kaspersky

Kaspersky Endpoint Security 14.1 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 la aplicación: Estándar, EDR Agent, Light Agent
- Kit de distribución
- Requisitos de hardware y software
- Comparación de las características disponibles de 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 mediante Kaspersky Security Center
  - Instalación estándar de la aplicación
  - Creación de un paquete de instalación
  - Actualización de las bases de datos incluidas en el paquete de instalación
  - Creación de una tarea de instalación remota
- Instalación local a través del Asistente
- Instalación remota de la aplicación con System Center Configuration Manager
- Descripción de la configuración de instalación del archivo setup.ini
- Cambiar componentes de la aplicación
- Actualización de una versión más antigua de la aplicación
  - Actualización de la aplicación sin reiniciar el equipo
  - Actualización SMU de la aplicación
- Eliminar la aplicación

Licencia de la aplicación
- Acerca del Contrato de licencia de usuario final
- Acerca de la licencia
- Acerca del certificado de licencia
- Acerca de la suscripción
- Acerca de la clave de licencia
- Acerca del código de activación
- Acerca del archivo de 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 la información de la licencia
- Adquisición de una licencia
- Renovación de una suscripción

Primeros pasos
- Acerca del Complemento de administración para 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 aplicación
Icono de la aplicación en el área de notificación de la barra de tareas
Interfaz de la aplicación simplificada
Configuración de la visualización de la interfaz de la aplicación
Preparar la aplicación para su uso
Administración de directivas
Creación de una directiva
Exportar e importar una directiva
Indicador del nivel de seguridad
Administración de tareas
Configuración local de la aplicación
Iniciar y detener Kaspersky Endpoint Security
Suspensión y reanudación de la protección y control del equipo
Crear y utilizar un archivo de configuración
Restauración de la configuración predeterminada de la aplicación
Rendimiento de Kaspersky Endpoint Security y su compatibilidad con otras aplicaciones
Activación o desactivación del modo de ahorro de energía
Activación o desactivación de la dispensación de recursos para otras aplicaciones
Prácticas recomendadas para optimizar el rendimiento de Kaspersky Endpoint Security
Análisis de malware
Análisis del equipo
Análisis de unidades extraíbles cuando se conectan al equipo
Análisis en segundo plano
Análisis desde el menú contextual
Comprobación de integridad de la aplicación
Editar el alcance del análisis
Ejecutar un análisis programado
Ejecutar un análisis como un usuario diferente
Optimización de análisis
Actualización de bases de datos y módulos de software de la aplicación
Modalidades de actualización para las bases de datos y los módulos
Actualización con un repositorio de servidor
Actualización con una carpeta compartida
Actualización con Kaspersky Update Utility
Actualización en modo móvil
Inicio y detención de una tarea de actualización
Inicio de una tarea de actualización según los derechos 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
Protección contra archivos peligrosos
Habilitación y deshabilitación de la Protección contra archivos peligrosos
Suspensión automática de la Protección contra amenazas de archivos
Cambio de la acción tomada respecto de archivos infectados por el componente Protección contra amenazas de archivos
Formación del alcance de la protección del componente Protección contra archivos peligrosos
Uso de métodos de análisis
Utilización de tecnologías de análisis en la operación del componente Protección contra amenazas de archivos
Optimización del análisis de archivos
Análisis de archivos compuestos
Modificación del modo de análisis
Análisis de contenedores
Prevención de intrusiones en el host
Habilitación y deshabilitación de la Prevención de intrusiones en el host
Administración de grupos de confianza de aplicaciones
Modificación del grupo de confianza de una aplicación
Configuración de los derechos disponibles en los grupos de confianza
Selección de un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security
Selección del grupo de confianza para aplicaciones desconocidas
Selección del grupo de confianza para aplicaciones con firma digital
Administración de los derechos de las aplicaciones
Protección de recursos del sistema operativo y datos personales
Eliminación de la información sobre las aplicaciones en desuso
Monitoreo de Prevención de intrusiones en el host
Protección del acceso a dispositivos de audio y video
Prevención de ataques BadUSB
Habilitación y deshabilitación de Prevención de ataques BadUSB
Usar el Teclado en pantalla para la autorización de dispositivos USB
Autorización del lector de códigos de barras
Protección vía AMSI
Habilitación y deshabilitación de la Protección vía AMSI
Optimización del análisis de archivos mediante la Protección vía AMSI
Protección contra amenazas web
Habilitación y deshabilitación de la Protección contra amenazas web
Configuración de métodos de detección de direcciones web maliciosas
Anti-Phishing
Creación de la lista de direcciones web de confianza
Exportar e importar la lista de direcciones web de confianza
Protección contra amenazas de correo
Habilitación y deshabilitación de la Protección contra amenazas de correo
Modificación de la acción que se llevará a cabo en mensajes de correo electrónico infectados
Formación del alcance de protección del componente Protección contra amenazas de correo
Análisis de archivos compuestos adjuntos a mensajes de correo electrónico
Filtrado de datos adjuntos de mensajes de correo electrónico
Exportar e importar extensiones para filtrado de datos adjuntos
Análisis de correo electrónico en Microsoft Office Outlook
Análisis de correos electrónicos en Thunderbird, MyOffice y R7-Office

Protección contra amenazas de red
Habilitación y deshabilitación de la Protección contra amenazas de red
Bloquear un equipo atacante
Configuración de direcciones de exclusiones del bloqueo
Exportar e importar la lista de exclusiones de bloqueo
Configurar Protección contra amenazas de red por tipo
Firewall
Habilitación o deshabilitación del Firewall
Cambio del tipo de la conexión de red
Administración de reglas de paquetes de red
Creación de una regla de paquetes de red
Habilitación o deshabilitación de una regla de paquetes de red
Cambio de la acción del Firewall para una regla de paquetes de red
Cambio de la prioridad de una regla de paquetes de red
Exportar e importar reglas de paquetes de red
Definir las reglas de paquetes de red en XML
Administración de reglas de red para aplicaciones
Creación de una regla de red para una aplicación
Activación y desactivación de una regla de red para aplicaciones
Cambio de la acción del Firewall para una regla de red para aplicaciones
Cambio de la prioridad de una regla de red para aplicaciones
Monitor de red
Prevención de exploits
Habilitación y deshabilitación de la Prevención de exploits
Protección de la memoria de procesos del sistema
Detección de comportamiento
Anticifrador
Habilitación y deshabilitación de la protección de carpetas compartidas contra el cifrado externo
Configuración del período de bloqueo de un equipo no confiable
Editar el alcance de la protección
Agregar equipos de confianza para el cifrado de datos externo
Exportar e importar una lista de exclusiones de la protección de carpetas compartidas contra el cifrado externo
Motor de reparación
Kaspersky Security Network
Habilitación y deshabilitación del uso de Kaspersky Security Network
Limitaciones de Kaspersky Private Security Network
Habilitación y deshabilitación del modo nube para los componentes de protección
Configuración del proxy de KSN
Comprobación de la reputación de un archivo en Kaspersky Security Network
Análisis de conexiones cifradas
Cómo habilitar el análisis de conexiones cifradas
Instalación de certificados raíz de confianza
Análisis de conexiones cifradas con un certificado no confiable
Cómo agregar el certificado de Kaspersky a un almacén de certificados propio
Creación de exclusiones para el análisis de conexiones cifradas
Eliminación de datos

Control del equipo
Control Web
Agregar una regla de acceso a recursos web
Filtrar por direcciones de recursos web
Filtrar por contenido de recursos web
Prueba de las reglas de acceso a recursos web
Exportar e importar 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 del 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
Acerca de las reglas de acceso
Administrar el acceso a dispositivos según su tipo
Administrar el acceso a los dispositivos mediante el bus de conexión
Diferentes derechos de acceso de usuarios a los dispositivos
Administrar el acceso a los dispositivos móviles
Administrar el acceso a los dispositivos Bluetooth
Control de impresión
Control de conexiones Wi-Fi
Supervisar el uso de unidades extraíbles
Cambiar la duración del almacenamiento en caché
Acciones con dispositivos de confianza
Agregar un dispositivo a la lista De confianza desde la interfaz de la aplicación
Añadir un dispositivo a la lista De confianza desde Kaspersky Security Center
Exportar e importar 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 del Control de dispositivos
Anti-Bridging
Habilitar Anti-Bridging
Edición del estado de una regla de conexiones
Cambio de prioridad de una regla de conexión
Control de anomalías adaptativo
Aprendizaje del Control de anomalías adaptativo
Habilitación y deshabilitación 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 para una regla del Control de anomalías adaptativo
Exportar e importar exclusiones para 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 la funcionalidad del Control de aplicaciones
Recepción de información sobre las aplicaciones que se instalan en equipos de usuarios
Cómo habilitar el modo de aplicaciones bloqueadas
Control de aplicaciones basado en un equipo de referencia
Administración de las reglas de Control de aplicaciones
Adición de una condición de activación para la regla de Control de aplicaciones
Agregar archivos ejecutables de la carpeta Archivos ejecutables a la categoría de la aplicación
Adición de archivos ejecutables relacionados con eventos a la categoría de la aplicación
Agregar una regla de control de aplicaciones
Cambio del estado de una regla de Control de aplicaciones mediante Kaspersky Security Center
Exportar e importar Reglas de control de aplicaciones
Visualización de eventos resultantes de la operación del componente Control de aplicaciones
Acceso al informe sobre las aplicaciones bloqueadas
Prueba de las reglas de Control de aplicaciones
Habilitación y deshabilitación de la prueba de reglas de Control de aplicaciones
Acceso al informe sobre las aplicaciones bloqueadas en el modo de prueba
Visualización de eventos resultantes de la operación de prueba del componente Control de aplicaciones
Monitor de actividades de aplicaciones
Reglas para crear máscaras de nombres para archivos o carpetas
Edición de las plantillas de mensajes de Control de aplicaciones
Variables en las plantillas de mensajes de Control de aplicaciones
Prácticas recomendadas para implementar una lista de aplicaciones permitidas
Configuración del modo de lista de autorización para aplicaciones
Prueba del modo de lista de admitidos
Compatibilidad del modo de lista de admitidos
Supervisión de puertos de red
Habilitación de la supervisión 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 supervisarán todos los puertos de red
Exportar e importar listas de puertos supervisados
Inspección de registros
Configuración de reglas predefinidas
Agregar reglas personalizadas
Control de integridad del sistema
Acerca de las reglas de Control de integridad del sistema
Control de integridad del sistema en tiempo real
Comprobación de integridad del sistema a pedido
Exportación e importación de las reglas de Control de integridad del sistema
Visualización de los informes de Control de integridad del sistema
Restablecimiento del estado de integridad del sistema
Cloud Discovery
Zona de confianza
Cómo crear una exclusión de análisis
Crear una exclusión por tipo de objeto detectado
Modificación de la lista de aplicaciones de confianza
Crear una zona de confianza local

Exportar e importar la zona de confianza
Administrar aplicaciones con una firma digital de confianza
Apéndice. Exclusiones de análisis y aplicaciones de confianza predefinidas
Servidor SQL
Servidor Microsoft Exchange
System Center Configuration Manager
Citrix
VMware
Administración del Depósito de copias de seguridad
Configuración del período de almacenamiento máximo de los archivos en Copias de seguridad
Configuración del tamaño máximo de Copias de seguridad
Restauración de archivos desde copias de seguridad
Eliminar copias de seguridad de archivos de Copias de seguridad
Servicio de notificación
Configuración de los parámetros del registro de eventos
Configuración de la visualización y el envío de notificaciones
Configuración de la visualización de advertencias acerca del estado de la aplicación en el área de notificación
Comunicación entre el administrador y los usuarios
Administración de informes
Cómo acceder a los informes
Configuración de la duración máxima del almacenamiento de informes
Configuración del tamaño máximo del archivo del informe
Almacenamiento de informes en archivos
Borrado de informes
Autoprotección de Kaspersky Endpoint Security
Habilitar y deshabilitar el componente Autoprotección
Habilitar y deshabilitar la compatibilidad con AM-PPL
Protección de los servicios de aplicación contra la administración externa
Compatibilidad con aplicaciones de administración remota
Protección con contraseña
Habilitar la protección con contraseña
Asignación de permisos a usuarios o grupos individuales
Uso de 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 la conexión del Servidor de administración
Cifrado de datos
Limitaciones de la función de 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
Cómo iniciar el 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
Habilitación de la tecnología de inicio de sesión único (SSO)
Administración de cuentas del Agente de autenticación

Uso de un token y de una tarjeta inteligente con el Agente de autenticación
Descifrado de discos duros
Restaurar el acceso a una unidad protegida con la tecnología Cifrado de disco de Kaspersky
Inicio de sesión con la cuenta del servicio del Agente de autenticación
Actualización del sistema operativo
Eliminación de errores de actualización de la funcionalidad de cifrado
Seguimiento del Agente de autenticación
Edición de los textos de ayuda del Agente de autenticación
Eliminación de objetos y datos residuales tras evaluar el funcionamiento del Agente de autenticación
Administración de BitLocker
Activación del Cifrado de unidad BitLocker
Cómo descifrar un disco duro protegido con BitLocker
Restaurar el acceso a una unidad protegida con BitLocker
Suspensión de la protección de BitLocker para actualizar el software
Cifrado de archivos en discos de equipos locales.
Cifrado de archivos en discos locales del equipo.
Formación de reglas de acceso a archivos cifrados para aplicaciones
Cifrado de archivos que son creados o modificados por aplicaciones específicas
Generación de una regla de descifrado
Descifrado de archivos en unidades de disco locales del equipo
Creación de paquetes cifrados
Procedimiento para recuperar el acceso a archivos cifrados
Restauración del acceso a datos cifrados después de una falla del sistema operativo
Modificación de plantillas de mensajes de acceso a archivos cifrados
Cifrado de unidades extraíbles
Inicio del cifrado de unidades extraíbles
Agregar una regla de cifrado para unidades extraíbles
Exportar e importar una lista de reglas de cifrado para unidades extraíbles
Modo portátil para acceder a unidades extraíbles con archivos cifrados
Descifrado de unidades extraíbles
Visualización de detalles del cifrado de datos
Visualización del estado de cifrado
Cómo ver las estadísticas de cifrado en los paneles de Kaspersky Security Center
Visualización de errores de cifrado en unidades de disco locales del equipo
Visualización del informe de cifrado de datos
Trabajar con dispositivos cifrados cuando no tenemos acceso a ellos
Recuperación de datos con la Utilidad de restauración FDERT
Creación de un disco de rescate del sistema operativo
Soluciones 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)
Instalar EDR Agent
Integrar EDR Agent con MDR

- Integrar KATA Agent con EDR (EDR)
- Integrar KATA Agent con NDR (EDR)
- Integración del EDR Agent con EDR Expert (on-premises)
- Compatibilidad con aplicaciones de EPP de terceros

Managed Detection and Response
- Integración del agente incorporado con MDR
- Guía de migración de KEA a KES para MDR

Endpoint Detection and Response
- Integración del agente incorporado con EDR Optimum/EDR Expert
- Analizar en busca de indicadores de compromiso (tarea estándar)
- Telemetría extendida de Análisis de IOC
- Mover el archivo a cuarentena
- Obtener archivo
- Eliminar archivo
- Inicio de proceso
- Terminar proceso
- Prevención de la ejecución
- Aislamiento de la red del equipo
- Cloud Sandbox
- Guía de migración de KEA a KES para EDR Optimum

Kaspersky Sandbox
- Integración del agente incorporado 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 incorporado 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 archivos excluidas
  - Ejemplo 4. Modificaciones de registros excluidas
- KATA Sandbox
  - Integración del agente incorporado 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 incorporado con EDR Expert (on-premises)
- Configuración de telemetría de EDR Expert (on-premises)
- Exclusiones de telemetría EDR Expert (on-premises)
- Exportar e importar filtros de eventos de EDR Expert (on-premises)
- Consideraciones especiales al usar perfiles de directiva para configurar la integración con EDR Expert (on-premises) y EDR (KATA)

Solo Endpoint Detection and Response Expert (cloud)
- Integración del agente incorporado con EDR Expert (cloud)
- Configuración de telemetría de EDR Expert (cloud)

Exclusiones de telemetría EDR Expert (cloud)
Exportar e importar filtros de eventos de EDR Expert (cloud)
Gestión de la cuarentena
Configurar el tamaño máximo de cuarentena
Envío de datos acerca de los archivos en cuarentena a Kaspersky Security Center
Restauración de archivos en Cuarentena
Supervisión de acciones de EDR
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Integración de Kaspersky Endpoint Security con KUMA
Filtrar eventos para enviar a KUMA
Exportar e importar filtros de eventos de KUMA
Guía de migración de KSWS a KES
Correspondencia de los componentes de KSWS y KES
Correspondencia de las configuraciones 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]
Asegúrese de que Kaspersky Security for Windows Server se haya eliminado con éxito
Activar KES con una clave de KSWS
Consideraciones especiales para migrar servidores de alta carga
Cómo administrar la aplicación desde un servidor en modo Server Core
Migrar de [KSWS+KEA] a [KES+agente incorporado]
Modo de Light Agent para proteger máquinas virtuales
Consideraciones especiales para el modo de 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
Instalar Light Agent
Conectar Light Agent a SVM
Detección de SVM
Configurar el algoritmo de selección de SVM para Light Agent
Distribuir las conexiones de los Light Agents a las SVM (etiquetas)
Proteger la conexión entre un Light Agent y una SVM
Activar Light Agent
Guía de migración de KSVLA Light Agent a KES Light Agent
Instalar KES Light Agent en lugar de KSVLA Light Agent
Correspondencia de los componentes de KSVLA Light Agent y KES Light Agent
Migrar 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. Recuperar la aplicación

Comando de AVP
SCAN. Análisis de malware
UPDATE. Actualización de bases de datos y módulos de software de la aplicación
ROLLBACK. Reversión de la última actualización
TRACES. Seguimiento
START. Iniciar un perfil
STOP. Detener un perfil
STATUS. Estado del perfil
STATISTICS. Estadísticas sobre el funcionamiento de los perfiles
RESTORE. Restauración de archivos desde copias de seguridad
EXPORT. Exportar ajustes de la aplicación
IMPORT. Importar ajustes de la aplicación
ADDKEY. Aplicar un archivo de clave.
LICENSE. Administración de licencias
RENEW. Adquisición de una licencia
PBATESTRESET. Restablecer los resultados de la comprobación del disco antes de cifrarlo
EXIT. Salir de la aplicación
EXITPOLICY. Deshabilitar una directiva
STARTPOLICY. Habilitar una directiva
DISABLE. Deshabilitar la protección
SPYWARE. Detección de spyware
KSN. Cambiar entre KSN/KPSN
SERVERBINDINGDISABLE. Deshabilitar la protección de la conexión con el servidor.
Comando de KESCLI
Scan. Análisis de malware
GetScanState. Estado de la finalización del análisis
GetLastScanTime. Determinación de la hora de finalización del análisis
GetThreats. Obtención de datos sobre las amenazas detectadas
UpdateDefinitions. Actualización de bases de datos y módulos de software de la aplicación
GetDefinitionState. Determinación de la fecha y hora de la última actualización de las bases de datos
EnableRTP. Habilitación de la protección
GetRealTimeProtectionState. Estado de la Protección contra archivos peligrosos
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. Administrar la prevención de la ejecución
ISOLATION. Administrar el aislamiento de la red
RESTORE. Restauración de archivos en Cuarentena
IOCSCAN. Analizar en busca de indicadores de compromiso (IOC)
MDRLICENSE. Activación de MDR
EDRKATA. Integración con EDR (KATA)
KUMA. Integración con KUMA
YARA. Ejecución de YARA Scan
TELEMETRYFILTERS. Filtrar eventos para enviar a KUMA

