecución automática
- Dirección web de la solicitud web procesada
- Origen del enlace de la solicitud web procesada
- Agente de usuario de la solicitud web procesada
- Tipo de solicitud web procesada (`GET` o `POST`)
- Puerto IP local de la solicitud web procesada
- Puerto IP remoto de la solicitud web procesada
- Dirección de conexión (entrante o saliente) de la solicitud web procesada
- Identificador del proceso en el que se incrustó el código malicioso

Kaspersky Sandbox

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

Datos de servicio

Kaspersky Endpoint Security almacena los siguientes datos procesados durante la respuesta automática:

- Archivos procesados y datos ingresados por el usuario durante la configuración del agente integrado de Kaspersky Endpoint Security:
  - Archivos en Cuarentena
  - Clave pública del certificado utilizado para la integración con Kaspersky Sandbox

- Caché del agente integrado de Kaspersky Endpoint Security:
  - Hora en que los resultados del análisis se escribieron en la memoria caché
  - Hash MD5 de la tarea de análisis
  - Identificador de tarea de análisis
  - Resultado del análisis del objeto
- Cola de solicitudes de análisis de objetos:
  - ID del objeto en la cola
  - Hora en que el objeto se colocó en la cola
  - Estado de procesamiento del objeto en la cola
  - ID de la sesión de usuario en el sistema operativo donde se creó la tarea de análisis de objetos
  - Identificador del sistema (SID) del usuario del sistema operativo cuya cuenta se utilizó para crear la tarea
  - Hash MD5 de la tarea de análisis de objetos
- Información sobre las tareas para las que el agente integrado de Kaspersky Endpoint Security espera los resultados del análisis de Kaspersky Sandbox:
  - Hora en que se recibió la tarea de análisis de objetos
  - Estado de procesamiento del objeto
  - ID de la sesión de usuario en el sistema operativo donde se creó la tarea de análisis de objetos
  - Identificador de la tarea de análisis de objetos
  - Hash MD5 de la tarea de análisis de objetos
  - Identificador del sistema (SID) del usuario del sistema operativo cuya cuenta se utilizó para crear la tarea
  - Esquema XML de la IOC creada automáticamente
  - Hash MD5 o SHA256 del objeto analizado
  - Errores de procesamiento
  - Nombres de los objetos para los que se creó la tarea
  - Resultado del análisis del objeto

Datos en solicitudes a Kaspersky Sandbox

Los siguientes datos de las solicitudes del agente integrado de Kaspersky Endpoint Security a Kaspersky Sandbox se almacenan localmente en el equipo:

- Hash MD5 de la tarea de análisis
- Identificador de tarea de análisis
- Objeto analizado y todos los archivos relacionados

Datos recibidos como resultado de la ejecución de la tarea Análisis de IOC (tarea independiente)

Kaspersky Endpoint Security envía automáticamente datos sobre los resultados de la ejecución de la tarea *Análisis de IOC* a Kaspersky Security Center.

Los datos de los resultados de la ejecución de la tarea *Análisis de IOC* pueden contener la siguiente información:

- Dirección IP de la tabla ARP
- Dirección física de la tabla ARP
- Tipo y nombre del registro de DNS
- Dirección IP del equipo protegido
- Dirección física (dirección MAC) del equipo protegido
- Identificador en la entrada del registro de eventos
- Nombre del origen de los datos del registro
- Nombre de registro
- Hora del evento
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo (ruta incluida)
- Tamaño del archivo
- Dirección IP remota y puerto al que se estableció la conexión durante el análisis
- Dirección IP del adaptador local
- Puerto abierto en el adaptador local
- Protocolo como un número (de acuerdo con el estándar IANA)

- Nombre del proceso
- Argumentos del proceso
- Ruta al archivo de proceso
- Identificador de Windows (PID) del proceso
- Identificador de Windows (PID) del proceso principal
- Cuenta de usuario que inició el proceso
- Fecha y hora en que se inició el proceso
- Nombre del servicio
- Descripción del servicio
- Ruta y nombre del servicio DLL (para svchost)
- Ruta y nombre del archivo ejecutable del servicio
- Identificador de Windows (PID) del servicio
- Tipo de servicio (por ejemplo, un controlador o adaptador de kernel)
- Estado del servicio
- Modo de lanzamiento del servicio
- Nombre de la cuenta de usuario.
- Nombre del volumen
- Letra del volumen
- Tipo de volumen
- Valor del registro de Windows
- Valor de colmena de registro
- Ruta de la clave de registro (sin nombre de colmena ni de valor)
- Configuración del registro
- Sistema (entorno)
- Nombre y versión del sistema operativo instalado en el equipo
- Nombre de red del equipo protegido
- Dominio o grupo al que pertenece el equipo protegido
- Nombre del navegador