Comandos de administración de Light Agent
KSVLAINFO. Determinación del modo de Light Agent
VIISINFO. Estado de la conexión del Light Agent con el Servidor de integración
SVMINFO. Estado de la conexión del Light Agent con el Servidor de protección
Códigos de error
Apéndice. Perfiles de la aplicación
Uso de la API REST para administrar la aplicación
Habilitar el uso de la API REST al instalar la aplicación
Uso de la API
Fuentes de información acerca de la aplicación
Contacto con Soporte técnico
Contenidos y almacenamiento de los archivos de rastreo
Seguimiento de la operación de aplicaciones
Seguimiento del rendimiento de aplicaciones
Creación de archivos de volcado
Protección de los archivos de volcado y de seguimiento
Obtención de datos del sistema operativo (Kaspersky Get System Info)
Limitaciones y advertencias
Glosario
Administrador de archivos portátiles
Agente de autenticación
Agente de red
Alcance de la protección
Alcance del análisis
Archivo de almacenamiento
Archivo de IOC
Archivo infectable
Archivo infectado
Autenticación Kerberos
Base de datos de direcciones web fraudulentas
Base de datos de direcciones web malintencionadas
Bases de datos de antivirus
Certificado de licencia
Clave activa
Cloud Discovery
Desinfección
Emisor de 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 contra archivos peligrosos
Protección contra amenazas web
Protección contra amenazas de correo
Protección contra amenazas de red
Firewall
Prevención de ataques BadUSB
Protección vía AMSI
Prevención de exploits
Detección de comportamiento
Prevención de intrusiones en el host
Motor de reparación
Kaspersky Security Network
Inspección de registros
Anticifrador
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 con KUMA
Cifrado de disco completo
Cifrado de archivos
Cifrado de unidades extraíbles
Plantillas (cifrado de datos)
Exclusiones
Configuración de la aplicación
Informes y repositorios
Configuración de red
Interfaz
Administrar configuración
Actualización de bases de datos y módulos de software 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 filtro de adjuntos de Protección contra amenazas de correo
Apéndice 5. Configuración de red para la interacción con servicios externos

Apéndice 6. Eventos de la aplicación
Crítico
Error funcional
Advertencia
Mensaje informativo
Apéndice 7. Extensiones de archivo compatibles para la Prevención de ejecución
Apéndice 8. Intérpretes de scripts compatibles para la prevención de ejecución
Apéndice 9. Alcance del análisis de IOC en el registro (RegistryItem)
Apéndice 10. Requisitos de archivos de IOC
Apéndice 11. API para respuesta a amenazas de EDR
Apéndice 12. Cuentas de usuario en las reglas del componente de la aplicación
Información legal
Suministro de datos
Suministro de datos estipulado en el Contrato de licencia de usuario final
Provisión de datos al utilizar Kaspersky Security Network
Provisión de datos al utilizar las 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 (RGPD)
Avisos de marca registrada
Información acerca de código de terceros

Ayuda de Kaspersky Endpoint Security para Windows

Novedades

Actualización 14.1

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

1. Se agregó compatibilidad con el sistema operativo Windows Server 2025.

2. Se incrementó el límite en el 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). Kaspersky Endpoint Security admite ahora hasta 10 000 reglas de filtrado, tanto inclusivas como exclusivas, en total.

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

4. Para la tarea *Análisis de malware*, ahora puede especificar un intervalo de tiempo durante el cual la tarea se pondrá en pausa, por ejemplo, para minimizar el impacto en el rendimiento del equipo durante períodos de mayor carga.

5. Se optimizó el rendimiento del subsistema de disco duro en el equipo protegido 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 para Windows 14.0 tiene las siguientes características y mejoras:

1. Los equipos basados en Arm ahora son compatibles. 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 hay nuevos eventos de telemetría disponibles para los usuarios de Kaspersky Endpoint Detection and Response. Estos nuevos eventos mejoran las capacidades de detección de amenazas de 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, PF24011.

Actualización 12.12

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

1. La protección de carpetas compartidas contra el cifrado externo que solía incluirse en el componente Detección de comportamiento ahora es un componente independiente: Anticifrador.

2. Ahora se admite el protocolo Kerberos para autenticar la aplicación a través de un servidor proxy con acceso a Internet.

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

4. Ahora los usuarios cuentan con más características de la tarea *Análisis de IOC* en las soluciones de Endpoint Detection and Response (EDR). La funcionalidad Análisis retrospectivo de IOC ya está disponible. En el modo *Análisis retrospectivo de IOC* de la tarea *Análisis de IOC*, Kaspersky Endpoint Security analiza los indicadores de vulneración mediante el uso de datos durante un período determinado. Este modo está diseñado para detectar indicadores de vulneración en los datos de la actividad de red del equipo. Kaspersky Endpoint Security analiza los datos de los registros del sistema operativo y del navegador del equipo.

5. Los usuarios de Kaspersky Endpoint Detection and Response (EDR) pueden quitar el límite al tamaño de Cuarentena. Es posible que esto sea necesario para completar el análisis YARA porque la aplicación podría guardar un archivo de volcado de memoria de gran tamaño. Ahora puede usar todo el espacio libre en el disco para Cuarentena.

6. Se admite la compresión HTTPS para optimizar la exportación de eventos a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Esto permite 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, PF24011.

Actualización 12.11

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

1. La aplicación revisa la configuración de los componentes de control antes de guardar los ajustes. La revisión se implementó para los componentes Control de aplicaciones, Control de dispositivos y Control de integridad del sistema. Ahora, la aplicación muestra una advertencia si la configuración actual del componente de control podría aumentar la carga en la computadora o causar fallas en el sistema. Por ejemplo, en el caso del Control de aplicaciones, si seleccionó el modo que bloquea todas las aplicaciones excepto las permitidas y no agregó nunca regla de permisos, la aplicación muestra una advertencia porque una configuración así podría causar fallas en el sistema.

2. Se agregó la compatibilidad para la carga de archivos automática 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 los objetos en servidores especiales con imágenes virtuales implementadas de los sistemas operativos Microsoft Windows (servidores de Sandbox). Para que KATA Sandbox funcione en modo automático, se debe implementar Kaspersky Anti Targeted Attack Platform 8.0.

3. Envíos de telemetría de EDR optimizados. Ahora puede especificar el largo máximo del paquete.

4. Diagnósticos de conexión a Kaspersky Security Network mejorados. Detalles de errores de conexión ampliados para que Kaspersky Security Network resuelva posibles errores.

5. Ahora se puede configurar el envío de listas de eventos a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Además de las listas de eventos predefinidas en KUMA, ahora puede agregar eventos a la telemetría o excluir eventos según su Id. en el registro de eventos de Windows.

6. Se actualizó la interfaz de la directiva en Web Console. La disposición de las secciones de la directiva se cambió para poder acceder más rápido a las funciones esenciales.

7. Compatibilidad con 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, PF22014.

Actualización 12.10

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

1. En el caso del componente Prevención de ataques BadUSB, se agregó la opción para autorizar lectores de códigos de barras mediante la lectura de un código de barras desde la pantalla. Ahora no es necesario ingresar el código con el teclado en pantalla para autorizar lectores 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 agregar 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 mejoró 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.

   - Se mejoró la respuesta ante la detección de IOC. Ahora puede poner en cuarentena los archivos que se detectaron mediante la tarea de *Análisis de IOC* directamente desde 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 las listas de hashes de archivos, direcciones IP o nombres DNS generados en un archivo TXT.

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

3. Se agregó un nuevo permiso de protección con contraseña: *Exportar configuración*. De forma predeterminada, solo el usuario KLAdmin puede crear un archivo de configuración que contenga los ajustes de Kaspersky Endpoint Security desde la interfaz de la aplicación. Para conceder 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 agregó la nueva funcionalidad para *administrar contraseñas temporales*. La contraseña temporal le permite proporcionar acceso a Kaspersky Endpoint Security con la protección con contraseña habilitada para un equipo diferente. Administración de contraseñas temporales permite guardar el historial de contraseñas (hasta 30 días), controlar el estado de la contraseña temporal (*Activo*, *Caducada*, *Revocado*) y revocar contraseñas temporales.

2. Se agregó la opción para terminar la conexión a los recursos web prohibidos por las reglas de Control web inmediatamente después de que se aplique la directiva. En versiones anteriores de la aplicación, Control web restringía solo las conexiones nuevas a los recursos web prohibidos.

3. Para los usuarios de Kaspersky Anti Targeted Attack Platform, se agregó una opción para ejecutar la comprobación YARA localmente en el equipo. Para hacerlo, debe descargar un archivo con reglas YARA y ejecutar el comando en CMD.

4. Se corrigió el comportamiento de la aplicación cuando BitLocker está habilitado en equipos en los que las unidades ya se protegen con BitLocker y 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 una nueva sección llamada **Historial de respuestas**, disponible para los usuarios de las soluciones Detection and Response de Kaspersky. Esta sección contiene información sobre las acciones de respuesta ante amenazas que se realizan en la computadora. Por ejemplo, estas acciones incluyen ejecutar la tarea *Finalizar proceso* o aislar el equipo de la red. La sección Historial de respuestas solo está disponible para los usuarios de las siguientes soluciones de Kaspersky: MDR, EDR, KATA.

6. Para los usuarios de Kaspersky Unified Monitoring and Analysis Platform, ya está disponible la compatibilidad con las acciones de respuesta ante amenazas de EDR. Cuando responde a las amenazas, KUMA ejecuta scripts que crean las tareas de EDR correspondientes. Para realizar las tareas de EDR, usted debe crear una regla de respuesta para el script personalizado en la consola KUMA y seleccionar los 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 de 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. Intercepción de operaciones de archivos en contenedores Docker en servidores ahora es compatible. Un *contenedor* es un entorno aislado en el que una aplicación puede ejecutarse sin interactuar directamente con el sistema operativo. Kaspersky Endpoint Security analiza los archivos de los contenedores a los que el usuario obtiene acceso. Cuando se detecta una amenaza, la aplicación la bloquea e intenta desinfectar el archivo dentro del contenedor. Si el archivo no se puede desinfectar, la aplicación detiene el contenedor.

3. Ahora puede definir el alcance de la protección para proteger carpetas compartidas contra el cifrado externo (componente Detección de comportamiento). Ahora puede especificar las carpetas compartidas que la aplicación debe controlar para detectar actividad en los archivos. También puede excluir archivos del alcance de la protección. En versiones anteriores de la aplicación, el componente Detección de comportamiento supervisaba todas las carpetas compartidas para detectar actividad en 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 utilizando 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 agregó la opción para seleccionar Exclusiones de análisis y aplicaciones de confianza predefinidas. 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). Esas exclusiones abarcan, por ejemplo, archivos de máquina virtual VHD y VHDX. Se pueden agregar exclusiones al crear un paquete de instalación de la aplicación o una directiva, o al instalar Kaspersky Endpoint Security.

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

7. Se agregó 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 deshabilitar este protocolo y usar versiones más recientes de TLS 1.2 o TLS 1.3. De manera predeterminada, Kaspersky Endpoint Security bloquea las conexiones de TLS 1.0. Después de actualizar la versión de la aplicación, la operación de servicios de terceros que usan el protocolo TLS 1.0 puede generar errores. Para evitar problemas durante la operación de 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 las tareas del *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 mientras se analiza el equipo.

2. Ahora puede enviar archivos para analizar 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 los objetos en servidores especiales con imágenes virtuales implementadas de los sistemas operativos Microsoft Windows (servidores de Sandbox). Si desea enviar un archivo para analizar en KATA Sandbox, seleccione el comando relevante 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) forma parte de Kaspersky Anti Targeted Attack Platform. Puede configurar la interacción con NDR tanto en modo estándar como en modo EDR Agent.

4. Se agregó compatibilidad con la versión 2021 del cliente de correos de Microsoft Office Outlook a la extensión de Protección contra amenazas de correo. La extensión permite analizar mensajes en el nivel de cliente de correo en lugar de en el 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 realiza 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. Se agregó la funcionalidad para la integración con la solución SIEM de Kaspersky, *Kaspersky Unified Monitoring and Analysis Platform (KUMA)*. 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) de todos los equipos en los que está instalado Kaspersky Endpoint Security, sin instalar agentes de KUMA en estos equipos.

2. Se agregó el componente nuevo *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 del registro y la conexión de los dispositivos externos. El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que podrían indicar filtraciones de seguridad en el equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos y las alertas correspondientes, y las envía al administrador. Monitor de integridad de archivos ya forma parte de la aplicación. La configuración de Monitor de integridad de archivos se migra automáticamente a Control de integridad del sistema cuando se actualiza la aplicación. Para garantizar el correcto funcionamiento de Control de integridad del sistema, tanto la aplicación de Kaspersky Endpoint Security como el complemento de administración deben actualizarse a la versión 12.6.

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

4. Se agregó la opción de seleccionar Exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis y aplicaciones de confianza predefinidas ayudan a configurar rápidamente la zona de confianza al usar la aplicación en servidores SQL, servidores de Microsoft Exchange y System Center Configuration Manager. Esas exclusiones abarcan, por ejemplo, archivos de base de datos MDF y LDF. Se pueden agregar exclusiones al crear una nueva directiva, modificar una directiva existente o al instalar Kaspersky Endpoint Security.

5. La visualización de los detalles de las alertas para Kaspersky Endpoint Detection and Response Optimum se movió desde el complemento de administración de Kaspersky Endpoint Security hasta un complemento de administración independiente de Kaspersky Endpoint Detection and Response. Este complemento de administración de EDR es un complemento único para trabajar con agentes en los sistemas operativos Windows, Mac y Linux. Ahora, cuando trabaja con EDR Optimum, necesitará el complemento de administración de Kaspersky Endpoint Security para crear tareas de respuesta ante amenazas y el complemento de administración de EDR para ver los detalles de las alertas.

6. Compatibilidad con 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 agregó la opción para configurar las exclusiones de telemetría. *Telemetría* es una lista de eventos que ocurrieron en el equipo protegido. Kaspersky Anti Targeted Attack Platform (EDR) usa los datos de telemetría para supervisar y proteger la infraestructura de TI de la organización. La configuración de exclusiones de telemetría ayuda a mejorar el rendimiento del equipo y a 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 agregar sus propias exclusiones de análisis (locales) y aplicaciones de confianza. Esto evita el acceso no autorizado de un intruso a la zona de confianza, lo que aumenta el nivel de seguridad del equipo.

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

4. Se agregó una nueva categoría de recursos web *Herramientas de IA generativas*. Puede configurar el acceso a los sitios web desde la nueva categoría usando Control web.

5. Ahora puede seleccionar la ubicación de una regla 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 agregar al final de la lista, después de lo cual uno debía mover manualmente la regla a través de la lista para priorizarla. Ahora, al agregar una regla, es posible elegir si la regla se debe colocar al principio de la lista, al final de esta o al lado de la regla seleccionada.

6. En las reglas de los componentes de Kaspersky Endpoint Security, ahora puede seleccionar usuarios no solo de Active Directory, sino también de la lista de usuarios en Kaspersky Security Center. También puede ingresar los datos de la cuenta de usuario local manualmente. Se agregó esta posibilidad 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 Protección contra amenazas de red). Ahora puede ver la dirección MAC del equipo atacante en el informe, además de su dirección IP. Esto es útil para investigar 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 aumentó el nivel de los requisitos de protección informática. El nivel de protección alto ahora requiere habilitar la protección de los servicios de la aplicación contra la administración externa. Compruebe el indicador de nivel de seguridad en la parte superior de la ventana de la directiva. Si tiene un nivel de seguridad medio o bajo, puede habilitar 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 agregó compatibilidad para nuevos eventos de detección de objetos cuando la aplicación se ejecuta con la configuración de Endpoint Detection and Response Agent (EDR Agent). Estos eventos ya eran compatibles con la configuración de [KES + agente incorporado].

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 y pf16013.

Actualización 12.4

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

1. Se agregó una nueva funcionalidad para proteger la conexión del equipo a Kaspersky Security Center. La nueva tarea *Protección de la conexión del Servidor de administración* permite establecer una contraseña para conectarse a un servidor de confianza. Esto significa que no se puede reconectar el equipo y ejecutar comandos desde otro servidor sin esta contraseña.

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

3. Compatibilidad con Windows 11 23H2.

Actualización 12.3

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

1. Ahora puede 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 (p. ej., 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 mejoró el funcionamiento de Kaspersky Endpoint Security con dispositivos Bluetooth. Ahora puede configurar exclusiones y restringir el acceso a todos los dispositivos Bluetooth, excepto los dispositivos de entrada (teclados inalámbricos, mouses, etc.).

3. Se optimizó 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 aumentó el nivel de los requisitos de protección informática. El nivel de protección alto ahora requiere habilitar la protección con contraseña. Compruebe el indicador de nivel de seguridad en la parte superior de la ventana de directiva. Si tiene un nivel de protección medio o bajo, puede habilitar la protección con contraseña en la ventana de recomendación del indicador de nivel de seguridad.

5. Se agregó compatibilidad con el protocolo HTTPS para permitir que la aplicación funcione con Kaspersky Security Network. Habilite el uso de HTTPS en las propiedades del Servidor de administración en 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 agregó compatibilidad con el protocolo WPA3 para controlar las conexiones a 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 la Protección contra amenazas de 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 de red desde direcciones IP de confianza.

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

Actualización 12.1

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

1. Se agregó un agente incorporado para la solución Kaspersky Anti Targeted Attack Platform. Ya no necesita Kaspersky Endpoint Agent para usar EDR (KATA). Kaspersky Endpoint Security llevará a cabo todas las funciones de Kaspersky Endpoint Agent. Para migrar las directivas de Kaspersky Endpoint Agent, use el Asistente de migración. Luego de actualizar la aplicación, Kaspersky Endpoint Security pasa a usar el agente incorporado y elimina Kaspersky Endpoint Agent. Se agregó Kaspersky Endpoint Agent a la lista de software no compatible. Kaspersky Endpoint Security tiene agentes incorporados para todas las soluciones de Detection and Response, por lo que ya no es necesario instalar Kaspersky Endpoint Agent para la integración con esas soluciones.

2. Ahora se admite el modo de compatibilidad de Azure WVD. Esta función garantiza la correcta visualización del estado de la máquina virtual Azure en la consola de Kaspersky Anti Targeted Attack Platform. El modo de compatibilidad de Azure WVD permite asignar una identificación de sensor único y permanente a estas máquinas virtuales.

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

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

Problemas solucionados

En la siguiente tabla, se enumeran todos los problemas detectados en versiones anteriores de Kaspersky Endpoint Security y solucionados en la versión actual.

Lista de problemas solucionados en la versión 14.1

ID del problema	Descripción del problema
10140523	Habilitar 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 habilitado, el Explorador de Windows no actualiza automáticamente el contenido de una carpeta de red después de que se modifica desde otro dispositivo.
9722863	El informe de Control de dispositivos no incluye el evento de desconexión del 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.