- Versión del navegador
- Hora en que se accedió por última vez al recurso web
- URL de la solicitud HTTP
- Nombre de la cuenta utilizada para la solicitud HTTP
- Nombre de archivo del proceso que realizó la solicitud HTTP
- Ruta completa al archivo del proceso que realizó la solicitud HTTP
- Identificador de Windows (PID) del proceso que realizó la solicitud HTTP
- Referencia HTTP (URL de origen de la solicitud HTTP)
- URI del recurso solicitado a través de HTTP
- Información sobre el agente de usuario HTTP (la aplicación que realizó la solicitud HTTP)
- Tiempo de ejecución de la solicitud HTTP
- Identificador único del proceso que realizó la consulta de HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

Datos de servicio

El agente integrado de Kaspersky Endpoint Security almacena los siguientes datos localmente:

- Datos necesarios para la integración con el componente EDR Expert (on-premises):
  - Dirección y puerto para conectarse al servidor de KATA Central Node
  - Dirección y puerto para conectarse al servidor de transmisión de telemetría
  - Dirección y puerto para conectarse al servidor de respuesta
  - Información sobre los certificados utilizados para la integración con KATA Central Node
  - Información sobre los certificados utilizados para la integración con el servidor de transmisión de telemetría
  - Información sobre los certificados utilizados para la integración con el servidor de respuesta
- Archivos en Cuarentena

Datos de eventos de telemetría transmitidos

- **Datos de telemetría**
  - Datos en archivos:
    - Identificadores únicos del archivo
    - Tipo de archivo
    - Ruta completa del archivo
    - Tamaño del archivo
    - Atributos de archivo
    - Identificador de zona
    - Fecha y hora en que se creó el archivo
    - Fecha y hora en que se modificó el archivo por última vez
    - Nombre del archivo original
    - Nombre de aplicación
    - Versión de la aplicación.
    - Proveedor de aplicaciones
    - Descripción del archivo
    - Versión del archivo.
    - Hashes MD5 y SHA256 del objeto
    - Resultado de la verificación de la firma del archivo
    - Nombre del emisor del certificado
    - Nombre del titular del certificado
    - Número de serie del certificado
  - Datos sobre el análisis de AMSI:
    - Identificador único del proceso que inició la actividad
    - Tipo de contenido del objeto transmitido a AMSI
    - Contenido del objeto transmitido a AMSI

- Nombre del objeto
- Hashes MD5 y SHA256 del objeto

- Datos sobre el bloqueo de la aplicación:
  - Identificador único del proceso que inició el bloqueo de la aplicación
  - Identificador único del proceso principal
  - Identificador de sistema único del proceso
  - Comando utilizado para iniciar un proceso
  - ID de sesión de inicio de sesión
  - Nivel de integridad del proceso
  - Estado del proceso
  - Identificador único del archivo de proceso
  - Línea de comando del proceso
  - Lista de identificadores únicos de archivos interpretados
- Datos sobre aperturas de archivos bloqueadas:
  - Identificador único del proceso que inició la apertura del archivo
  - Identificadores únicos del archivo
- Datos sobre la carga del controlador:
  - Identificador único del controlador cargado
- Datos sobre eventos:
  - Identificador único del evento
  - Fecha y hora del evento
- Datos sobre la modificación de archivos:
  - Identificador único del proceso que inició la modificación del archivos
  - Identificadores únicos del archivo
  - Tipo de operación de modificación
  - Indicador que informa de que el archivo se eliminará después de reiniciar el equipo
  - Identificador único del archivo de modificado
  - Identificador único del archivo antes de la modificación

    - Conjunto de indicadores de bits que determinan cómo se abrió el archivo
    - Datos sobre las operaciones en la lista de control de acceso
    - Datos sobre cambios en la propiedad o el grupo principal del archivo
- Datos sobre sesión de inicio de sesión:
    - ID de sesión de inicio de sesión
    - Nombre del usuario que inició sesión
    - Tipo de cuenta de usuario
    - Tipo de sesión
- Datos sobre las conexiones de red:
    - Identificador único del proceso que inició la conexión
    - Dirección IP local utilizada para iniciar la conexión
    - Dirección IP remota del punto final de la conexión
    - Dirección de conexión
    - Protocolo de transferencia de datos
    - Método HTTP
    - Ruta sin el nombre de host
    - Nombre de host
    - Estado del proceso dinámico en el momento de la conexión
    - Indicador que informa de que la conexión está abierta en el nivel de socket sin formato
    - Versión de TLS utilizada en la sesión de conexión
    - Nombre del servidor TLS
    - Hash MD5 y SHA1 del certificado del servidor TLS
    - Lista de nombres alternativos del sujeto (SAN) del certificado
    - Nombre del emisor del certificado TLS
    - Número de serie del certificado
    - Algoritmo de cifrado utilizado
    - Fechas de inicio y finalización del certificado