ID del problema	Descripción del problema
10157563	Folder Redirection puede no funcionar después de un reinicio en estaciones de trabajo VDI.
10158494	Control de dispositivos registra varios eventos de conexión y desconexión de un dispositivo extraíble sin que este se vuelva a conectar físicamente.

Preguntas frecuentes

GENERAL

¿En qué equipos puedo usar Kaspersky Endpoint Security?

¿Qué cambió 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 en 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 ejecutar un análisis de malware sin que el usuario lo sepa?

¿Cómo suspendo la protección de Kaspersky Endpoint Security?

¿Cómo restauro un archivo que Kaspersky Endpoint Security eliminó 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 Wi-Fi 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 juegos de computadora?

¿Cómo verifico si Control de aplicaciones se configuró correctamente?

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

DISPOSITIVOS

¿Cómo puedo impedir el uso de unidades flash?

¿Cómo agrego 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?

¿Podré obtener acceso 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 habilito una escritura en archivos de volcado?

Kaspersky Endpoint Security para Windows

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

La aplicación no está diseñada para 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. Los expertos de Kaspersky desarrollaron este modelo. Posteriormente, 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 de expertos

Kaspersky Endpoint Security utiliza datos de amenazas agregados 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. A continuación, el sistema determina la reputación del objeto y agrega los datos a las bases de datos antivirus. Si el sistema no puede determinar la reputación del objeto, consulta a los analistas de virus de Kaspersky.

Sandbox

Kaspersky Endpoint Security procesa el objeto en una máquina virtual. Kaspersky Sandbox analiza el comportamiento del objeto y decide sobre su reputación. Esta tecnología solo está disponible si usa la solución Kaspersky Sandbox.

Cloud Sandbox

Kaspersky Endpoint Security analiza objetos en un entorno aislado que brinda Kaspersky. La tecnología Cloud Sandbox está habilitada de forma permanente y está disponible para todos los usuarios de Kaspersky Security Network, independientemente del tipo de licencia que utilicen. Si ya implementó la solución Endpoint Detection and Response, puede habilitar un contador independiente para las amenazas que detecte Cloud Sandbox.

Árbol de selección

Cada tipo de amenaza es procesado por un componente exclusivo. Los componentes se pueden habilitar o deshabilitar de forma independiente y su configuración se puede configurar.

Sección	Componente
Protección básica contra amenazas	**Protección contra amenazas de archivo** El componente Protección contra archivos peligrosos le permite evitar la infección del sistema de archivos del equipo. De manera predeterminada, el componente Protección contra amenazas de archivo reside permanentemente en la memoria RAM del equipo y analiza en tiempo real todos los archivos abiertos, guardados y ejecutados. El componente analiza archivos en todas las unidades de la computadora, incluidas las unidades conectadas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network. **Protección contra amenazas web** El componente Protección contra amenazas web está diseñado para bloquear sitios web maliciosos y fraudulentos e impedir la descarga de archivos dañinos de Internet. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network. **Protección contra amenazas de correo** El componente Protección contra amenazas de correo analiza los archivos adjuntos a los mensajes de correo entrantes y salientes para detectar virus y otras amenazas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network. La Protección contra amenazas de 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 agregar el certificado de Kaspersky al almacén de certificados y seleccionar su almacén de certificados propios. La Protección contra amenazas de correo no es compatible con otros protocolos y clientes de correo. Es posible que la Protección contra amenazas de correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, la Protección contra amenazas de correo incluye una extensión para Microsoft Office Outlook. La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365. En equipos basados en Arm, la extensión de Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64. **Protección contra amenazas de red** El componente *Protección contra amenazas de red* (también llamado 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 ataque de red contra el equipo del usuario, bloquea la conexión al equipo agresor. Las distintas clases de ataques de red sobre las que se tiene registro, así como las maneras de combatirlos, se describen en las bases de datos de la aplicación. La lista de ataques de red que detecta el componente Protección contra amenazas de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación. **Firewall** El componente Firewall impide que se establezcan conexiones no autorizadas cuando el equipo está conectado a una red local o a Internet. Firewall también controla la actividad de red de las aplicaciones instaladas en el equipo. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el servicio de nube Kaspersky Security Network y las *reglas de red* predefinidas. **Prevención de ataques BadUSB** El componente Prevención de ataques BadUSB impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo. **Protección vía AMSI** El componente Protección vía AMSI está diseñado para admitir la Antimalware Scan Interface de Microsoft. La *interfaz de análisis antimalware AMSI* permite que las aplicaciones de terceros envíen a Kaspersky Endpoint Security aquellos objetos que precisan analizar (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 avanzada contra amenazas	**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 los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, los servicios KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web analizadas, así como información sobre la categoría y la reputación de los archivos analizados . **Detección de comportamiento** El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones del equipo y transmite esta información a los demás componentes de protección para mejorar su rendimiento. El componente Detección de comportamiento utiliza firmas de patrones de comportamiento para aplicaciones. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Endpoint Security realiza la acción de respuesta especificada. Las funcionalidades de Kaspersky Endpoint Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo. El componente Detección de comportamiento también supervisa los puertos de red en busca de procesos de aplicaciones que podrían representar una amenaza para la seguridad del equipo. La aplicación recibe información sobre dichos procesos y las bases de datos antivirus. **Anticifrador** El componente Anticifrador analiza la actividad en las carpetas compartidas. Cuando la actividad coincide con una firma de patrones de comportamiento que suele verse en actos de 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. Por ejemplo, los exploits pueden utilizar un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malintencionado. 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 podrían representar una amenaza para la seguridad del equipo. La aplicación recibe información sobre dichos procesos y las bases de datos antivirus. **Prevención de intrusiones en el host** El componente Prevención contra intrusos impide que las aplicaciones realicen acciones que puedan ser peligrosas para el sistema operativo y garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus y el servicio de nube Kaspersky Security Network. **Motor de reparación** El componente Motor de reparación permite a Kaspersky Endpoint Security deshacer acciones que han sido realizadas por el malware en el sistema operativo.

Sección	Componente
Controles de seguridad	**Control de aplicaciones** El componente Control de aplicaciones se utiliza para gestionar la ejecución de aplicaciones en los equipos de los usuarios. Permite, con ello, implementar una directiva de seguridad corporativa que regule el uso de aplicaciones. Gracias a las restricciones de acceso, el componente también ayuda a reducir el riesgo de que los equipos se infecten. **Control de dispositivos** El Control de dispositivos administra el acceso de los usuarios a los dispositivos que se instalan o se conectan al equipo (por ejemplo, discos duros, cámaras o módulos Wi-Fi). Esto impide la infección del equipo cuando se conectan dichos dispositivos y evita las pérdidas o fugas de datos. **Control web** Control web permite regular el acceso de los usuarios a los recursos web. Esto permite reducir el tráfico y el uso inadecuado del tiempo de trabajo. Cuando un usuario intente abrir un sitio web restringido por Control web, Kaspersky Endpoint Security bloquea el acceso y le muestra una advertencia. **Control de anomalías adaptativo** El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos conectados a una red corporativa. Para ello utiliza una serie de reglas, diseñadas para buscar comportamientos que no se consideran típicos (por ejemplo, la regla *Inicio de Microsoft PowerShell desde una aplicación de ofimática*). Los especialistas de Kaspersky crean estas reglas basándose en casos característicos de actividad maliciosa. La manera en que el Control de anomalías adaptativo responde ante cada regla es configurable; esto significa que, por ejemplo, es posible permitir la ejecución de scripts de PowerShell que se hayan creado para automatizar ciertos aspectos de un flujo de trabajo. Las reglas se actualizan junto con las bases de datos de Kaspersky Endpoint Security. **Inspección de registros** Inspección de registro monitorea la integridad del entorno protegido en función del análisis del registro de eventos de Windows. Cuando la aplicación detecta indicios de un comportamiento atípico en el sistema, informa al administrador, ya que este comportamiento puede indicar un intento de ciberataque. **Control de integridad del sistema** El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que podrían indicar filtraciones de seguridad en el equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos y las alertas correspondientes, y las envía al administrador.
Tareas	**Análisis de malware** Kaspersky Endpoint Security analiza el equipo en busca de virus y otras amenazas. Análisis de malware ayuda a descartar la posibilidad de propagar malware que no detectaron los componentes de protección, por ejemplo, debido a un nivel bajo de seguridad. **Actualización de bases de datos y módulos de la aplicación** Kaspersky Endpoint Security descarga bases de datos y módulos de la aplicación actualizados. El proceso de actualización mantiene al equipo protegido contra los últimos virus y otras amenazas. La aplicación se actualiza automáticamente de forma predeterminada, pero, si es necesario, puede actualizar manualmente las bases de datos y los módulos de la aplicación. **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 la aplicación a sus versiones anteriores cuando sea necesario, por ejemplo, cuando 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 verifica los módulos de la aplicación presentes en la carpeta de instalación de la aplicación en busca de fallas o modificaciones. Si un módulo de la aplicación tiene una firma digital incorrecta, el módulo se considera dañado.
Cifrado de datos	**Cifrado de archivos** El componente permite crear reglas de cifrado de archivos. Puede seleccionar carpetas predefinidas 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 uso de Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker. **Cifrado de unidades extraíbles** El componente permite proteger datos en unidades extraíbles. Puede utilizar 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 lo sucesivo, también denominada "EDR Optimum"). *Kaspersky Endpoint Detection and Response* es una solución para proteger la infraestructura de TI corporativa contra amenazas cibernéticas avanzadas. Las características de la solución combinan la detección automática de las amenazas con la capacidad para reaccionar a estas amenazas para contrarrestar los 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 lo sucesivo, también denominada "EDR Expert"). EDR Expert ofrece más funcionalidades de supervisión y respuesta antes 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 incorporados 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 que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. 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 adquirir todas las unidades funcionales o las unidades funcionales individuales por separado. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform. **Sandbox** Agente incorporado 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 los objetos en servidores especiales con imágenes virtuales implementadas de los sistemas operativos Microsoft Windows (servidores de Sandbox). Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Sandbox y la Ayuda de Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Agente integrado para dar soporte a la operación 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 usa datos de telemetría recibidos de puntos de conexión y aprendizaje automático. MDR envía los datos de los incidentes a los expertos de Kaspersky. A continuación, los expertos pueden procesar el incidente y, por ejemplo, agregar una nueva entrada a las bases de datos antivirus. Alternativamente, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener más detalles sobre el funcionamiento de la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Modos de la aplicación: Estándar, EDR Agent, Light Agent

Kaspersky Endpoint Security para Windows forma parte de muchas soluciones de Kaspersky. Según la solución, debe seleccionar un modo para la aplicación.

Modo estándar

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 forma parte de Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security brinda una protección integral 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, entre otros.

EDR Agent

Este modo permite implementar 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 SIEM de Kaspersky: Kaspersky Unified Monitoring and Analysis Platform (KUMA).

En este modo, los componentes de protección estándar, como Protección contra amenazas de archivo o Protección contra amenazas web, no están disponibles. La solución EPP de terceros brinda la protección estándar del equipo. EDR 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 el modo de Light Agent forma parte de la solución Kaspersky Hybrid Cloud Security. Light Agent protege las máquinas virtuales con sistemas operativos huéspedes para estaciones de trabajo y servidores. En este modo, están disponibles los mismos componentes de protección y control que en el modo Estándar. La diferencia es que los objetos se analizan en busca de virus y otro malware mediante un componente de solución especial instalado en una máquina virtual independiente, SVM (Secure Virtual Machine). Por lo tanto, Light Agent utiliza los recursos de la SVM para garantizar la seguridad de la infraestructura en lugar de usar 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 su instalación en computadoras con arquitectura x86/x64. Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado Estándar de Cifrado Avanzado (AES, Advanced Encryption Standard) con una eficaz longitud de clave de 256 bits.

- **AES56**

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

- **Arm64**

  Este paquete de distribución está diseñado para instalarse en equipos basados en Arm. Este paquete de distribución no está diseñado para su instalación 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 de almacenamiento autoextraíble en formato EXE. Para ver el contenido del paquete de distribución, debe extraer el archivo de almacenamiento en una carpeta separada. Cada paquete de distribución contiene los siguientes archivos:

`kes_win.msi`	Paquete de instalación de Kaspersky Endpoint Security.
`setup_kes.exe`	Los archivos necesarios para instalar la aplicación utilizando 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 incompatible.
`incompatible.txt`	Archivo que contiene la lista de software que podría generar problemas de compatibilidad con Kaspersky Endpoint Security. Kaspersky no garantiza la compatibilidad de Kaspersky Endpoint Security con el software presente en la lista.
`ksn_<language ID>.txt`	Archivo donde puede leer los términos de participación en Kaspersky Security Network.
`license.txt`	Archivo donde puede leer el Contrato de licencia de usuario final y la Política de privacidad.
`installer.ini`	Archivo installer.ini que contiene las configuraciones internas del kit de distribución.
`kes.cab`	Archivos para la interfaz gráfica de la aplicación.
`aes256.cab` / `aes56.cab`	Archivos para el algoritmo criptográfico 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 quiere cambiar opciones de instalación, use el archivo setup.ini.

Requisitos de hardware y software

En este artículo se enumeran las versiones de software en las que se probó 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 sometieron a un ciclo de pruebas completo y no están incluidas en la lista de versiones con compatibilidad garantizada.

Para asegurarse de que Kaspersky Endpoint Security funcione correctamente, su equipo debe cumplir los siguientes requisitos:

Para instalar la aplicación, necesita derechos de administrador en la computadora.

Requisitos mínimos generales

Requisitos mínimos	Estación de trabajo (x86/x64)	Servidor (x86/x64)	Arm
Depósito	2 GB	2 GB	2 GB
CPU	1 GHz, compatible con instrucciones SSE2	1,4 GHz, compatible con instrucciones SSE2	1 GHz, arquitectura Armv8.1
RAM	Estación de trabajo (x86): 1 GB Estación de trabajo (x64): 2 GB	2 GB Nota: El servidor necesita 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 en 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
- Windows 11 for 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 se habilita de manera predeterminada si se instalan una tarjeta de red y controladores compatibles en el equipo. Deshabilitar URO en el equipo de un usuario puede reducir de manera significativa el rendimiento de la aplicación.

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

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

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

Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows 11, visite la Base de conocimientos del Servicio de 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 para Windows Server en los servidores y clústeres de su organización (Cluster Mode). La aplicación también es compatible con Server Core Mode (consulte problemas conocidos).

Sistemas operativos admitidos en servidores:

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

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

- 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 (se incluye el modo Server Core)
- Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter (se incluye el modo Server Core)
- Windows Server 2016 Essentials/Standard/Datacenter (se incluye el modo Server Core)
- Windows Server 2019 Essentials/Standard/Datacenter (se incluye el modo Server Core)

- Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition (se incluye modo Server Core)
- Windows Server 2025 Standard / Datacenter

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

Para obtener más información sobre el soporte técnico de los sistemas operativos Microsoft Windows Server 2016 y Microsoft Windows Server 2019, consulte la Base de conocimientos del Servicio de soporte técnico.

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

Sistemas operativos para servidores no compatibles:

- 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 Core Standard/Enterprise/Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard/Premium Service Pack 2

Plataformas virtuales

Plataformas virtuales compatibles con el funcionamiento estándar de la aplicación:

- VMware Workstation Pro 26H1
- VMware ESXi 8.0, actualización 3i
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4.

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

Máquinas virtuales para instalar 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 ser compatible con la especificación SMBIOS versión 2.1 o posterior.

Se deben instalar los siguientes paquetes y utilidades en las máquinas virtuales en los siguientes casos:

- Si utiliza Microsoft Hyper-V: paquete Integration Services.
- Si utiliza VMware vSphere: paquete VMware Tools.
- Si utiliza XenServer: paquete XenTools.
- Si utiliza HUAWEI FusionSphere: paquete HUAWEI Tools.
- Cuando se utilizan hipervisores basados en KVM: QEMU Guest Agent.

Consulte la Ayuda de Kaspersky Security for Virtualization Light Agent si desea conocer los requisitos de la infraestructura para ejecutar la aplicación en el modo de 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 compatibles:

- 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 es compatible con el funcionamiento de 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

Comparación de las características disponibles de la aplicación según el tipo de sistema operativo

El conjunto de características disponibles en Kaspersky Endpoint Security depende de si el sistema operativo está diseñado para estaciones de trabajo o para servidores (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 utilizando 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 características de Kaspersky Endpoint Security

Característica	Estaciones de trabajo	Estación de trabajo basada en Arm	Servidores	Modo Server Core
Protección avanzada contra amenazas				
Kaspersky Security Network	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓

Característica	Estaciones de trabajo	Estación de trabajo basada en Arm	Servidores	Modo Server Core
Anticifrador	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	–	–
Motor de reparación	✓	✓	✓	✓
Protección básica contra amenazas				
Protección contra amenazas de archivo	✓	✓	✓	✓
Protección contra amenazas web	✓	✓	✓	–
Protección contra amenazas de correo	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓	✓
Prevención de ataques BadUSB	✓	✓	✓	–
Protección vía 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	✓	✓	✓	✓

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 de más abajo).

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

- Consola de administración. Complemento para Microsoft Management Console (MMC) que se instala en la estación de trabajo del administrador.

- Web Console. Componente de Kaspersky Security Center que se instala en el Servidor de administración. Para trabajar con Web Console, utilice el navegador de cualquier equipo que tenga acceso al Servidor de administración.

La aplicación también se puede administrar a través de Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* es la versión en la nube de Kaspersky Security Center. Ello significa que el Servidor de administración y los demás componentes de Kaspersky Security Center están instalados en la infraestructura de nube de Kaspersky. Para más detalles sobre cómo administrar la aplicación con Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Kaspersky Endpoint Security forma parte de la solución Pro View de Kaspersky Next. Para obtener más información sobre las características que ofrece la aplicación cuando funciona como parte de esta solución, consulte la Ayuda de Kaspersky Next.

Comparación de las características de Kaspersky Endpoint Security

Característica	Kaspersky Security Center		Kaspersky Security Center
	Consola de administración	Web Console	Cloud Console
Protección avanzada contra amenazas			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Detección de comportamiento	✓	✓	✓
Anticifrador			
Prevención de exploits	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	✓
Motor de reparación	✓	✓	✓
Protección básica contra amenazas			
Protección contra amenazas de archivo	✓	✓	✓
Protección contra amenazas web	✓	✓	✓
Protección contra amenazas de correo	✓	✓	✓
Firewall	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓
Prevención de ataques BadUSB	✓	✓	✓
Protección vía AMSI	✓	✓	✓
Controles de seguridad			
Inspección de registros	✓	✓	✓
Control de aplicaciones	✓	✓	✓
Control de dispositivos	✓	✓	✓
Control web	✓	✓	✓
Control de anomalías adaptativo	✓	✓	✓
Control de integridad del sistema	✓	✓	✓

Característica	Kaspersky Security Center		Kaspersky Security Center
	Consola de administración	Web Console	Cloud Console
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			
Agregar clave	✓	✓	✓
Cambiar componentes de la aplicación	✓	✓	✓
Inventario	✓	✓	✓
Actualización	✓	✓	✓
Reversión de la actualización	✓	✓	✓
Análisis de malware	✓	✓	✓
Comprobación de integridad de la aplicación	✓	✓	–
Eliminación de datos	✓	✓	✓
Administrar cuentas del Agente de autenticación (Cifrado de Disco de Kaspersky)	✓	✓	–
Análisis de IOC (EDR)	–	✓	✓
Poner archivo en cuarentena (EDR)	–	✓	✓
Obtener archivo (EDR)	–	✓	✓
Eliminar archivo (EDR)	–	✓	✓
Iniciar proceso (EDR)	–	✓	✓
Finalizar proceso (EDR)	–	✓	✓

Compatibilidad con otras aplicaciones

Kaspersky Endpoint Security no es compatible con algunas aplicaciones de Kaspersky ni con algunas aplicaciones de terceros. Entonces, antes de instalar, actualizar la versión de la aplicación y cambiar los componentes de la aplicación, Kaspersky Endpoint Security analiza el equipo para verificar si hay aplicaciones de este tipo.

Compatibilidad con aplicaciones de terceros

Kaspersky Endpoint Security no es compatible con aplicaciones que forman parte de sistemas de protección para endpoints de terceros (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security también puede tener problemas de compatibilidad con otras aplicaciones. Para determinar la compatibilidad, Kaspersky Endpoint Security verifica una lista de software que elaboró Kaspersky. Esta lista se encuentra en el archivo incompatible.txt. El archivo está incluido en el kit de distribución.

Kaspersky no garantiza la compatibilidad de Kaspersky Endpoint Security con el software presente en 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 está de acuerdo con ignorar los riesgos y desea 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 Detection and Response de Kaspersky.

  > Kaspersky está cambiando toda la Detection and Response para trabajar con el agente incorporado 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 la versión 12.0 de Kaspersky Endpoint Security, ahora 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 a que finalice este proceso antes de continuar con la instalación de Kaspersky Endpoint Security.

Omitir la verificación de software que podría generar problemas de compatibilidad

Si Kaspersky Endpoint Security detecta software presente en la lista incompatible.txt, se detendrá la instalación de la aplicación. Para continuar con la instalación, debe eliminar dicha aplicación. Sin embargo, si el proveedor del software de terceros indica 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, un 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 verificación del software instalado. Para hacerlo, pase los siguientes parámetros al instalador:

- `SKIPPRODUCTCHECK=1` Deshabilite la búsqueda de software instalado. La lista de software que podría generar problemas de compatibilidad se encuentra en el archivo incompatible.txt, que forma parte del kit de distribución. Si no se fija un valor para este parámetro y se detecta algún software de esta lista, la instalación de Kaspersky Endpoint Security se detendrá.

- `SKIPPRODUCTUNINSTALL=1` Deshabilite la eliminación automática del software detectado presente en la lista incompatible.txt. Si no se fija un valor para este parámetro, Kaspersky Endpoint Security intentará eliminar el software que podría generar problemas de compatibilidad.

- `CLEANERSIGNCHECK=0` Deshabilite la comprobación de firmas digitales de las aplicaciones encontradas mediante la verificación. Si no se establece este parámetro, la verificación de firmas digitales se deshabilita al implementar la aplicación a través de Kaspersky Security Center. Cuando la aplicación se instala localmente, la verificación de firma digital está habilitada de manera predeterminada.

Puede pasar parámetros en la línea de comando al instalar la aplicación de forma local.

Si durante el proceso de instalación omitió el análisis en busca de software que pudiera causar problemas de compatibilidad, Kaspersky Endpoint Security puede volver a realizar esta comprobación cuando cambien los componentes de la aplicación. Para omitir el análisis de 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 Kaspersky Endpoint Security de forma remota, debe agregar los parámetros apropiados al archivo de generación del paquete de instalación llamado `kes_win.kud` en `[Setup]` (detalles a continuación). El archivo `kes_win.kud` está incluido 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 manera local, utilizando el Asistente de instalación;
- de manera local, utilizando la línea de comandos;
- de manera remota, a través de Kaspersky Security Center;
- de manera 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 manera 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 valores recibidos del archivo setup.ini,
2. los valores recibidos del archivo installer.ini,
3. los valores recibidos de la línea de comandos,
4. los valores recibidos del archivo de configuración (install.cfg).

Se recomienda cerrar todas las aplicaciones en ejecución antes de iniciar 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 ocurrir errores. Para obtener más información sobre cómo solucionar estos errores, consulte la Base de conocimientos del Servicio de soporte técnico.

Despliegue mediante Kaspersky Security Center

Kaspersky Endpoint Security puede desplegarse en equipo dentro de una red corporativa de varias maneras. 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 el Agente de red de Kaspersky Security Center esté instalado en el equipo. El *Agente de red* facilita la interacción entre el Servidor de administración y un equipo cliente.

Los principales métodos de despliegue que admite Kaspersky Security Center son los siguientes:

- Instalación de la aplicación utilizando el Asistente de despliegue de 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.

  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.

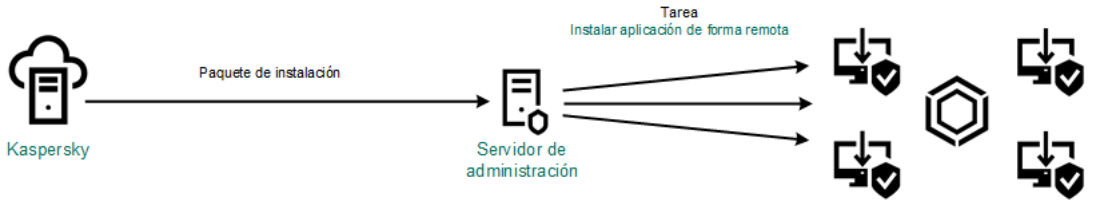
Instalación estándar de la aplicación

Kaspersky Security Center cuenta con un Asistente de despliegue de la protección, que puede usar para instalar la aplicación en los equipos de la empresa. 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 configuraciones necesarias para instalar la aplicación y ponerla en ejecución inmediatamente después de la instalación. El paquete de instalación se crea utilizando archivos con las extensiones .kpd y .kud incluidas en el kit de distribución de la aplicación. El paquete de instalación de Kaspersky Endpoint Security es común para todas las versiones de Windows y los tipos de arquitectura de procesador compatibles.

2. Creación de la tarea *Instalar aplicación de forma remota* del Servidor de administración de Kaspersky Security Center.



Implementación de Kaspersky Endpoint Security

Cómo ejecutar el Asistente de despliegue de la 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 vínculo **Desplegar paquete de instalación a los dispositivos administrados (estaciones de trabajo)**.

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

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

Paso 1. Seleccionar un paquete de instalación.

En la lista, seleccione el paquete de instalación de Kaspersky Endpoint Security. Si la lista no contiene el paquete de instalación para Kaspersky Endpoint Security, puede crearlo con el Asistente.

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

El Agente de red 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 instala otra vez.

Paso 2. Seleccionar el origen de paquete de instalación

Seleccione la fuente **Desplegar paquete de Kaspersky Security Center**.

Paso 3. Seleccionar los dispositivos en los que se instalará el software

Seleccione los equipos en los que desee instalar Kaspersky Endpoint Security. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. El Agente de red no está instalado en dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Configurar la tarea de instalación remota

Configure los siguientes parámetros adicionales:

- **Forzar la descarga del paquete de instalación**. Seleccione el método con el que se instalará la aplicación:

  - **Con 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 está instalado, la tarea finaliza con un error. En este caso, agregue el paquete de instalación del Agente de red a la tarea *Instalar aplicación de forma remota* y habilite la entrega de archivos a través de los recursos del sistema operativo. Luego, el Agente de red se instalará utilizando los recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.

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

  - **Con los recursos del sistema operativo a través del Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante el uso de 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 para 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 hacer que, por ejemplo, una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes Servidores de Administración u otros conflictos.

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

- **Asignar la instalación del Agente de red en las directivas de grupo de Active Directory**. Instalar el Agente de red en forma manual, utilizando los 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. Seleccionar una clave de licencia

Agregue al paquete de instalación la clave que se usará para activar la aplicación. Este paso es opcional. Si el Servidor de administración contiene una clave de licencia que puede distribuirse automáticamente, se la agregará más adelante sin que usted intervenga. También puede activar la aplicación más tarde usando la tarea *Agregar clave*.

Paso 6. Seleccionar la opción de reinicio del sistema operativo

Elija la acción que se realizará en el caso de que se necesite reiniciar un equipo. No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación.

Paso 7. Eliminar las aplicaciones incompatibles antes de la instalación

Revise detenidamente la lista de aplicaciones incompatibles y permita que se las elimine. Si se instalan aplicaciones incompatibles en el equipo, la instalación de Kaspersky Endpoint Security finaliza con un error.

Paso 8. Seleccionando una cuenta para acceder a los dispositivos

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

Paso 9. Comienzo de la instalación

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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

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

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

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

Paso 1. Seleccionar un paquete de instalación.

En la lista, seleccione el paquete de instalación de Kaspersky Endpoint Security. Si la lista no contiene el paquete de instalación para Kaspersky Endpoint Security, puede crearlo con el Asistente. Para crear el paquete de instalación, no es necesario buscar el paquete de distribución correspondiente y guardarlo en el equipo. Kaspersky Security Center le mostrará una lista de paquetes de distribución disponibles en los servidores de Kaspersky, y el paquete de instalación se creará automáticamente. Kaspersky actualiza la lista después del lanzamiento de nuevas versiones de aplicaciones.

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

Paso 2. Seleccionar una clave de licencia

Agregue al paquete de instalación la clave que se usará para activar la aplicación. Este paso es opcional. Si el Servidor de administración contiene una clave de licencia que puede distribuirse automáticamente, se la agregará más adelante sin que usted intervenga. También puede activar la aplicación más tarde usando la tarea *Agregar clave*.

Paso 3. Selección del 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 instala otra vez.

Paso 4. Seleccionar los dispositivos en los que se instalará el software

Seleccione los equipos en los que desee instalar Kaspersky Endpoint Security. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. El Agente de red no está instalado en dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 5. Configuración de los parámetros avanzados

Configure los siguientes parámetros adicionales:

- **Forzar la descarga del paquete de instalación**. Seleccione el método con el que se instalará la aplicación:
  - **Con 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 está instalado, la tarea finaliza con un error. En este caso, agregue el paquete de instalación del Agente de red a la tarea *Instalar aplicación de forma remota* y habilite la entrega de archivos a través de los recursos del sistema operativo. Luego, el Agente de red se instalará utilizando los recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.
  - **Con los recursos del sistema operativo a través de los puntos de distribución**. El paquete de instalación se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si hay al menos un punto de distribución en la red. Para obtener más información sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.
  - **Con los recursos del sistema operativo a través del Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante el uso de 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 está instalada**. Desactive esta casilla de verificación si desea instalar una versión anterior de la aplicación, por ejemplo.
- **Asignar la 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. Seleccionar la opción de reinicio del sistema operativo

Elija la acción que se realizará en el caso de que se necesite reiniciar un equipo. No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación.

Paso 7. Eliminar las aplicaciones incompatibles antes de la instalación

Revise detenidamente la lista de aplicaciones incompatibles y permita que se las elimine. Si se instalan aplicaciones incompatibles en el equipo, la instalación de Kaspersky Endpoint Security finaliza con un error.

Paso 8. Asignación a un grupo de administración

Seleccione el grupo de administración al que se moverán los equipos una vez que se instale el Agente de red. Los equipos deben incluirse en algún grupo de administración; de lo contrario, no será posible aplicar directivas ni tareas de grupo. Los equipos que ya pertenezcan a un grupo de administración no se moverán. Si no selecciona un grupo de administración, los equipos se agregarán al grupo de **Dispositivos no asignados**.

Paso 9. Seleccionando una cuenta para acceder a los dispositivos

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

Paso 10. Iniciar la instalación

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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 configuraciones necesarias para instalar la aplicación y ponerla en ejecución inmediatamente después de la instalación. El paquete de instalación se crea utilizando archivos con las extensiones .kpd y .kud incluidas en el kit de distribución de la aplicación. El paquete de instalación de Kaspersky Endpoint Security es común 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**.

   Se abre una lista con los 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

Escriba el nombre que se le dará al paquete de instalación, por ejemplo *Kaspersky Endpoint Security para Windows 14.1*.

Paso 3. Seleccionar el paquete de distribución para la instalación

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

Si es necesario, actualice las bases de datos antivirus en el paquete de instalación mediante 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 los términos del Contrato de licencia de usuario final y de la Política de privacidad.

Se creará el paquete de instalación y se lo agregará a Kaspersky Security Center. Con 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 sistemas operativos. 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 seleccionó para ese tipo de sistema operativo. De esta manera, puede usar el mismo paquete de instalación para estaciones de trabajo y servidores.

El paquete de instalación contendrá las bases de datos antivirus que existan en el repositorio del Servidor de administración. Si lo desea, puede actualizar las bases de datos incluidas en el paquete de instalación para que se requiera menos tráfico para actualizarlas cuando concluya la instalación de Kaspersky Endpoint Security.

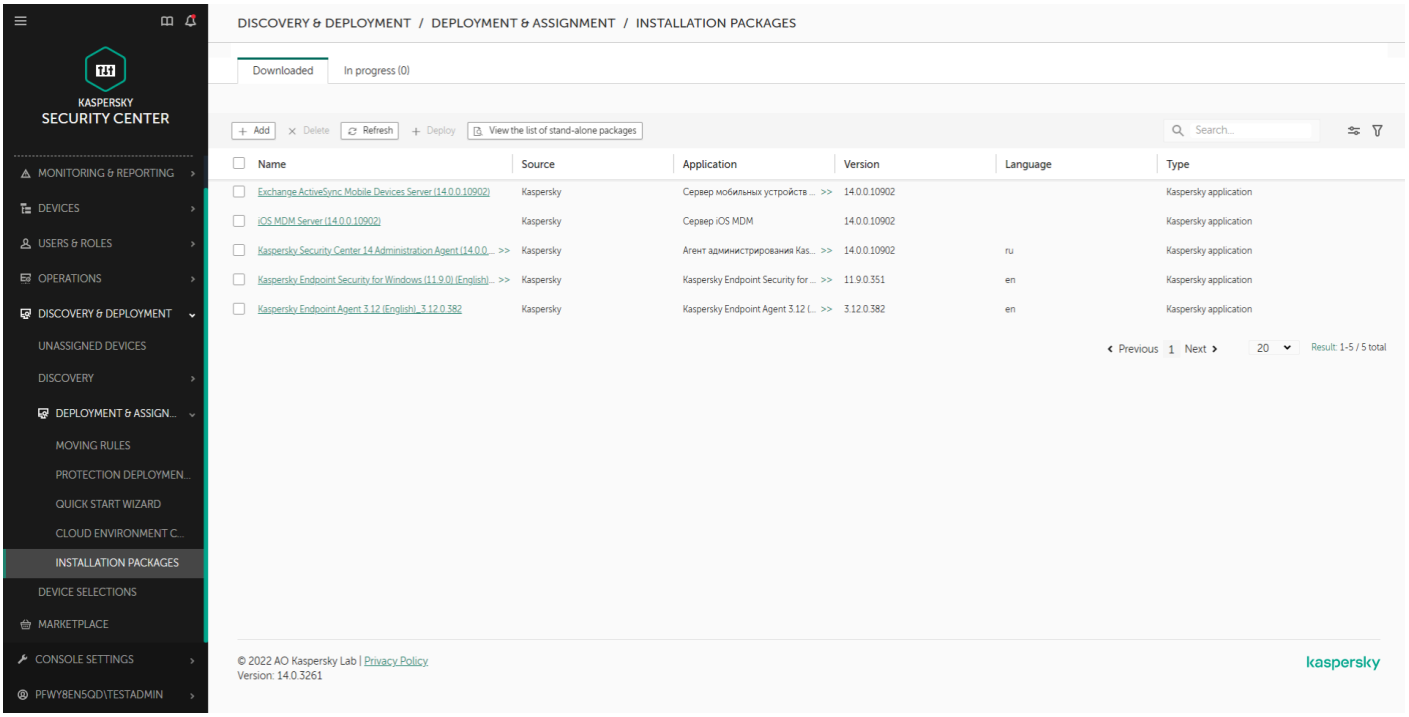
Cómo crear un paquete de instalación en Web Console y Cloud Console

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

   Se abre una lista con los paquetes de instalación que se han descargado a Kaspersky Security Center.

2. Haga clic en **Agregar**.

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



Lista de paquetes de instalación

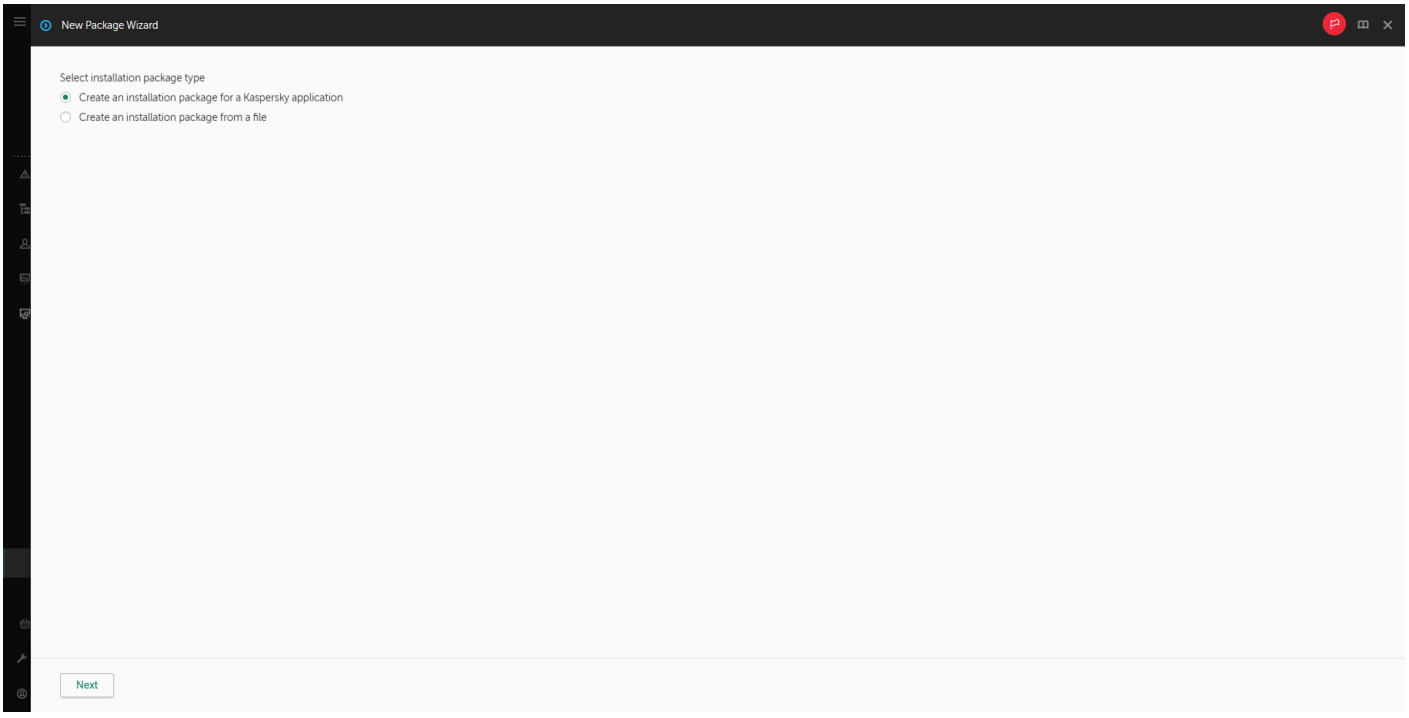
Paso 1. Seleccionar el tipo de paquete de instalación

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 lanzan nuevas versiones de aplicaciones. Para instalar Kaspersky Endpoint Security, recomendamos utilizar esta opción.