    - Huella JA3 del cliente TLS
    - Huella JA3S del servidor
- Datos capturados mientras se escucha en un puerto de red:
    - Identificador único del proceso que inició la conexión
- Datos de entrada de la línea de comandos:
    - Identificador único del proceso que inició la entrada en la consola
    - Tipo de entrada de consola
    - Texto introducido por un usuario o un proceso
- Datos sobre la creación del proceso:
    - Identificador único del proceso
    - Identificador único del proceso principal
    - Identificador de sistema único del proceso
    - Comando utilizado para iniciar un proceso
    - ID de sesión de inicio de sesión
    - Nivel de integridad del proceso
    - Identificador único del archivo de proceso
    - Lista de identificadores únicos de archivos interpretados
    - Tipo de proceso
- Datos sobre el módulo cargado por el proceso:
    - Identificador único del proceso que inició la descarga
    - Ruta completa al archivo que se cargó en el proceso
    - Identificador único del archivo de módulo
    - Nombre completo del ensamblado .NET, si el archivo cargado es un módulo .NET
    - Indicadores del ensamblado .NET definido en su manifiesto
- Datos sobre la terminación del proceso:
    - Identificador único del proceso terminado

- Datos sobre la modificación del registro:
  - Identificador único del proceso que inició la modificación del registro
  - Tipo de operación de registro
  - Ruta completa a la clave de registro
  - Nombre del valor dentro de una clave de registro
  - Tipo de datos almacenados en el valor de la clave de registro
  - Datos especificados en el valor de la clave de registro
  - Nombre de la clave antes de cambiar el nombre
  - Información sobre un cambio en la propiedad de la clave o grupo de claves principales
  - Lista de cambios en la lista de control de acceso (ACL) de la clave
- Datos sobre la amenaza detectada y su procesamiento:
  - Bandera que indica que la detección de amenazas se ejecutó en segundo plano
  - Veredicto de amenaza
  - Nombre del veredicto
  - Identificador único del registro de la base de datos
  - Hora a la que se guardó el registro de amenaza en la base de datos
  - Estado de procesamiento de la amenaza
  - Tipo de objeto infectado
  - Nombre del objeto infectado
  - Hashes MD5 y SHA256 del objeto
  - Identificador único del objeto infectado
  - Identificador único del proceso que descargó el objeto infectado de Internet
  - URL desde la que se descargó el objeto infectado
  - Dirección de correo electrónico del remitente que envió el objeto infectado
  - Protocolo de red a través del cual se recibió el objeto infectado
  - Dirección local desde la que se recibió el objeto infectado
  - Dirección externa desde la que se recibió el objeto infectado

- Tipo de contenido del objeto
- Contenido del objeto

- Datos sobre el acceso a los procesos:
  - Identificador único del proceso que intentó el acceso
  - Identificador único del proceso de destino al que se accedió
  - Conjunto de derechos solicitados del proceso de destino
  - Tipo de operación
  - Conjunto de llamadas en el momento de acceder a un proceso
  - Descriptor del proceso de origen
  - Descriptor del proceso de destino
- Datos sobre DNS:
  - Identificador único del proceso que inició la consulta de DNS
  - Dirección IP del servidor DNS
  - Indicadores que administran el comportamiento de una consulta de DNS
  - Estado de finalización de la solicitud
  - Nombre de dominio totalmente cualificado especificado en la consulta de DNS
  - Tipo de datos en la consulta de DNS
  - Respuestas del servidor DNS
- Datos sobre la inyección de código:
  - Identificador único del proceso que intentó inyectar el código
  - Método de acceso utilizado
  - Conjunto de llamadas en el momento en que se detectó el código inyectado
  - Identificador único del proceso de destino en el que se cargó el código
  - Datos sobre cambios en la secuencia de comandos del proceso de destino
  - Dirección del proceso de destino
  - Nombre de la biblioteca DLL que se cargó en el proceso de destino
  - Ruta completa al archivo de DDL

- Datos sobre operaciones con canales con nombre:
  - Identificador único del proceso que creó o se conectó al canal
  - Nombre completo del canal nombrado
  - Tipo de operación (creación o conexión)
- Datos sobre consultas WMI:
  - Identificador único del proceso que inició la operación de WMI
  - Tipo de operación de WMI
  - Nombre del dispositivo de destino para la consulta WMI
  - Cuenta de usuario que inició la consulta WMI
  - Texto de la consulta WMI
  - Espacio de nombres en el que se realiza la consulta WMI
  - Nombre del filtro WMI
  - Nombre del objeto consumidor
  - Texto que describe la acción del objeto consumidor
- Datos sobre consultas LDAP:
  - Identificador único del proceso que realizó la consulta de LDAP
  - Cobertura de búsqueda de consultas LDAP
  - Filtro LDAP
  - Parámetro que especifica la partición de Active Directory a la que se dirigió la consulta
  - Atributos de la búsqueda de LDAP
- Datos sobre dispositivos USB conectados:
  - Tipo de operación del dispositivo USB
  - Tipo de dispositivo USB
  - Identificador del dispositivo USB
  - Nombre del dispositivo USB
  - Ruta al dispositivo USB
  - Indicador que informa de que el dispositivo USB es una unidad del sistema
- Datos sobre la creación, eliminación y modificación de una tarea programada