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

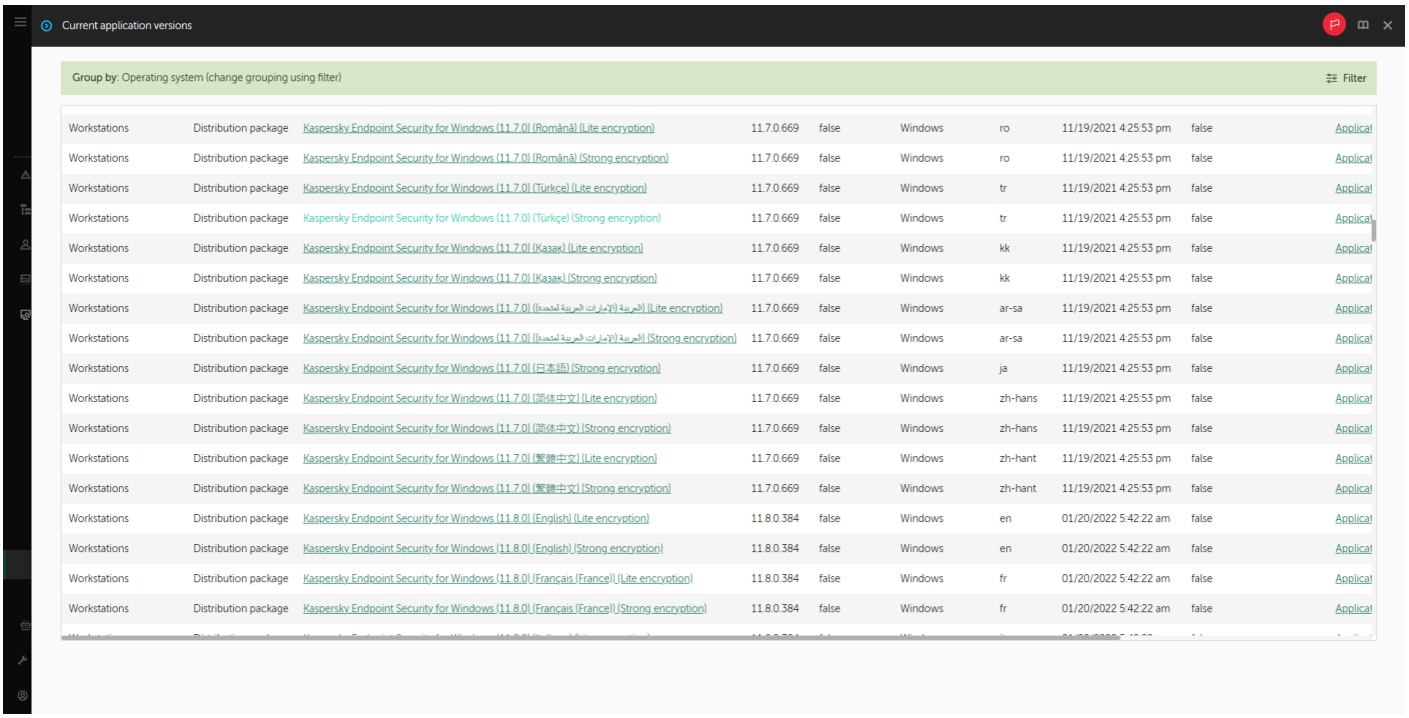
La posibilidad de crear un paquete de instalación para Kaspersky Endpoint Security a partir de un archivo solo está disponible en Kaspersky Security Center Web Console.



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 de la Política de privacidad.



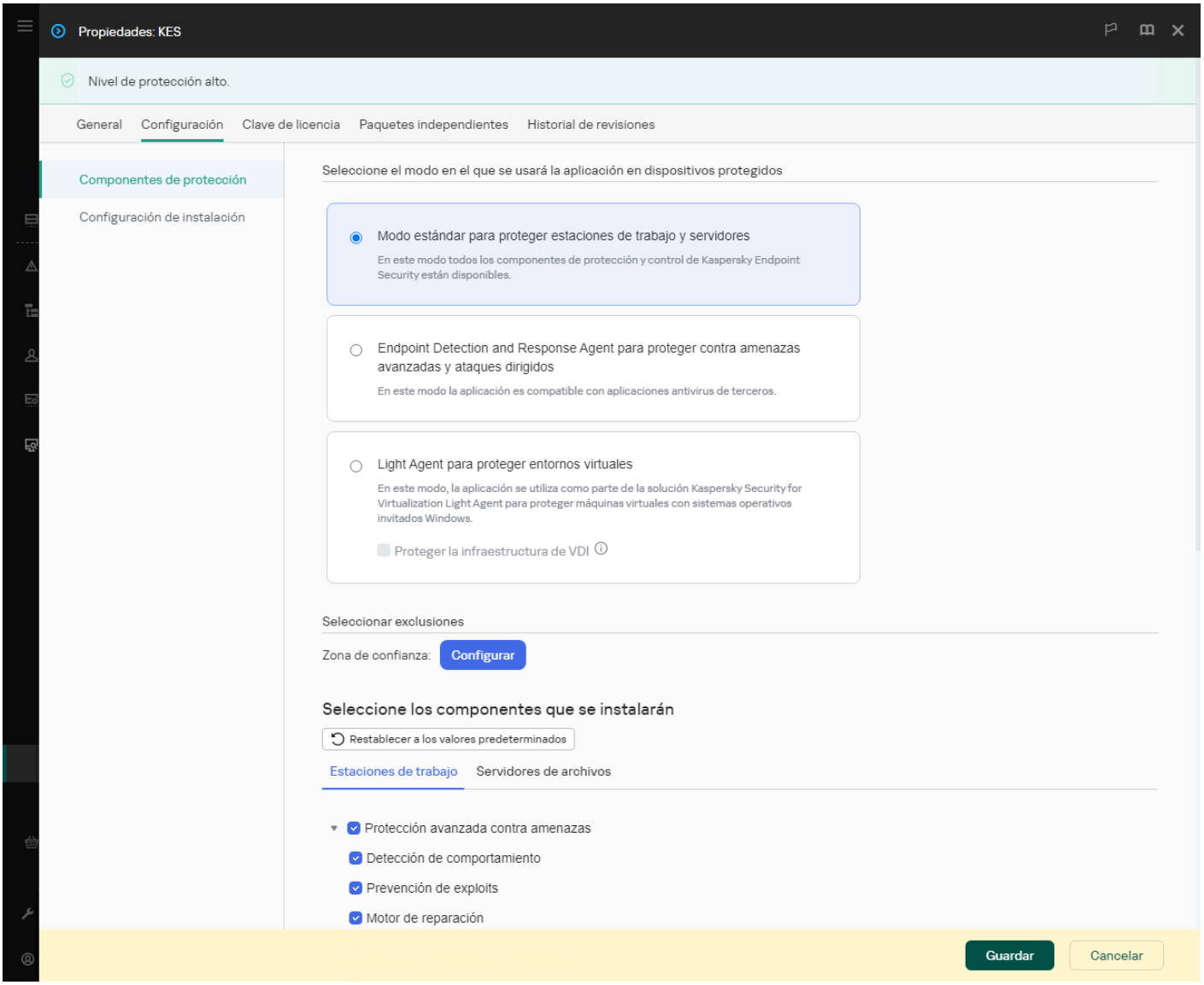
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Lite encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Strong encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Lite encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Strong encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Казак) (Lite encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Казак) (Strong encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) ((العربية (الإمارات العربية المتحدة)) (Lite encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) ((العربية (الإمارات العربية المتحدة)) (Strong encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (日本語) (Strong encryption)	11.7.0.669	false	Windows	ja	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Lite encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Strong encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Lite encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Strong encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat

Lista de paquetes de instalación en servidores de Kaspersky

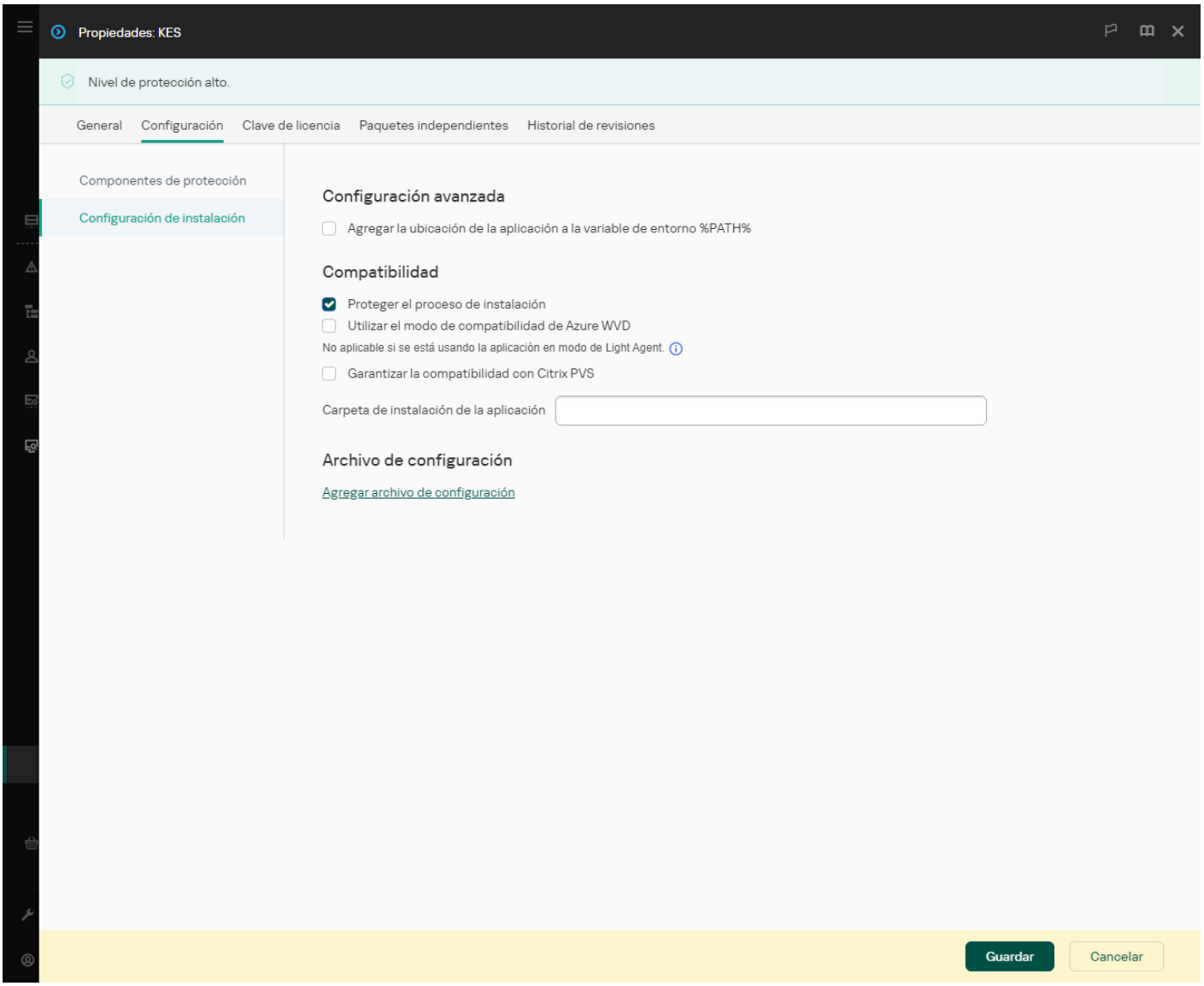
Se creará el paquete de instalación y se lo agregará a Kaspersky Security Center. Con el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación.

En la configuración del paquete de instalación, puede seleccionar componentes de la aplicación para diferentes tipos de sistemas operativos. 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 seleccionó para ese tipo de sistema operativo. De esta manera, puede usar el mismo paquete de instalación para estaciones de trabajo y servidores.

El paquete de instalación contendrá las bases de datos antivirus que existan en el repositorio del Servidor de administración. Si lo desea, puede actualizar las bases de datos incluidas en el paquete de instalación para que se requiera menos tráfico para actualizarlas cuando concluya la instalación de Kaspersky Endpoint Security.



Componentes incluidos en el paquete de instalación



Configuración de instalación del paquete de instalación

Configuraciones del paquete de instalación

Sección	Descripción
Componentes de protección	**Modo estándar**. La configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para las soluciones Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra una variedad de 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 Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros. **Light Agent para proteger entornos virtuales**. Esta configuración está pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.
Exclusiones	A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 el modo de Light Agent para proteger entornos virtuales. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de 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.

Sección	Descripción
Seleccionar componentes para instalar	En esta sección, puede seleccionar los componentes de la aplicación que estarán disponibles. El conjunto de componentes de las aplicaciones puede modificarse 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 seleccionó para ese tipo de sistema operativo. De esta manera, puede usar 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** El componente Prevención de ataques BadUSB, el componente Detection and Response y los componentes de cifrado de datos no se instalan de forma predeterminada. Si desea utilizar estos componentes, puede agregarlos 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 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 hacer eso, debe agregar la clave al Servidor de administración. Para obtener más información sobre cómo agregar una clave al Servidor de administración de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.
Aplicaciones incompatibles	Revise detenidamente la lista de aplicaciones incompatibles y permita que se las elimine. Si se instalan aplicaciones incompatibles en el equipo, la instalación de Kaspersky Endpoint Security finaliza con un error.
Configuración de instalación	**Agregar la ruta del archivo avp.com a la variable del sistema %PATH%**. Puede agregar la ruta de instalación a la variable %PATH% para facilitar el uso de la interfaz de línea de comandos. **Proteger el proceso de instalación**. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda deshabilitar 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. **Utilizar el modo de compatibilidad de Azure WVD**. Esta función garantiza la correcta visualización del estado de la máquina virtual Azure en la consola de Kaspersky Anti Targeted Attack Platform. Para monitorear el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores de KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar una Sensor ID única y permanente a estas máquinas virtuales. Si el modo de compatibilidad está desactivado, la Sensor ID puede cambiar después de reiniciar el equipo debido a cómo funcionan 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.14.1`. **Archivo de configuración**. Instalación de la aplicación con una configuración predefinida. Para continuar, debe cargar un archivo que defina la configuración de Kaspersky Endpoint Security. Puede crear un archivo de configuración en la interfaz local de la aplicación.

Actualización de las bases de datos incluidas en el paquete de instalación

Las bases de datos antivirus incluidas en un paquete de instalación se toman del repositorio del Servidor de administración y son las últimas disponibles al momento de crearse el paquete. Si lo desea, después de crear un paquete de instalación, puede actualizar las bases de datos antivirus que este contiene. Ello ayudará a reducir el volumen de tráfico cuando se las deba actualizar al concluir la instalación de Kaspersky Endpoint Security.

Para actualizar las bases de datos antivirus del repositorio del Servidor de administración, se utiliza una tarea del Servidor de administración llamada *Descargar actualizaciones en el repositorio del Servidor de administración*. Si necesita más información para actualizar las bases de datos antivirus almacenadas en el repositorio del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

Para actualizar las bases de datos incluidas en el paquete de instalación, puede usar la Consola de administración o Kaspersky Security Center Web Console. No es posible usar Kaspersky Security Center Cloud Console para este fin.

Cómo actualizar las bases de datos antivirus del 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**.

   Se abre una lista con los 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 del paquete de instalación se actualizarán utilizando la copia almacenada en el repositorio del Servidor de administración. El archivo `bases.cab` incluido en el kit de distribución se sustituirá con la carpeta `bases`. Los archivos del paquete de actualización estarán en la carpeta.

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

1. En la ventana principal de Web Console, seleccione **Descubrimiento 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 paquete de instalación de Kaspersky Endpoint Security que contenga las bases de datos que deban actualizarse.

   Se abrirá la ventana de propiedades del paquete de instalación.
3. En la ficha **Información general**, haga clic en el vínculo **Actualizar bases de datos**.

Como resultado, las bases de datos antivirus del paquete de instalación se actualizarán utilizando la copia almacenada en el repositorio del Servidor de administración. El archivo `bases.cab` incluido en el kit de distribución se sustituirá con la carpeta `bases`. Los archivos del paquete de actualización estarán en la carpeta.

Creación de una tarea de instalación remota

La tarea *Instalar aplicación de forma remota* está diseñada para instalar Kaspersky Endpoint Security a distancia. Puede usar la tarea *Instalar aplicación de forma remota* para implementar el paquete de instalación de la aplicación en todos los equipos de su organización. Antes de comenzar con el despliegue, puede modificar las propiedades del paquete para seleccionar los componentes que estarán disponibles en la aplicación. Puede también actualizar las bases de datos antivirus incluidas en el paquete.

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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Servidor de administración de Kaspersky Security Center** → **Instalar aplicación de forma remota**.

Paso 2. Seleccionar un paquete de instalación.

En la lista, seleccione el paquete de instalación de Kaspersky Endpoint Security. Si la lista no contiene el paquete de instalación para Kaspersky Endpoint Security, puede crearlo con el Asistente.

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

El Agente de red 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 instala otra vez.

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

Configure los siguientes parámetros adicionales:

- **Forzar la descarga del paquete de instalación**. Seleccione el método con el que se instalará la aplicación:

  - **Con 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 está instalado, la tarea finaliza con un error. En este caso, agregue el paquete de instalación del Agente de red a la tarea *Instalar aplicación de forma remota* y habilite la entrega de archivos a través de los recursos del sistema operativo. Luego, el Agente de red se instalará utilizando los recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.

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

  - **Con los recursos del sistema operativo a través del Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante el uso de 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 para 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 hacer que, por ejemplo, una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes Servidores de Administración u otros conflictos.

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

Paso 5. Seleccionar la opción de reinicio del sistema operativo

Elija la acción que se realizará en el caso de que se necesite reiniciar un equipo. No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. 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 los equipos en los que desee instalar Kaspersky Endpoint Security. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. El Agente de red no está instalado en dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 7. Selección de la cuenta con la que se ejecutará la tarea

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

Paso 8. Programación de la tarea

Programe la ejecución de la tarea. La tarea puede iniciarse manualmente o cuando el equipo está inactivo, por ejemplo.

Paso 9. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Instalar Kaspersky Endpoint Security para Windows 14.1*.

Paso 10. Fin de la creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. 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 **Agregar**.

Se inicia el Asistente de tareas. 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 de forma remota**.

3. En el campo **Nombre de la tarea**, ingrese una breve descripción, por ejemplo, *Instalación de Kaspersky Endpoint Security para administradores*.

4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

Paso 2. Selección de equipos para la instalación

En este paso, seleccione los equipos en los que se instalará Kaspersky Endpoint Security de acuerdo con la opción de alcance 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 (14.1).

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 instala otra vez.

3. En el bloque **Forzar la descarga del paquete de instalación**, seleccione el método de instalación de la aplicación:

   - **Con 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 está instalado, la tarea finaliza con un error. En este caso, agregue el paquete de instalación del Agente de red a la tarea *Instalar aplicación de forma remota* y habilite la entrega de archivos a través de los recursos del sistema operativo. Luego, el Agente de red se instalará utilizando los recursos del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.

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

   - **Con los recursos del sistema operativo a través del Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante el uso de 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 simultáneas**, establezca un límite en el número de solicitudes de descarga de paquete de instalación enviadas al Servidor de administración. Un límite en 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 en el número de intentos para instalar la aplicación. Si la instalación de Kaspersky Endpoint Security finaliza con un error, la tarea iniciará automáticamente la instalación nuevamente.

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

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

8. Si es necesario, seleccione la casilla **Asignar la 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, seleccione la casilla **Solicitar a los usuarios que cierren las aplicaciones en ejecución**. La instalación de Kaspersky Endpoint Security utiliza los recursos informáticos. Para la comodidad del usuario, el Asistente de instalación de aplicaciones le solicita que cierre las aplicaciones en ejecución antes de iniciar la instalación. Esto ayuda a evitar interrupciones en el funcionamiento de otras aplicaciones y evita posibles fallos de funcionamiento de 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 hacer que, por ejemplo, una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes Servidores de Administración u otros conflictos.

Paso 4. Selección de la cuenta con la que se ejecutará la tarea

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

Paso 5. Completar creación de la tarea

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 local a través del Asistente

La interfaz del Asistente de instalación de la aplicación consiste en una secuencia de ventanas correspondiente 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 en el equipo del usuario.
2. Ejecute setup_kes.exe.

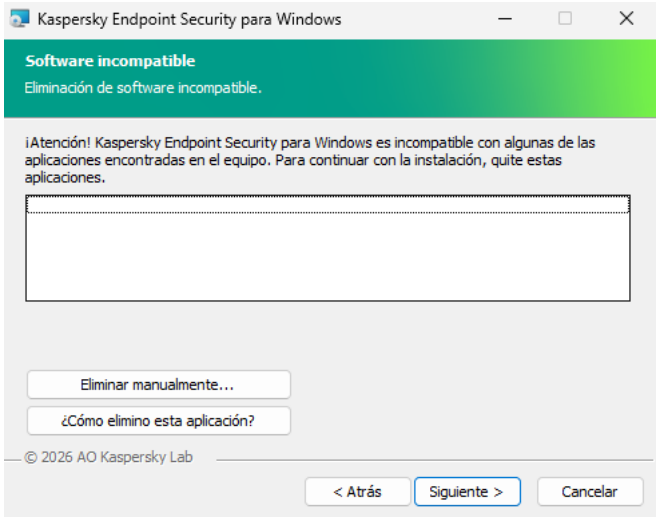
Se inicia el Asistente de instalación.

Preparativos para la instalación

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

- Compruebe si hay algún programa instalado que pueda presentar problemas de compatibilidad con Kaspersky Endpoint Security (la lista de programas se encuentra en el archivo incompatible.txt incluido en el paquete de distribución).
- Si se cumplen los requisitos de hardware y software.
- Si Microsoft .NET Framework está instalado.
- Si el usuario tiene los derechos necesarios para instalar el producto de software.

Si no se cumple alguno de los requisitos anteriores, se muestra una notificación pertinente en la pantalla. Por ejemplo, una notificación sobre software incompatible (consulte la imagen a continuación).



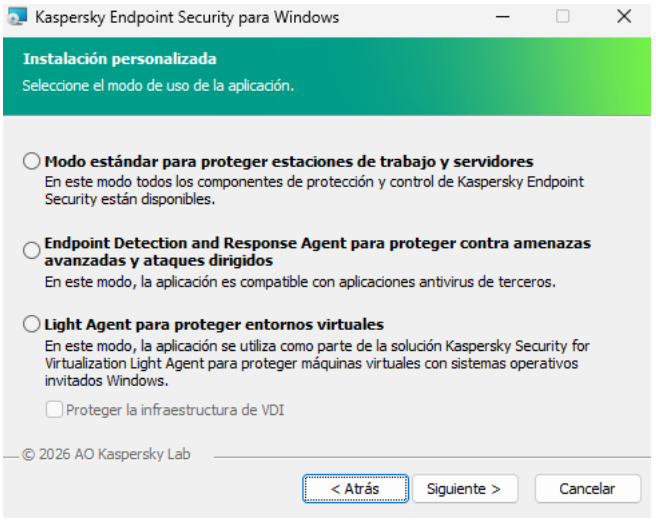
Eliminación de software incompatible

Si el equipo cumple los requisitos mencionados anteriormente, el Asistente de instalación busca las aplicaciones de Kaspersky que podrían generar conflictos de ejecutarse mientras se está instalando la aplicación. 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, los datos de activación y la configuración de la aplicación) se conservan y se usan durante la instalación de Kaspersky Endpoint Security 14.1 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 12.1 para Windows (versión 12.1.0.506)
- Kaspersky Endpoint Security 12.2 para Windows (versión 12.2.0.462)
- Kaspersky Endpoint Security 12.3 para Windows (versión 12.3.0.493)
- Kaspersky Endpoint Security 12.4 para Windows (versión 12.4.0.467)
- Kaspersky Endpoint Security 12.5 para Windows (versión 12.5.0.539)
- Kaspersky Endpoint Security 12.6 para Windows (versión 12.6.0.438)
- Kaspersky Endpoint Security 12.7 para Windows (versión 12.7.0.533)
- Kaspersky Endpoint Security 12.8 para Windows (versión 12.8.0.505)
- Kaspersky Endpoint Security 12.9 para Windows (versión 12.9.0.384)
- Kaspersky Endpoint Security 12.10 para Windows (versión 12.10.0.466)
- Kaspersky Endpoint Security 12.11 para Windows (versión 12.11.0.637)
- Kaspersky Endpoint Security 12.12 para Windows (versión 12.12.0.522)
- Kaspersky Endpoint Security 14.0 para Windows (versión 14.0.0.504)

Configuración de Kaspersky Endpoint Security



Elegir la configuración de la aplicación

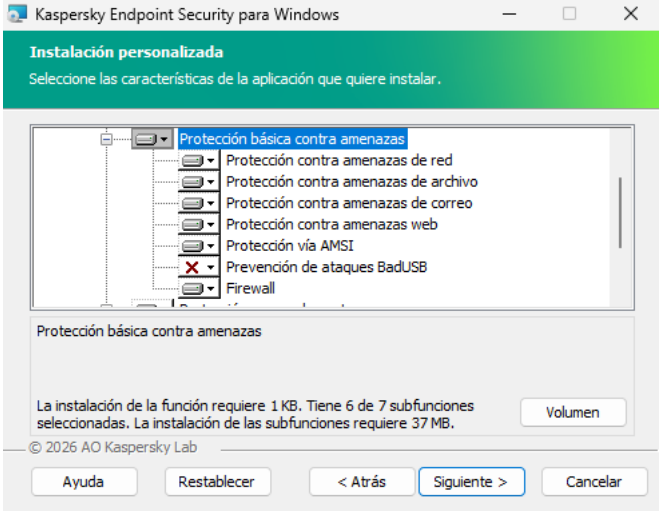
Modo estándar. La configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para las soluciones Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra una variedad de 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 Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros.

Light Agent para proteger entornos virtuales. Esta configuración está pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Componentes de Kaspersky Endpoint Security

Durante la instalación, puede seleccionar los componentes de Kaspersky Endpoint Security que desea instalar (consulte la figura a continuación). El componente Protección contra archivos peligrosos es un componente obligatorio que se debe instalar. No puede cancelar su instalación.



Selección de los componentes de la aplicación para instalar

De forma predeterminada, todos los componentes de la aplicación están seleccionados para su instalación, excepto los siguientes:

- Prevención de ataques BadUSB.
- Componentes de cifrado de datos.
- Componentes Detection and Response.

Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles. Para ello, deberá ejecutar el Asistente de instalación nuevamente y seleccionar la opción que permite cambiar los componentes disponibles.

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

- 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 solo
- 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.14.1`.

Configurar la zona de confianza

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 el modo de Light Agent para proteger entornos virtuales. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de 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.

La configuración avanzada

Configuración avanzada de la instalación de la aplicación

Proteger el proceso de instalación de la aplicación. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda deshabilitar 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.

Agregar la ruta del archivo avp.com a la variable del sistema %PATH%. Puede agregar la ruta de instalación a la variable %PATH% para facilitar el uso de la interfaz de línea de comandos.

Instalación remota de la aplicación con System Center Configuration Manager

Estas instrucciones corresponden a System Center Configuration Manager 2012 R2.

Para instalar la aplicación en forma remota con System Center Configuration Manager:

1. Abra la consola del Administrador de configuración.
2. En la parte derecha de la consola, en el bloque **Administración de aplicaciones**, seleccione **Paquetes**.
3. En la parte superior de la consola en el panel de control, haga clic en el botón **Crear paquete**.
   Se iniciará 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**, ingrese 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**, ingrese el nombre único correspondiente al paquete de instalación (por ejemplo: el nombre de la aplicación, incluida la versión).
      - En el campo **Línea de comandos**, especifique las opciones de instalación de Kaspersky Endpoint Security desde 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 el elemento **Ejecutar con derechos administrativos** seleccionado.

d. En la sección **Requisitos**:

- Seleccione la casilla **Ejecutar otro programa primero** si quiere que se inicie otra aplicación antes de instalar Kaspersky Endpoint Security.

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

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

  En la lista de abajo, seleccione las casillas que se encuentran frente a los sistema operativos en los que se instalará Kaspersky Endpoint Security.

Este paso es opcional.

e. En la sección **Resumen**, compruebe todos los valores de los parámetros ingresados y haga clic en **Siguiente**.

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

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

   Se inicia el *Asistente de implementación*.

6. En el Asistente de implementación:

   a. En la sección **General**:

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

   - En el campo **Conjunto**, ingrese el nombre del conjunto de equipos en los cuales se instalará la aplicación, seleccione el conjunto haciendo clic en el botón **Examinar**.

   b. En la sección **Contiene**, agregue puntos de distribución (para obtener información más detallada, consulte la documentación de ayuda correspondiente a System Center Configuration Manager).

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

   d. En la sección **Resumen**, compruebe todos los valores de los parámetros ingresados y haga clic en **Siguiente**.

   Una vez finalizado 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 cuando la aplicación se instala a través de la línea de comandos o al usar el Editor de directivas de grupo de Microsoft Windows. Para aplicar la configuración del archivo setup.ini, colóquelo en la misma carpeta que el paquete de distribución de Kaspersky Endpoint Security.

Utilice el archivo setup.ini solo cuando instale la aplicación en modo silencioso.

No puede agregar 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 coloca en la carpeta que contiene el kit de distribución de Kaspersky Endpoint Security. Para aplicar la configuración desde el 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 consta de las siguientes secciones:

- `[Setup]`: parámetros generales para instalar la aplicación.
- `[Components]`: selección de componentes que se instalarán con la aplicación en el modo estándar. Si no se especifica ningún componente, se instalarán todos los componentes que estén disponibles para el sistema operativo. Protección contra archivos peligrosos es un componente obligatorio y se instala en el equipo independientemente 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 ninguna tarea, se incluyen todas las tareas en 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`.

Parámetros 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 los términos del Contrato de licencia de usuario final. El texto del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Es necesario aceptar los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar su versión.

Sección	Parámetro	Descripción
	`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 la versión de la aplicación, deberá aceptar la Política de privacidad.
	`KSN`	Participar o negarse a participar en Kaspersky Security Network (KSN). Si no especifica ningún valor para este parámetro, se le preguntará si desea participar en KSN cuando inicie Kaspersky Endpoint Security por primera vez. Valores disponibles: • `1`: participar en KSN. • `0`: negarse a participar en KSN (valor predeterminado). El paquete de distribución de Kaspersky Endpoint Security está optimizado para ser utilizado con Kaspersky Security Network. Si opta por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que se haya completado la instalación.
	`CLEANERSIGNCHECK`	Verificación de firmas digitales de los archivos de software detectados presentes en la lista 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 confiable 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 es diferente según el método de instalación del software: • `0` significa que la verificación de firma digital está deshabilitada (valor predeterminado si se implementa a través de Kaspersky Security Center). • `1` significa que la verificación de firma digital está habilitada (valor predeterminado si la aplicación se instala localmente).
	`Login`	Permite definir el nombre de usuario con el que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (componente de Protección con contraseña). El nombre de usuario se configura a la par de los parámetros `Password` y `PasswordArea`. El nombre de usuario predeterminado es KLAdmin.
	`Password`	Permite definir la contraseña con la que se accederá a las funciones y a las opciones de configuración 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`	Permite especificar el alcance de la contraseña de acceso a Kaspersky Endpoint Security. Cuando un usuario intente realizar una acción que esté dentro del alcance de la contraseña, Kaspersky Endpoint Security le solicitará las credenciales (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`: deshabilitar los componentes de protección y detener las tareas de análisis. • `DISPOLICY`: deshabilitar la directiva de Kaspersky Security Center. • `UNINST`: eliminar la aplicación del equipo. • `DISCTRL`: deshabilitar los componentes de control. • `REMOVELIC`: eliminar la clave. • `REPORTS`: acceder a los informes. • `EXPORT`: exportar configuración de la aplicación. Por ejemplo, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Habilitar o deshabilitar el mecanismo para proteger la instalación de la aplicación. Valores disponibles: • `1`: habilitar el mecanismo para proteger la instalación (valor predeterminado). • `0`: deshabilitar el mecanismo para proteger la instalación. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda deshabilitar la protección del proceso de instalación.

Sección	Parámetro	Descripción
	`PROTECTOSSERVICES`	Funcionalidad de protección de los servicios del sistema operativo. La protección de los servicios del sistema operativo impide que las aplicaciones de terceros interfieran con el funcionamiento de los servicios del sistema operativo. Estos servicios incluyen, entre otros, el inicio automático de las aplicaciones. • `1` significa que la protección de los servicios del sistema operativo está habilitada (valor predeterminado). • `0` significa que la protección de los servicios del sistema operativo está deshabilitada.
	`EnableAzureSupport`	Habilitar o deshabilitar el modo de compatibilidad de Azure WVD. Valores disponibles: • `1` – El modo de compatibilidad de Azure WVD está habilitado. • `0` – El modo de compatibilidad de Azure WVD está deshabilitado (valor predeterminado). Esta función garantiza la correcta visualización del estado de la máquina virtual Azure en la consola de Kaspersky Anti Targeted Attack Platform. Para monitorear el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores de KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar una Sensor ID única y permanente a estas máquinas virtuales. Si el modo de compatibilidad está desactivado, la Sensor ID puede cambiar después de reiniciar el equipo debido a cómo funcionan las máquinas virtuales de Azure. Esto puede hacer que aparezcan duplicados de máquinas virtuales en la consola.
	`Reboot`	Permitir que el equipo se reinicie automáticamente, de ser necesario, cuando la aplicación termine de instalarse o actualizarse. Si no especifica ningún valor para este parámetro, se bloquea el reinicio automático del equipo. No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación.
	`AddEnvironment`	Agregar a la variable del sistema %PATH% la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security. Valores disponibles: • `1`: la variable del sistema %PATH% se complementará con la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security. • `0`: la variable del sistema %PATH% no se complementará con la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security.
	`AMPPL`	Habilitar o deshabilitar el uso de la tecnología AM-PPL (Antimalware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019. Valores disponibles: • `1`: los procesos de Kaspersky Endpoint Security se protegerán con la tecnología AM-PPL. • `0`: los procesos de Kaspersky Endpoint Security no se protegerán con la tecnología AM-PPL.
	`UPGRADEMODE`	Modo de actualización de la aplicación: • `Seamless` significa actualizar la aplicación con un reinicio del equipo (valor predeterminado). • `Force` significa actualizar la aplicación sin reiniciar. Puede actualizar la aplicación sin reiniciar el equipo a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo. También puede instalar parches sin reiniciar el equipo a partir de la versión 11.11.0. No es necesario reiniciar al instalar Kaspersky Endpoint Security. Así, el modo de actualización se especificará en la configuración de la aplicación. Puede cambiar este parámetro en la configuración de la aplicación o en la directiva. Cuando se actualiza una aplicación ya instalada, la prioridad del parámetro especificado en el archivo setup.ini es mayor 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 y se establece el modo `Seamless` en la configuración de la aplicación, la actualización se instalará sin un reinicio (`Force`). Si utiliza el archivo setup.ini en el que no se especifica el parámetro `UPGRADEMODE`, el instalador utilizará el valor predeterminado (`Seamless`) e instalará la actualización con el reinicio del equipo.
	`SetupReg`	Grabar las claves del archivo setup.reg en el Registro. Para que esto ocurra, el parámetro `SetupReg: setup.reg` debe tener el valor setup.reg.

Sección	Parámetro	Descripción
	`EnableTraces`	Habilitar o deshabilitar el seguimiento de la aplicación. Una vez que se inicia Kaspersky Endpoint Security, guarda los archivos de seguimiento en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Valores disponibles: • `1`: la función de seguimiento está habilitada. • `0`: la función de seguimiento está deshabilitada (valor predeterminado).
	`TracesLevel`	Nivel de detalle de los archivos de seguimiento. Valores disponibles: • `100` (crítico). Solo mensajes sobre errores graves. • `200` (alto). Mensajes sobre todos los errores, incluidos los 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. Si desea administrar la aplicación mediante REST API, deberá configurar el parámetro `RESTAPI_User` para especificar el nombre de usuario. Valores disponibles: • `1`: la aplicación podrá administrarse a través de la API REST. • `0`: la aplicación no podrá administrarse a través de la API REST (valor predeterminado). Si desea administrar la aplicación mediante REST API, debe permitir el uso de sistemas de administración. Para ello, defina el parámetro `AdminKitConnector=1`. Si opta por utilizar la API REST, no podrá usar los sistemas de administración de Kaspersky para controlar la aplicación.
	`RESTAPI_User`	Nombre de usuario de la cuenta de dominio de Windows que se usará para administrar la aplicación a través de la API REST. Solo este usuario podrá administrar la aplicación con la API REST. El nombre de usuario debe especificarse en formato `<DOMAIN>\<UserName>` (por ejemplo, `RESTAPI_User=COMPANY\Administrator`). El uso de la API REST está limitado a un único usuario. Especificar este valor es requisito indispensable para administrar la aplicación a través de la API REST.
	`RESTAPI_Port`	Puerto que se usará 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 reconocer solicitudes (por ejemplo, `RESTAPI_Certificate=C:\cert.pem`). La interacción segura de Kaspersky Endpoint Security con el cliente de REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga 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 admitir 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 admite otros componentes de la aplicación. Valores disponibles: • `1` para instalar la aplicación en modo agente EDR. • `0` para instalar la aplicación en Modo estándar (predeterminado).
	`KSVLAMode`	Instalar la aplicación en el modo de Light Agent. Esta configuración está pensada para 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).