- Datos sobre creación, eliminación y modificación de servicios
- Datos sobre el montaje/desmontaje del sistema de archivos
- Datos sobre el funcionamiento del componente local de EDR Expert:
  - Información sobre el inicio/detención del agente
  - Información sobre la instalación/desinstalación del agente
  - Identificador único para el inicio del agente
  - Identificador del sistema del proceso del agente
  - Identificador único del proceso del agente
  - Motivo de la terminación del agente
  - Código de terminación del proceso del agente

- Configuración de filtrado de eventos:
  - Nombres de módulos
  - Rutas completas a objetos
  - Hashes MD5 y SHA256 de los objetos
  - Identificadores de las entradas en el registro de eventos de Windows
  - Configuración de certificados digitales
  - Dirección del tráfico, direcciones IP, puertos, protocolos, rutas íntegras a archivos ejecutables
  - Nombres de usuario
  - Tipos de inicio de sesión de usuario
  - Tipos de eventos de telemetría para los que se aplican filtros

Datos de las solicitudes del componente EDR Expert al agente integrado de Kaspersky Endpoint Security

- Configuración general de tareas:
  - Tipo de tarea
  - Configuración de la programación de las tareas
  - Nombres y contraseñas de las cuentas en las que se pueden ejecutar las tareas
  - Versiones de configuración

- Identificadores de objetos en Cuarentena
- Rutas a los objetos
- Hashes MD5 y SHA256 de los objetos
- Línea de comando para iniciar el proceso con los argumentos
- Indicadores de las acciones adicionales realizadas al finalizar las tareas
- Identificadores de archivos de IOC que se recuperarán del servidor
- Archivos IOC
- Nombre del servicio
- Tipo de inicio de servicio
- Carpetas para las que se deben recibir los resultados de la tarea *Obtener datos forenses*
- Máscaras de los nombres de objetos y extensiones de la tarea *Obtener datos forenses*

- Configuración del aislamiento de red:
  - Tipos de configuraciones
  - Versiones de configuración
  - Listas de exclusiones del aislamiento de red y configuración de la exclusión: dirección del tráfico, direcciones IP, puertos, protocolos y rutas completas a archivos ejecutables
  - Indicadores de las acciones adicionales
  - Tiempo de desactivación del aislamiento automático
- Configuración de prevención de ejecución:
  - Tipos de configuraciones
  - Versiones de configuración
  - Listas de reglas de prevención de ejecución y configuración de reglas: rutas a objetos, tipos de objetos, hashes MD5 y SHA256 de objetos
  - Indicadores de las acciones adicionales

Datos de solicitudes enviadas por Kaspersky Endpoint Security al componente EDR Expert

Cuando se integran con la solución EDR Expert (on-premises), los siguientes datos se almacenan localmente en los equipos:

- En solicitudes de sincronización:
  - ID exclusivo
  - Parte básica de la dirección web del servidor
  - Nombre del equipo
  - Dirección IP del equipo
  - Dirección MAC del equipo
  - Hora local en el equipo
  - Estado de autoprotección de Kaspersky Endpoint Security
  - Nombre y versión del sistema operativo instalado en el equipo
  - Versión de Kaspersky Endpoint Security
  - Versiones de la configuración de la aplicación y la configuración de la tarea
  - Estados de tareas: identificadores de tareas, estados de ejecución, códigos de error
- En las solicitudes de obtención de archivos del servidor:
  - Identificadores únicos de archivos
  - Identificador único de Kaspersky Endpoint Security
  - Identificadores únicos de certificados
  - Parte básica de la dirección web del servidor con el componente Central Node instalado
  - Dirección IP del host
- En los informes de resultados de ejecución de tareas:
  - Dirección IP del host
  - Información sobre los objetos detectados durante un análisis de IOC o un análisis de YARA
  - Indicadores de las acciones adicionales realizadas al finalizar las tareas
  - Errores de ejecución de tareas y códigos de retorno
  - Estados de finalización de las tareas

- Hora de finalización de las tareas
- Versiones de la configuración utilizada para la ejecución de las tareas
- Información sobre los objetos enviados al servidor, objetos en Cuarentena y objetos restaurados de la Cuarentena: rutas a objetos, hashes MD5 y SHA256, identificadores de objetos en Cuarentena
- Información sobre los procesos iniciados o detenidos en un equipo a solicitud del servidor: PID y UniquePID, código de error, hashes MD5 y SHA256 de los objetos
- Información sobre los servicios iniciados o detenidos en el equipo a solicitud del servidor: nombre del servicio, tipo de inicio, código de error, hashes MD5 y SHA256 de las imágenes de archivo de los servicios
- Información sobre los objetos para los que se realizó un volcado de memoria para un análisis de YARA (rutas, identificador de archivo de volcado)
- Archivos solicitados por el servidor