Sección	Parámetro	Descripción
	`InstallOnVDI`	Habilitación del modo de protección VDI al instalar la aplicación en el modo de Light Agent (`KSVLAMode=1`). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas. Valores disponibles: • `1` para habilitar el modo de protección VDI. • `0` para deshabilitar el modo de protección VDI (predeterminado).
	`KESExclusions`	Agregar exclusiones de análisis y aplicaciones de confianza predefinidas al instalar la aplicación en el servidor. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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` habilita exclusiones de análisis y aplicaciones de confianza predefinidas. • `0` deshabilita exclusiones de análisis y aplicaciones de confianza predefinidas (predeterminado).
	`LAExclusions`	Agregar exclusiones de análisis y aplicaciones de confianza predefinidas al instalar la aplicación en una máquina virtual (modo de Light Agent). Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de Citrix y VMware. Valores disponibles: • `1` habilita exclusiones de análisis y aplicaciones de confianza predefinidas. • `0` deshabilita exclusiones de análisis y aplicaciones de confianza predefinidas (predeterminado).
	`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 madre. En algunos casos, por ejemplo, cuando se utiliza 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 cual se envía la telemetría. Para crear un Sensor ID único, debe configurar 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 garantiza un Sensor ID único. De manera predeterminada, el parámetro no está establecido. 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, 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`	Instalar todos los componentes. Si el valor del parámetro es `1`, se instalarán todos los componentes, sin que se tenga en cuenta la configuración de instalación de cada componente individual. Debido a la forma en que se gestionan las soluciones de detección y respuesta, 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 contra amenazas de correo.
	`WebThreatProtection`	Protección contra amenazas web.
	`AMSI`	Protección vía AMSI.
	`HostIntrusionPrevention`	Prevención de intrusiones en el host

Sección	Parámetro	Descripción
	`BehaviorDetection`	Detección de comportamiento.
	`ExploitPrevention`	Prevención de exploits.
	`RemediationEngine`	Motor de reparación.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Protección contra amenazas de 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`	Anticifrador
	`FileThreatProtection`	Protección contra archivos peligrosos.
	`SystemIntegrityMonitor`	Control de integridad del sistema.
	`FileEncryption`	Bibliotecas de cifrado de archivos.
	`DiskEncryption`	Bibliotecas de cifrado de disco completo.
	`MSBitLocker`	Bibliotecas de administración del cifrado BitLocker.
	`BadUSBAttackPrevention`	Prevención de ataques BadUSB.
	`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 Kaspersky Detection and Response. *KATA Sandbox* es un componente de la solución Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response

Sección	Parámetro	Descripción
	`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`	Permitir que la aplicación se administre a través de un sistema de administración. Kaspersky Security Center es uno de esos sistemas. Además de los sistemas de administración de Kaspersky, es posible utilizar soluciones de terceros. La API de Kaspersky Endpoint Security se ha diseñado para ello. Valores disponibles: • `1` : la aplicación podrá administrarse a través de un sistema de administración (valor predeterminado). • `0` : la aplicación podrá administrarse únicamente a través de su interfaz local.
	`KUMAIntegration`	Integración con KUMA.
	`StandaloneKATA`	Instalación de la aplicación en el modo de Endpoint Detection and Response Agent (EDR Agent) para integrar con Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Instalación de la aplicación en el modo de Endpoint Detection and Response Agent (EDR Agent) para integrar con Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalación de la aplicación en el modo de Endpoint Detection and Response Agent (EDR Agent) para integrar con Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalación de la aplicación en el modo de Endpoint Detection and Response Agent (EDR Agent) para integrar con KUMA.
`[Tasks]`	`ScanMyComputer`	Tarea de Análisis completo. Valores disponibles: • `1` : incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0` : no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.
	`ScanCritical`	Tarea de Análisis de áreas críticas. Valores disponibles: • `1` : incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0` : no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.
	`Updater`	Tarea de actualización. Valores disponibles: • `1` : incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0` : no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.

Cambiar componentes de la aplicación

Los componentes que estarán disponibles en la aplicación pueden seleccionarse al momento de instalarla. Tras la instalación, el conjunto de componentes puede modificarse de dos maneras:

- De manera local, utilizando el Asistente de instalación.

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

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

- De manera remota, a través de Kaspersky Security Center.

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

Si planea cambiar los componentes de la aplicación, tenga en cuenta lo siguiente:

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

- Si los discos duros del equipo están protegidos con la característica de cifrado de disco completo (FDE), no podrá eliminar el componente de cifrado de disco completo. Si necesita eliminar este componente, primero deberá descifrar todos los discos duros del equipo.

- Si el equipo contiene archivos cifrados (FLE) o el usuario utiliza unidades extraíbles cifradas (FDE o FLE) y usted elimina los componentes de cifrado de datos, ya no será posible acceder a esos archivos y unidades. Para recuperar el acceso, deberá reinstalar los componentes de cifrado de datos.

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

Cómo agregar o eliminar componentes de la 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Seleccionar componentes para instalar**.

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

Seleccione la configuración de la aplicación:

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

- **Endpoint Detection and Response Agent para proteger contra amenazas avanzadas y ataques dirigidos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros.

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

- **Light Agent para proteger entornos virtuales**. Esta configuración está pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

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

Paso 3. La configuración avanzada

Defina la configuración avanzada para 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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 5. Programación de la tarea

Programe la ejecución de la tarea. La tarea puede iniciarse manualmente o cuando el equipo está inactivo, por ejemplo.

Paso 6. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Agregar el componente Control de aplicaciones*.

Paso 7. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo agregar o eliminar componentes de 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 **Agregar**.

Se inicia el Asistente de tareas. 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 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, *Agregar el componente Control de aplicaciones*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione 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 ejecutará la tarea. Por ejemplo, seleccione un grupo de administración separado o cree una selección.

Paso 3. Completar creación de la tarea

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

En Propiedades de la 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**. La configuración predeterminada. Esta configuración le permite utilizar todos los componentes de la aplicación, incluidos los componentes que brindan soporte para las soluciones Detection and Response. Esta configuración se utiliza para una protección integral del equipo contra una variedad de amenazas, ataques de red y fraudes.

- **Endpoint Detection and Response Agent para proteger contra amenazas avanzadas y ataques dirigidos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros.

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

- **Light Agent para proteger entornos virtuales**. Esta configuración está pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

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

El conjunto de componentes de Kaspersky Endpoint Security se modificará en los equipos de los usuarios de manera silenciosa. 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 deshabilitados, y sus opciones de configuración no estarán disponibles.

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

Parámetro	Descripción
Configuración de la tarea	**Comprobar si hay aplicaciones incompatibles de terceros**. De manera predeterminada, Kaspersky Endpoint Security comprueba la compatibilidad de las aplicaciones instaladas. La lista del software que podría generar problemas de compatibilidad se encuentra en el archivo incompatible.txt. El archivo está incluido en el kit de distribución. Si está habilitado el análisis de software instalado, al detectar una aplicación de la lista, Kaspersky Endpoint Security detiene la tarea. Puede deshabilitar el análisis de software instalado si la documentación del proveedor del software externo afirma ser compatible con Endpoint Protection Platform (EPP). **Eliminar aplicaciones incompatibles de terceros**. Eliminación automática de las aplicaciones que figuran en el archivo incompatible.txt antes de cambiar el conjunto de componentes. Si se habilita esta funcionalidad, Kaspersky Endpoint Security intenta eliminar las aplicaciones que podrían causar problemas de compatibilidad a fin de poder continuar con la tarea. **Utilizar el modo de compatibilidad de Azure WVD**. Esta función garantiza la correcta visualización del estado de la máquina virtual Azure en la consola de Kaspersky Anti Targeted Attack Platform. Para monitorear el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores de KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar una Sensor ID única y permanente a estas máquinas virtuales. Si el modo de compatibilidad está desactivado, la Sensor ID puede cambiar después de reiniciar el equipo debido a cómo funcionan 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 aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 el modo de Light Agent para proteger entornos virtuales. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de 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 separado/Modo combinado	Puede crear conjuntos de componentes independientes para estaciones de trabajo y servidores: **Modo separado**. Antes de implementar el paquete de instalación, el instalador detecta el tipo de sistema operativo e instala solo los componentes de la aplicación que seleccionó para ese tipo de sistema operativo. De esta manera, puede usar 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 estaciones de trabajo y un paquete de instalación independiente para 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 habilitar la protección con contraseña para restringir el acceso a Kaspersky Endpoint Security. Es decir, para modificar la selección de componentes de la aplicación, debe ingresar credenciales de un usuario que tenga permiso para **Eliminar, modificar o restaurar la aplicación**. Por ejemplo, puede utilizar la cuenta KLAdmin.
Utilice la contraseña para desinstalar el servidor Kaspersky Endpoint Agent y Kaspersky Security for Windows Server	Los administradores suelen habilitar 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 incorporado], o si está migrando de KSWS a KES, debe ingresar una contraseña para eliminar estas aplicaciones.

Actualización de una versión más antigua de la aplicación

Si planea actualizar la aplicación a una versión más nueva, tenga en cuenta lo siguiente:

- La localización de la nueva versión de Kaspersky Endpoint Security debe coincidir con la localización de la versión instalada de la aplicación. Si las localizaciones de las aplicaciones no coinciden, la actualización de la aplicación se completará con un error.
- 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 pudiese bloquear, no se iniciaría la actualización de la instalación. El cifrado de disco completo se desbloqueará una vez que concluya la actualización.

Puede actualizar las siguientes versiones de Kaspersky Endpoint Security:

- Kaspersky Endpoint Security 12.1 para Windows (versión 12.1.0.506)
- Kaspersky Endpoint Security 12.2 para Windows (versión 12.2.0.462)
- Kaspersky Endpoint Security 12.3 para Windows (versión 12.3.0.493)
- Kaspersky Endpoint Security 12.4 para Windows (versión 12.4.0.467)
- Kaspersky Endpoint Security 12.5 para Windows (versión 12.5.0.539)
- Kaspersky Endpoint Security 12.6 para Windows (versión 12.6.0.438)
- Kaspersky Endpoint Security 12.7 para Windows (versión 12.7.0.533)
- Kaspersky Endpoint Security 12.8 para Windows (versión 12.8.0.505)
- Kaspersky Endpoint Security 12.9 para Windows (versión 12.9.0.384)
- Kaspersky Endpoint Security 12.10 para Windows (versión 12.10.0.466)
- Kaspersky Endpoint Security 12.11 para Windows (versión 12.11.0.637)
- Kaspersky Endpoint Security 12.12 para Windows (versión 12.12.0.522)
- Kaspersky Endpoint Security 14.0 para Windows (versión 14.0.0.504)

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

Métodos de actualización de aplicaciones

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

- Mediante el servicio de actualización de Kaspersky (Seamless Update – SMU).
- de manera local, utilizando el Asistente de instalación;
- de manera local, utilizando la línea de comandos;
- de manera remota, a través de Kaspersky Security Center;
- de manera 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 manera remota, utilizando System Center Configuration Manager.

Si la aplicación se instaló en la red corporativa con una selección de componentes diferente de la predeterminada, tendrá que atender a ciertas diferencias dependiendo de si va a actualizar la aplicación a través de la Consola de administración (MMC), por un lado, o con Web Console o Cloud Console, por el otro. Cuando vaya a actualizar Kaspersky Endpoint Security, tenga en cuenta lo siguiente:

- Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console.

  La selección de componentes disponibles en el equipo del usuario no se modificará si crea un paquete de instalación para la versión nueva con la selección de componentes predeterminada. Si desea que Kaspersky Endpoint Security ofrezca la selección de componentes predeterminada, abra las propiedades del paquete de instalación, cambie la selección de componentes, restaure la selección de componentes original y guarde los cambios.

- la Consola de administración de Kaspersky Security Center,

  Al completarse la actualización, la selección de componentes disponibles en la aplicación será la indicada por el paquete de instalación. Ello quiere decir que si la nueva versión tiene la selección de componentes predeterminada, el componente Prevención de ataques BadUSB (por citar un ejemplo) se eliminará, ya que no forma parte de la instalación estándar. Para que la selección de componentes no se modifique tras la actualización, asegúrese de seleccionar los componentes que vaya a necesitar en la configuración del paquete de instalación.

Actualización de la aplicación sin reiniciar el equipo

La actualización de la aplicación sin reiniciar el equipo ofrece un funcionamiento ininterrumpido del servidor cuando se actualiza la versión de la aplicación.

La actualización de la aplicación sin reinicio tiene las siguientes limitaciones:

- Puede actualizar la aplicación sin reiniciar el equipo a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo.

- Puede instalar parches sin reiniciar el equipo a partir de la versión 11.11.0. Para instalar parches en versiones anteriores de la aplicación, es posible que sea necesario reiniciar el equipo.

- La actualización de la aplicación sin reiniciar no está disponible en equipos con cifrado de datos habilitado (cifrado de Kaspersky [FDE], BitLocker, cifrado de archivos [FLE]). Para actualizar la aplicación en equipos con cifrado de datos habilitado, debe reiniciar el equipo.

- La aplicación no se puede actualizar en una máquina virtual sin reiniciarla. Para mejorar 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 restaurarla, Kaspersky Endpoint Security se reinicia para comenzar a usar la nueva versión. El reinicio de Kaspersky Endpoint Security puede tardar hasta un minuto. Durante este tiempo, el nivel de protección del equipo se reduce. Tras reiniciar la aplicación, se restablecerá el nivel de protección del equipo.

Cómo seleccionar el modo de actualización de la aplicación 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 ficha **Configuración de la aplicación**.

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

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

6. Guarde los cambios.

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

2. Seleccione la directiva correspondiente 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**.

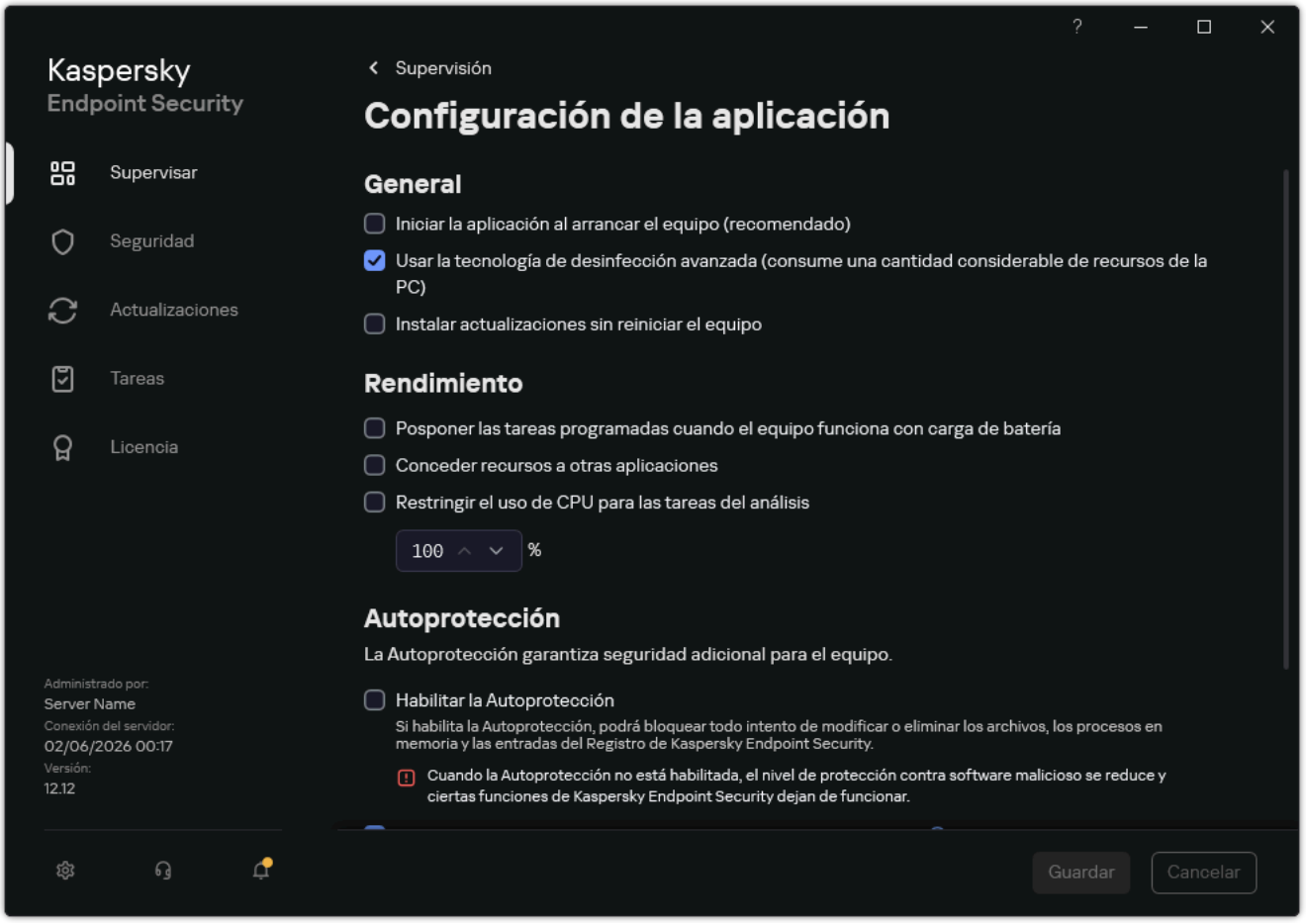
4. En el bloque **Configuración avanzada**, seleccione o desmarque la casilla **Instalar las actualizaciones de la aplicación sin reiniciar** para configurar el modo de actualización de la aplicación.

5. Guarde los cambios.

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

1. En la ventana principal de la aplicación 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 desmarque la casilla **Instalar actualizaciones sin reiniciar el equipo** para configurar el modo de actualización de la aplicación.

4. Guarde los cambios.

Una vez que finalice el procedimiento de actualización de la aplicación sin reiniciar, la nueva versión de Kaspersky Endpoint Security se habrá instalado 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 mediante el informe de la versión de la aplicación de Kaspersky en la consola de Kaspersky Security Center.

Actualización SMU de la aplicación

Para actualizar la aplicación usando 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 recibe la nueva versión de la aplicación junto con las bases de datos antivirus del mismo origen.

Una actualización de SMU permite actualizar la aplicación a la última versión en todos los equipos de la organización. 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 con el Asistente de configuración). No puede seleccionar equipos específicos al realizar una actualización de SMU.

El personal de Kaspersky determina el cronograma de actualizaciones de la aplicación. Para asegurarse de que la nueva versión de la aplicación se ejecute sin problemas, Kaspersky ofrece actualizaciones por etapas. 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 con la tarea *Actualización de 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 bases de datos y módulos de la aplicación*. Además, en la configuración de la tarea *Actualización de bases de datos y módulos de la aplicación*, puede permitir la actualización de la aplicación sin necesidad de reiniciarlo.