- Datos sobre procesos en ejecución:
  - Nombre del archivo ejecutable, incluida la ruta completa y la extensión
  - Parámetros de ejecución automática del proceso
  - ID del proceso
  - ID de sesión de inicio de sesión
  - Nombre de la sesión de inicio de sesión
  - Fecha y hora en que se inició el proceso
  - Hashes MD5 y SHA256 del objeto
- Datos en archivos:
  - Ruta del archivo
  - Nombre del archivo.
  - Tamaño del archivo
  - Atributos de archivo
  - Fecha y hora en que se creó el archivo
  - Fecha y hora en que se modificó el archivo por última vez
  - Descripción del archivo
  - Nombre de la empresa
  - Hashes MD5 y SHA256 del objeto
  - Clave de registro (para puntos de ejecución automática)

- Datos en errores que se producen cuando se recuperó información sobre objetos:
  - Nombre completo del objeto que se procesó cuando ocurrió un error
  - Código de error
- Datos en los resultados del análisis de YARA:

  El agente integrado de Kaspersky Endpoint Security transfiere automáticamente los resultados del análisis de YARA a Kaspersky Anti Targeted Attack Platform para crear una cadena de desarrollo de la amenaza.

  Los datos se almacenan temporalmente de forma local en la cola para enviar los resultados de la ejecución de la tarea al servidor de Kaspersky Anti Targeted Attack Platform. Los datos se eliminan del almacenamiento temporal una vez que se han enviado.
  - Hashes MD5 y SHA256 del archivo
  - Nombre completo del archivo
  - Ruta del archivo
  - Tamaño del archivo
  - Nombre del proceso
  - Argumentos del proceso
  - Ruta al archivo de proceso
  - Identificador de Windows (PID) del proceso
  - Identificador de Windows (PID) del proceso principal
  - Cuenta de usuario que inició el proceso
  - Fecha y hora en que se inició el proceso
- Datos en los resultados del análisis de IOC:
  - Dirección IP de la tabla ARP
  - Dirección física de la tabla ARP
  - Nombre de registro de DNS
  - Tipo de registro de DNS
  - Nombre de host
  - Dirección IP
  - Id. de evento en el registro
  - Nombre del origen de los datos del registro
  - Nombre de registro

- Nombres de usuario
- Fecha y hora en que se generó el evento, en formato ISO
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo
- Tamaño del archivo
- Dirección IP remota y puerto al que se estableció la conexión durante el análisis
- Dirección IP y puerto del adaptador local
- Protocolo
- Nombre del proceso
- Argumentos del proceso
- Ruta al archivo de proceso
- Identificador de Windows (PID) del proceso
- Identificador de Windows (PID) del proceso principal
- Cuenta de usuario que inició el proceso
- Fecha y hora en que se inició el proceso
- Ruta a la clave de registro
- Nombre de la clave de registro.
- Valor de texto de la clave de registro
- Nombre del servicio
- Descripción del servicio
- Ruta y nombre del servicio DLL
- Ruta y nombre del archivo ejecutable del servicio
- Identificador de Windows (PID) del servicio
- Tipo de servicio
- Estado del servicio
- Modo de lanzamiento del servicio
- Nombre del sistema operativo
- Versión del sistema operativo

- Nombre de la red informática sin dominio
- Dominio o grupo de trabajo
- Nombres de usuario
- Nombre del volumen
- Letra del volumen
- Tipo de volumen

Kaspersky Network Detection and Response (KATA)

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

Datos de telemetría

- **Datos sobre archivos**
  - Identificadores únicos del archivo
  - Tipo de archivo
  - Ruta completa del archivo
  - Tamaño del archivo
  - Atributos de archivo
  - Identificador de zona
  - Fecha y hora en que se creó el archivo
  - Fecha y hora en que se modificó el archivo por última vez
  - Nombre del archivo original
  - Nombre de aplicación
  - Versión de la aplicación.
  - Proveedor de aplicaciones
  - Descripción del archivo
  - Versión del archivo.

- Hashes MD5 y SHA256 del objeto
- Resultado de la verificación de la firma del archivo
- Fecha y hora en que se creó la firma del archivo
- Cadenas de certificados usadas en el archivo de firma
- Tipo de cadena de certificados
- Certificados en la cadena
- Nombre del emisor del certificado
- Nombre del titular del certificado
- Número de serie del certificado
- Algoritmo de impresión digital del certificado
- Impresión digital del certificado
- Periodo de validez del certificado

- **Datos sobre sesión de inicio de sesión**
  - ID de sesión de inicio de sesión
  - Nombre de cuenta del usuario que inició sesión
  - Tipo de cuenta de usuario
  - Tipo de sesión
  - Dirección IP del equipo desde el que se intentó iniciar sesión
  - Dirección IP del equipo local para el que se realizó el intento de inicio de sesión
  - Indicador de que la sesión representada por este evento tiene privilegios elevados y derechos administrativos
  - Parámetro que indica si otras sesiones están vinculadas a esta sesión de inicio de sesión
  - Protocolo usado para la sesión del terminal
  - Protocolo IPv4 usado para la sesión de terminal
- **Datos sobre comunicación de red**
  - Inicio y finalización del intervalo de tiempo durante el cual se reunieron los datos
  - Lista de conexiones
  - Dirección IP local del equipo

- Dirección MAC local del equipo
- Dirección IP remota del equipo
- Dirección MAC remota del equipo
- Dirección IP del gateway
- Número de paquetes de datos transmitidos
- Número de paquetes de datos recibidos
- Número total de bytes transferidos
- Protocolo de transferencia de datos
- Campo EtherType de trama Ethernet
- Prefijo de carga útil del primer paquete del intervalo
- Dirección IPv4 de la interfaz de red a través de la cual se capturó la comunicación

- **Datos sobre la conexión de red**
  - Identificador único del proceso que inició la conexión
  - Protocolo de transferencia de datos
  - Dirección IP local utilizada para iniciar la conexión
  - Dirección IP remota del punto final de la conexión
  - Método HTTP
  - Ruta sin el nombre de host
  - Nombre de host
  - Estado del proceso dinámico en el momento de la conexión
  - Dirección de conexión
  - Estado del proceso dinámico
  - Campo EtherType de trama Ethernet
- **Datos capturados mientras se escucha en un puerto de red**
  - Identificador único del proceso que inició la conexión
  - Protocolo de transferencia de datos
  - Dirección local
  - Estado del proceso dinámico en el momento de la conexión

- **Resultado de la verificación de la conexión**
  - Configuración de red del host
  - Descripción de la interfaz de red
  - Nombre de dominio de DNS
  - Dirección MAC local del equipo
  - Número de métrica de conexión IP
  - Lista de direcciones IP
  - Dirección IP
  - Máscara de red
  - Dirección IP del gateway
  - Dirección MAC del gateway
  - Lista de parches instalados
  - Número de parche
  - Fecha de instalación del parche
  - Modelo de dispositivo
  - Proveedor del dispositivo
  - ID de host en Kaspersky Security Center
  - Descripción del antivirus Kaspersky instalado
  - Nombre del componente del antivirus Kaspersky instalado
  - Versión del componente del antivirus Kaspersky instalado
  - Versión de la base de datos del componente antivirus de Kaspersky instalado
  - Fecha de la última actualización de la base de datos del componente antivirus de Kaspersky instalado
  - Estado del componente del antivirus Kaspersky instalado
  - Lista de claves de licencia
  - Número de serie de la clave
  - Tipo de clave

- Fecha de caducidad de la clave
- Estado de la clave

- **Datos sobre la creación de procesos en el host**
  - Identificador único del proceso
  - Identificador único del proceso principal
  - Identificador de sistema único del proceso
  - Comando utilizado para iniciar un proceso
  - ID de sesión de inicio de sesión
  - ID de sesión terminal
  - Identificador único del archivo de proceso
  - Nivel de integridad del proceso
  - Lista de tokens de derechos del proceso
  - Derechos del atributo
  - Lista de identificadores únicos de archivos interpretados
  - Estado del proceso
  - Comando utilizado para iniciar un proceso
- **Datos sobre la terminación del proceso**
  - Identificador único del proceso
- **Datos sobre amenaza detectada**
  - Información sobre la amenaza
  - Veredicto de amenaza
  - Número de registro de AMR
  - Versión de la base de datos antivirus
  - Modo de detección de amenazas
  - Identificador único de la amenaza
  - Tecnología de protección
  - Información sobre el objeto infectado
  - Tipo de objeto infectado

- Nombre del objeto infectado
- Hashes MD5 y SHA256 del objeto
- Identificador único del proceso infectado
- Identificador único del objeto infectado
- Identificador único del proceso que descargó el objeto infectado de Internet
- URL desde la que se descargó el objeto infectado
- Dirección de correo electrónico del remitente que envió el objeto infectado
- Protocolo de red a través del cual se recibió el objeto infectado
- Dirección local desde la que se recibió el objeto infectado
- Dirección externa desde la que se recibió el objeto infectado
- Tipo de contenido del objeto
- Contexto de la amenaza detectada
- Contenido del objeto
- Bandera que indica que la detección de amenazas se ejecutó en segundo plano

- **Datos sobre el procesamiento de amenazas**
  - Información sobre la amenaza
  - Veredicto de amenaza
  - Número de registro de AMR
  - Versión de la base de datos antivirus
  - Modo de detección de amenazas
  - Nombre del objeto infectado
  - Hashes MD5 y SHA256 del objeto
  - Identificador único del proceso infectado
  - Identificador único del objeto infectado
  - Protocolo de red a través del cual se recibió el objeto infectado
  - Dirección local desde la que se recibió el objeto infectado
  - Dirección externa desde la que se recibió el objeto infectado
  - Estado de procesamiento de la amenaza

- Razón por la que no se pudo remediar la amenaza
- Dirección física local

- **Datos sobre usuarios**
  - SID de usuario
  - ID de usuario
  - Nombres de usuario
  - Nombre completo del usuario
  - Descripción del usuario
  - Si la cuenta está activa o bloqueada
  - Si la contraseña ha caducado
  - Si se requiere un cambio de contraseña
  - Si se permite el cambio de contraseña
  - Tipo de cuenta de usuario
  - Si esta cuenta tiene activado el inicio de sesión automático
  - Lista de grupos a los que pertenece el usuario

Integración con Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

Al integrarse con Kaspersky Unified Monitoring and Analysis Platform (KUMA), se transfieren los datos de configuración de la conexión, así como todos los eventos registrados en los registros de Windows.

Los principales registros de eventos de Windows son Sistema, Seguridad, Aplicación, Eventos reenviados y Eventos de hardware. Los usuarios también pueden crear registros personalizados y trabajar con ellos para cumplir con sus requisitos específicos.

Cumplimiento de la legislación de la Unión Europea (GDPR)

Kaspersky Endpoint Security puede transmitir datos a Kaspersky en los siguientes escenarios:

- Uso de Kaspersky Security Network.
- Activar la aplicación con un código de activación.

- Actualización de módulos de aplicaciones y bases de datos antivirus.
- Al seguir enlaces en la interfaz de la aplicación.

Independientemente de la clasificación de datos y el territorio desde el que se reciben los datos, Kaspersky se adhiere a altos estándares de seguridad de datos y emplea diversas medidas legales, organizativas y técnicas para proteger los datos de los usuarios, para garantizar la seguridad y confidencialidad de los datos y, también, para garantizar la cumplimiento de los derechos de los usuarios garantizados por la legislación aplicable. El texto de la Política de privacidad se incluye en el kit de distribución de la aplicación y está disponible en el sitio web de Kaspersky.

Antes de utilizar Kaspersky Endpoint Security, lea atentamente la descripción de los datos transmitidos en el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network. Si los datos específicos transmitidos desde Kaspersky Endpoint Security en cualquiera de los escenarios descritos pueden clasificarse como datos personales de acuerdo con su legislación o estándar local, debe asegurarse de que dichos datos se procesen legalmente y obtener el consentimiento de los usuarios finales para la recopilación y transmisión de tales datos.

Puede leer el Contrato de licencia de usuario final y visitar el sitio web de Kaspersky para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn_<ID de idioma>.txt con el texto del Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network se incluyen en el kit de distribución de la aplicación.

Si no desea transmitir datos a Kaspersky, puede desactivar la provisión de datos.

Usar Kaspersky Security Network

Al utilizar Kaspersky Security Network, acepta proporcionar automáticamente los datos enumerados en la Declaración de Kaspersky Security Network. Si no acepta proporcionar estos datos a Kaspersky, utilice Kaspersky Private Security Network (KPSN) o desactive el uso de KSN. Para más información sobre KPSN, consulte la documentación de Kaspersky Private Security Network.

Activar la aplicación con un código de activación

Al utilizar un código de activación, acepta proporcionar automáticamente los datos enumerados en el Contrato de licencia de usuario final. Si no acepta proporcionar estos datos a Kaspersky, utilice un archivo clave para activar Kaspersky Endpoint Security.

Actualización de módulos de aplicaciones y bases de datos antivirus

Al utilizar los servidores de Kaspersky, acepta proporcionar automáticamente los datos enumerados en el Contrato de licencia de usuario final. Kaspersky requiere esta información para verificar que Kaspersky Endpoint Security se esté utilizando legítimamente. Si no acepta proporcionar esta información a Kaspersky, utilice Kaspersky Security Center para actualizaciones de la base de datos o Kaspersky Update Utility.

Al seguir enlaces en la interfaz de la aplicación

Al utilizar enlaces en la interfaz de la aplicación, acepta proporcionar automáticamente los datos enumerados en el Contrato de licencia de usuario final. La lista precisa de datos transmitidos en cada enlace específico depende de dónde se encuentra el enlace en la interfaz de la aplicación y del problema que pretende resolver. Si no acepta proporcionar estos datos a Kaspersky, utilice la interfaz simplificada de la aplicación u oculte la interfaz de la aplicación.

Escritura de volcado

Si ha activado la escritura de volcado, Kaspersky Endpoint Security creará un archivo de volcado que contendrá todos los datos de la memoria de los procesos de la aplicación al momento en que se creó este archivo de volcado.

Información de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Adobe, Acrobat, Flash, Reader y Shockwave son marcas registradas o marcas comerciales de Adobe en los Estados Unidos y/o en otros países.

Amazon, Amazon Web Services y AWS son marcas comerciales de Amazon.com, Inc. o sus empresas afiliadas.

Apple, FireWire, iTunes, Mac y Safari son marcas comerciales de Apple Inc.

Arm es una marca registrada de Arm Limited (o sus subsidiarias) en los EE. UU. o en otros lugares.

AutoCAD es una marca comercial o marca registrada de Autodesk, Inc. y/o de sus filiales y/o empresas afiliadas en los Estados Unidos y/o en otros países.

La palabra, marca y logotipos Bluetooth son propiedad de Bluetooth SIG, Inc.

Borland es una marca comercial o una marca registrada de Borland Software Corporation.

Cisco y Cisco AnyConnect, IOS son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. o sus empresas afiliadas en Estados Unidos y otros países.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop y XenServer son marcas comerciales registradas o marcas comerciales de Cloud Software Group, Inc. o sus filiales en los Estados Unidos o en otros países.

Cloudflare, Cloudflare Workers y el logotipo de Cloudflare son marcas comerciales y/o marcas comerciales registradas de Cloudflare, Inc. en los Estados Unidos y otras jurisdicciones.

Core es la marca comercial de Intel Corporation o sus filiales.

dBase es una marca de dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC y otras marcas comerciales son marcas comerciales de Dell Inc. o sus subsidiarias.

Docker y el logotipo de Docker son marcas comerciales y/o marcas comerciales registradas de Docker, Inc. en los Estados Unidos o en otros países. Docker, Inc. y otras partes también pueden tener derechos de marca comercial sobre otros términos utilizados en este documento.

ESET es una marca comercial o marca comercial registrada de ESET spol. s r.o. o la respectiva entidad de ESET.

Foxit es una marca registrada de Foxit Corporation.

Radmin es una marca registrada de Famatech.

Google, Android, Google Public DNS, Google Chrome y Chrome son marcas comerciales de Google, LLC.

HUAWEI, FusionCompute y FusionSphere son marcas comerciales de Huawei Technologies Co., Ltd.

ICQ es una marca registrada o marca de servicio de ICQ LLC.

Intel es la marca comercial de Intel Corporation o sus filiales.

IBM es una marca comercial de International Business Machines Corporation registrada en numerosas jurisdicciones de todo el mundo.

Lenovo y Lenovo ThinkPad son marcas comerciales de Lenovo en los Estados Unidos y/o en otros países.

Linux es la marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca registrada o marca comercial de Logitech en los Estados Unidos y/o en otros países.

LogMeIn Pro y Remotely Anywhere son marcas comerciales de LogMeIn, Inc.

Mail.ru es una marca comercial de Mail.ru LLC.

McAfee es la marca comercial o marca comercial registrada de McAfee LLC o sus empresas afiliadas en EE. UU. o en otros países.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server y Windows Store son marcas comerciales del grupo de empresas de Microsoft.

Mozilla, Firefox y Thunderbird son marcas comerciales de Mozilla Foundation en EE. UU. y otros países.

NetApp es una marca comercial o la marca comercial registrada de NetApp, Inc. en los Estados Unidos u otros países.

OpenSSL es una marca comercial propiedad de OpenSSL Software Foundation.

OpenStack es una marca comercial registrada de OpenStack Foundation en los Estados Unidos y otros países.

Oracle, Java y JavaScript son marcas registradas de Oracle y/o de sus filiales.

Python es una marca comercial o marca comercial registrada de Python Software Foundation.

Realtek es una marca comercial de Realtek Semiconductor Corporation.

SAMSUNG es una marca comercial de SAMSUNG en los Estados Unidos o otros países.

Thawte es una marca comercial o una marca comercial registrada de Symantec Corporation o sus empresas afiliadas en los Estados Unidos y otros países.

Trend Micro es una marca comercial o una marca comercial registrada de Trend Micro Incorporated.

VERISIGN es una marca registrada en los Estados Unidos y en otros países o una marca comercial no registrada de VeriSign, Inc. y sus subsidiarias.

VMware, VMware ESXi, Vmware Horizon, VMware Workstation, Vmware Tools y Vmware vSphere son marcas registradas y/o marcas comerciales de VMware, Inc. en los Estados Unidos y en otras jurisdicciones.

Información sobre el código de terceros

La información sobre el código de terceros se incluye en el archivo legal_notices.txt, en la carpeta de instalación de la aplicación.