Pasos de una actualización de SMU de la aplicación

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

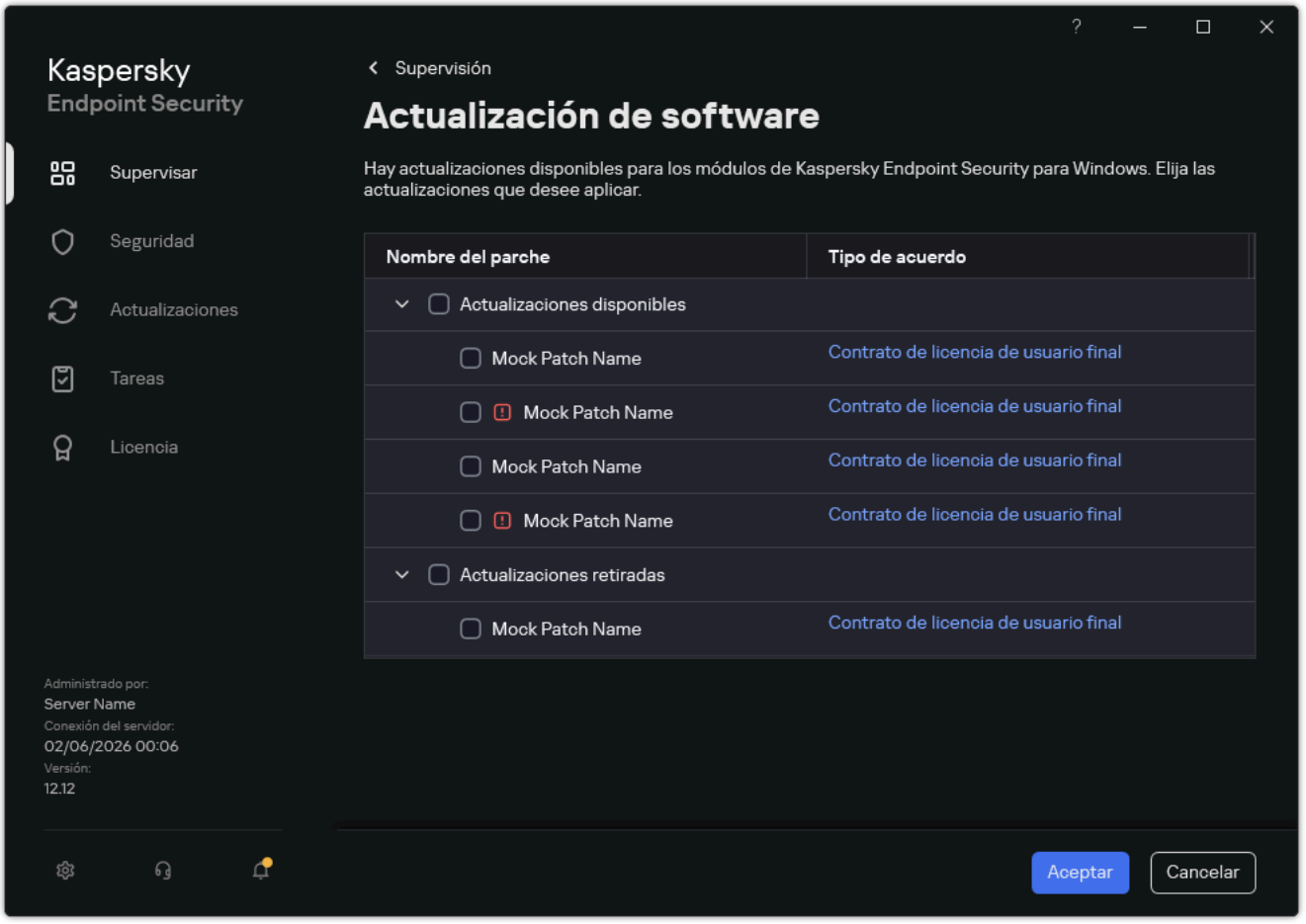
2. **El usuario debe aprobar la actualización de la aplicación.**

   Si el equipo está conectado a Kaspersky Security Center, la actualización estará disponible en Kaspersky Security Center, en la sección **Actualización de bases de datos y 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 estará 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 imagen siguiente).

3. **Kaspersky Endpoint Security ejecuta la tarea *Actualización de bases de datos y módulos de la aplicación* según la programación configurada.**

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 el equipo y los datos del usuario sin protección contra amenazas.

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

Eliminación remota de la aplicación a través de Kaspersky Security Center

Para desinstalar la aplicación a distancia, puede utilizar la tarea *Desinstalar aplicación de forma remota*. 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 desinstalar 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Servidor de administración de Kaspersky Security Center** → **Avanzado** → **Desinstalar aplicación de forma remota**.

Paso 2. Selección del programa que se desinstalará

Seleccione **Desinstalar aplicación admitida por Kaspersky Security Center**.

Paso 3. Configuración de la tarea para desinstalar la aplicación

Seleccione **Kaspersky Endpoint Security para Windows (14.1)**.

Paso 4. Configuración de la utilidad de desinstalación

Configure los siguientes parámetros adicionales:

- **Forzar la descarga de la utilidad de desinstalación**. Indique cómo se distribuirá la utilidad:
  - **Con el Agente de red**. Si el Agente de red no se ha instalado en la equipo, el primer Agente de red se instalará utilizando las herramientas del sistema operativo. Kaspersky Endpoint Security se desinstalará entonces con las herramientas del Agente de red.
  - **Con los recursos del sistema operativo a través del 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.
  - **Con los recursos del sistema operativo a través de los 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 hay al menos un punto de distribución en la red. Para obtener más información sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.
- **Verificar el tipo de sistema operativo antes de la descarga**. De ser necesario, desactive esta casilla. 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 con los requisitos del software, puede omitir esta verificación.

Si había definido una contraseña para desinstalar la aplicación, haga lo siguiente:

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

Paso 5. Seleccionar la opción de reinicio del sistema operativo

Cuando concluya la desinstalación, el equipo deberá reiniciarse. Elija 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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 7. Selección de la cuenta con la que se ejecutará la tarea

Seleccione la cuenta para instalar el Agente de red utilizando las herramientas del sistema operativo. En este caso, se requieren derechos de administrador para acceder al equipo. Puede agregar varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación usa 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. Programación de la tarea

Programe la ejecución de la tarea. La tarea puede iniciarse manualmente o cuando el equipo está inactivo, por ejemplo.

Paso 9. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Eliminar Kaspersky Endpoint Security 14.1*.

Paso 10. Fin de la creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

La aplicación se desinstalará en modo silencioso.

Cómo desinstalar 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 **Agregar**.

Se inicia el Asistente de tareas. 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 de forma remota**.

3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Desinstalar Kaspersky Endpoint Security de los equipos del Servicio de soporte técnico*).

4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione 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 ejecutará la tarea. Por ejemplo, seleccione un grupo de administración separado 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 la aplicación administrada**.

2. Seleccione **Kaspersky Endpoint Security para Windows**.

3. **Forzar la descarga de la utilidad de desinstalación**. Indique cómo se distribuirá la utilidad:

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

   - **Con los recursos del sistema operativo a través del 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.

   - **Con los recursos del sistema operativo a través de los 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 hay al menos un punto de distribución en la red. Para obtener más información sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

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

5. En el campo **N.° 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, anule la selección de la casilla **Verificar el tipo de sistema operativo antes de la descarga**. 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 con los requisitos del software, puede omitir esta verificación.

Paso 4. Selección de la cuenta con la que se ejecutará la tarea

Seleccione la cuenta para instalar el Agente de red utilizando las herramientas del sistema operativo. En este caso, se requieren derechos de administrador para acceder al equipo. Puede agregar varias cuentas. Si una cuenta no tiene suficientes derechos, el Asistente de instalación usa 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. Completar creación de la tarea

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 usar la contraseña de la cuenta KLAdmin en la tarea Desinstalar aplicación de forma remota:

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 **Desinstalar aplicación de forma remota** de Kaspersky Security Center.

   Se abre la ventana de propiedades de la tarea.

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

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

5. Escriba la contraseña de la cuenta KLAdmin.

6. Guarde los cambios.

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

Eliminación remota de la aplicación a través de Active Directory

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

Si había definido una contraseña para desinstalar la aplicación, haga 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. Para determinar cuál es este identificador, consulte la Base de conocimientos del Servicio de soporte técnico o utilice el siguiente comando:

   ```
   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.

Eliminación local de la aplicación

También 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 inicia 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 elimina completamente (consulte la figura a continuación).

Guardado de datos después de la eliminación

Puede guardar los siguientes datos:

- **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 agregará una clave de licencia automáticamente.

- **Archivos de Copias de seguridad**. Estos son los archivos que la aplicación analizó y guardó en el depósito Copias de seguridad.

A los archivos de Copias de seguridad que se guardan después de eliminar la aplicación se puede acceder solo desde la misma versión de la aplicación que se usó para guardar dichos archivos.

Si planea utilizar los objetos de Copias 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 de operación 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 los datos en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

También puede eliminar la aplicación de manera local mediante el uso de la línea de comandos.

Licencia de la aplicación

En esta sección, se proporciona información sobre 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 acuerdo vinculante entre usted y AO Kaspersky Lab en el que se establecen las condiciones bajo las cuales podrá utilizar la aplicación.

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

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

- Instalando Kaspersky Endpoint Security en modo interactivo.
- Cuando se lee el archivo license.txt. El documento forma parte del kit de distribución de la aplicación. También lo encontrará en la carpeta de instalación del programa, `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Al confirmar que está de acuerdo con el Contrato de licencia de usuario final al instalar la aplicación, usted indica que acepta los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe anular la instalación.

Acerca de la licencia

Una *licencia* es un derecho con límite de tiempo para usar la aplicación, que se otorga conforme al Contrato de licencia de usuario final.

La licencia le permite utilizar la aplicación según los términos del Acuerdo de licencia de usuario final y recibir soporte técnico. La lista de funciones disponibles y el período de uso de la aplicación depende del tipo de licencia que se usó para activar la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Prueba*: licencia gratuita diseñada para la prueba de la aplicación.

  Usualmente, una licencia de prueba tiene un plazo corto. Cuando la licencia de prueba se vence, se deshabilitan todas las características de Kaspersky Endpoint Security. Para continuar usando la aplicación, debe comprar una licencia comercial.

  La aplicación no puede activarse con una licencia de prueba más de una vez. La aplicación no se puede activar con una licencia de prueba después de que se haya activado con una licencia comercial.

- *Comercial:* licencia paga que se entrega cuando adquiere Kaspersky Endpoint Security.

  La funcionalidad de la aplicación disponible bajo una licencia comercial depende de la elección del producto. El producto seleccionado se indica en el Certificado de licencia. Se puede encontrar información sobre productos disponibles en el sitio web de Kaspersky.

Cuando la licencia comercial caduca, las funciones clave de la aplicación quedan deshabilitadas. Para seguir utilizando la aplicación, debe renovar su licencia comercial. Si no tiene previsto renovar la licencia, debe eliminar la aplicación del equipo.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se le transfiere al usuario con un archivo de clave o un código de activación.

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

- Id. de licencia o número de pedido,
- detalles del usuario a quien se le ha otorgado la licencia,
- detalles de la aplicación que se puede activar con la licencia,
- límite de unidades con licencia (por ejemplo, la cantidad de dispositivos en los cuales se puede usar la aplicación con la licencia),
- fecha de inicio del plazo de licencia,
- plazo de licencia o fecha de caducidad de la licencia,
- tipo de licencia.

Acerca de la suscripción

Una *suscripción a Kaspersky Endpoint Security* es una orden de compra para obtener la aplicación, con parámetros específicos (como fecha de caducidad de la suscripción y cantidad de dispositivos protegidos). Puede solicitar una suscripción a Kaspersky Endpoint Security a su proveedor de servicios (como su proveedor de servicios de Internet, o ISP). Puede renovar una suscripción en forma manual o automática, o puede cancelar su suscripción. Para administrar su suscripción, utilice el sitio web de su proveedor de servicios.

La suscripción puede ser limitada (por un año, por ejemplo) o ilimitada (sin fecha de caducidad). Si su suscripción es limitada, deberá renovarla una vez que caduque para que Kaspersky Endpoint Security continúe funcionando. La suscripción ilimitada se renueva en forma automática si los servicios del proveedor se han pagados por adelantado a tiempo.

Cuando una suscripción limitada caduca, le pueden proporcionar un período de gracia de renovación de la suscripción durante el cual la aplicación continuará funcionando. La disponibilidad y la duración del período de gracia son decisión del proveedor de servicios.

Para utilizar Kaspersky Endpoint Security con una suscripción, aplique el código de activación que le habrá enviado el proveedor de servicios. Una vez que aplique el código de activación, se agregará una clave activa. La clave activa determina con qué licencia operará la aplicación en el marco de la suscripción. No puede activar la aplicación en la suscripción utilizando un archivo de clave. El proveedor de servicios puede ofrecer un solo código de activación. No es posible agregar una clave de reserva en la modalidad de suscripción.

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

Acerca de la clave de licencia

La *clave de licencia* es una secuencia de bits que permite activar la aplicación y luego utilizarla en el marco del Contrato de licencia de usuario final.

Las claves que se agregan como parte de una suscripción no están acompañadas de un certificado de licencia.

Para agregar una clave de licencia a la aplicación, puede aplicar un archivo de clave o ingresar un código de activación.

Kaspersky puede bloquear la clave si se infringe el Contrato de licencia de usuario final. Si su clave se bloquea y desea seguir utilizando la aplicación, deberá agregar una clave diferente.

Existen dos tipos de claves: activa y de reserva.

Una *clave activa* es una clave que la aplicación utiliza actualmente. Una clave de prueba o licencia comercial puede agregarse como una clave activa. La aplicación no puede tener más de una clave activa.

Una *clave de reserva* es una clave que no se está utilizando en un momento dado, pero que confiere el derecho de usar la aplicación. La clave de reserva se activa automáticamente cuando la clave activa caduca. Para poder agregar una clave de reserva, es necesario que haya una clave activa disponible.

Solo se puede agregar una clave para una licencia de prueba como una clave activa. Tales claves no se pueden agregar como reserva. Una clave de licencia de prueba no puede reemplazar a la clave activa de una licencia comercial.

Si se agrega 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 agregado a la lista de claves prohibidas. Transcurridos los ocho días, la funcionalidad se limita al nivel disponible cuando caduca una licencia. Puede usar los componentes de protección y control y ejecutar un análisis usando las bases de datos de la aplicación que se instalaron antes de que la licencia expirara. La aplicación también sigue cifrando los archivos que se modificaron y se cifraron antes del vencimiento de la licencia, pero no cifra archivos nuevos. No está disponible el uso de Kaspersky Security Network.

Acerca del código de activación

Un *código de activación* es una secuencia única formada por 20 caracteres alfanuméricos. Cuando se introduce un código de activación, se agrega una clave de licencia con la cual se activa Kaspersky Endpoint Security. Recibirá un código de activación en la dirección de correo electrónico que indique al momento de comprar Kaspersky Endpoint Security.

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

Si utiliza un código de activación para activar la aplicación, se agregará una clave activa. Para agregar una clave de reserva, también deberá usar un código de activación; los archivos de clave no pueden usarse para este fin.

Si perdió un código de activación después activar la aplicación, puede restaurarlo. Podría necesitarlo para ciertos fines (por ejemplo, para registrarse en Kaspersky CompanyAccount). Si se perdió el código de activación después de la activación de la aplicación, comuníquese con el partner de Kaspersky al que le compró la licencia.

Acerca del archivo de clave

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

Kaspersky le enviará un archivo de clave a la dirección de correo electrónico que indique 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 de clave.

Puede recuperar el archivo de clave si se ha eliminado por error. Es posible que necesite un archivo de clave para registrarse en Kaspersky CompanyAccount, por ejemplo.

Para recuperar un archivo de clave, lleve a cabo una de las siguientes acciones:

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

Cuando la aplicación se activa con un archivo de clave, se agrega una clave activa. Para agregar una clave de reserva, también es necesario usar un archivo de clave; los códigos de activación no son válidos para este fin.

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

Para ver una comparación de las funcionalidades de la aplicación según el tipo de licencia de Kaspersky Next, consulte Ayuda de Kaspersky Next.

Comparación de las características de Kaspersky Endpoint Security

Característica	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 avanzada contra amenazas								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓	✓	✓
Anticifrador	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	✓	✓	✓	✓	✓	✓
Motor de reparación	✓	✓	✓	✓	✓	✓	✓	✓
Protección básica contra amenazas								
Protección contra amenazas de archivo	✓	✓	✓	✓	✓	✓	✓	✓
Protección contra amenazas web	✓	✓	✓	✓	✓	✓	✓	✓
Protección contra amenazas de correo	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de ataques BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protección vía 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								

Característica	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 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 debe comprarse por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Integración con KUMA *(la licencia para la integración con KUMA debe comprarse por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo de Light Agent *(para activar la aplicación, debe agregar 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

Para ver una comparación de las funcionalidades de la aplicación según el tipo de licencia de Kaspersky Next, consulte Ayuda de Kaspersky Next.

Característica	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 avanzada contra amenazas								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓	✓	✓
Anticifrador	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de intrusiones en el host	–	–	–	–	–	–	–	–
Motor de reparación	✓	✓	✓	✓	✓	✓	✓	✓
Protección básica contra amenazas								
Protección contra amenazas de archivo	✓	✓	✓	✓	✓	✓	✓	✓
Protección contra amenazas web	–	✓	✓	✓	✓	✓	✓	✓
Protección contra amenazas de correo	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓	✓	✓	✓	✓	✓
Prevención de ataques BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protección vía 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	–	–	–	–	–	–	–	–

Característica	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 debe comprarse por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Integración con KUMA *(la licencia para la integración con KUMA debe comprarse por separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo de Light Agent *(para activar la aplicación, debe agregar 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. Para activar la aplicación, se debe agregar una clave de licencia.

Puede activar la aplicación de las siguientes maneras:

- Localmente, desde la interfaz de la aplicación, mediante el Asistente de activación. Si utiliza este método, podrá agregar tanto una clave activa como una de reserva.
- De forma remota usando el paquete de software de Kaspersky Security Center.
  - Usando la tarea *Agregar clave*.

    Este método puede usarse para agregar una clave tanto en un equipo específico como en una serie de equipos pertenecientes a un grupo de administración. Si utiliza este método, podrá agregar tanto una clave activa como una de reserva.
  - Distribuyendo a los equipos una clave almacenada en el Servidor de administración de Kaspersky Security Center.

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

Se distribuye primero el código de activación adquirido bajo suscripción.

- Al añadir la clave al paquete de instalación de Kaspersky Endpoint Security.

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

- Con 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 de inmediato, puede interrumpir el proceso de activación en curso e iniciar la activación utilizando el Asistente de activación.

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

Activación de la aplicación

Cómo activar la 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Agregar clave**.

Paso 2. Selección de la clave que se agregará

Ingrese un código de activación o seleccione un archivo de clave.

Para más información sobre cómo agregar 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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Programación de la tarea

Programe la ejecución de la tarea. La tarea puede iniciarse manualmente o cuando el equipo está inactivo, por ejemplo.

Paso 5. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Activar Kaspersky Endpoint Security para Windows*.

Paso 6. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. Kaspersky Endpoint Security se activará en los equipos de los usuarios en modo silencioso.

Cómo activar 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 **Agregar**.

Se inicia el Asistente de tareas. 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 14.2.0**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Agregar clave**.
3. En el campo **Nombre de la tarea**, ingrese una breve descripción, por ejemplo, *Activación de Kaspersky Endpoint Security para Windows*.
4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea. Vaya al siguiente paso.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Selección de la licencia

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

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

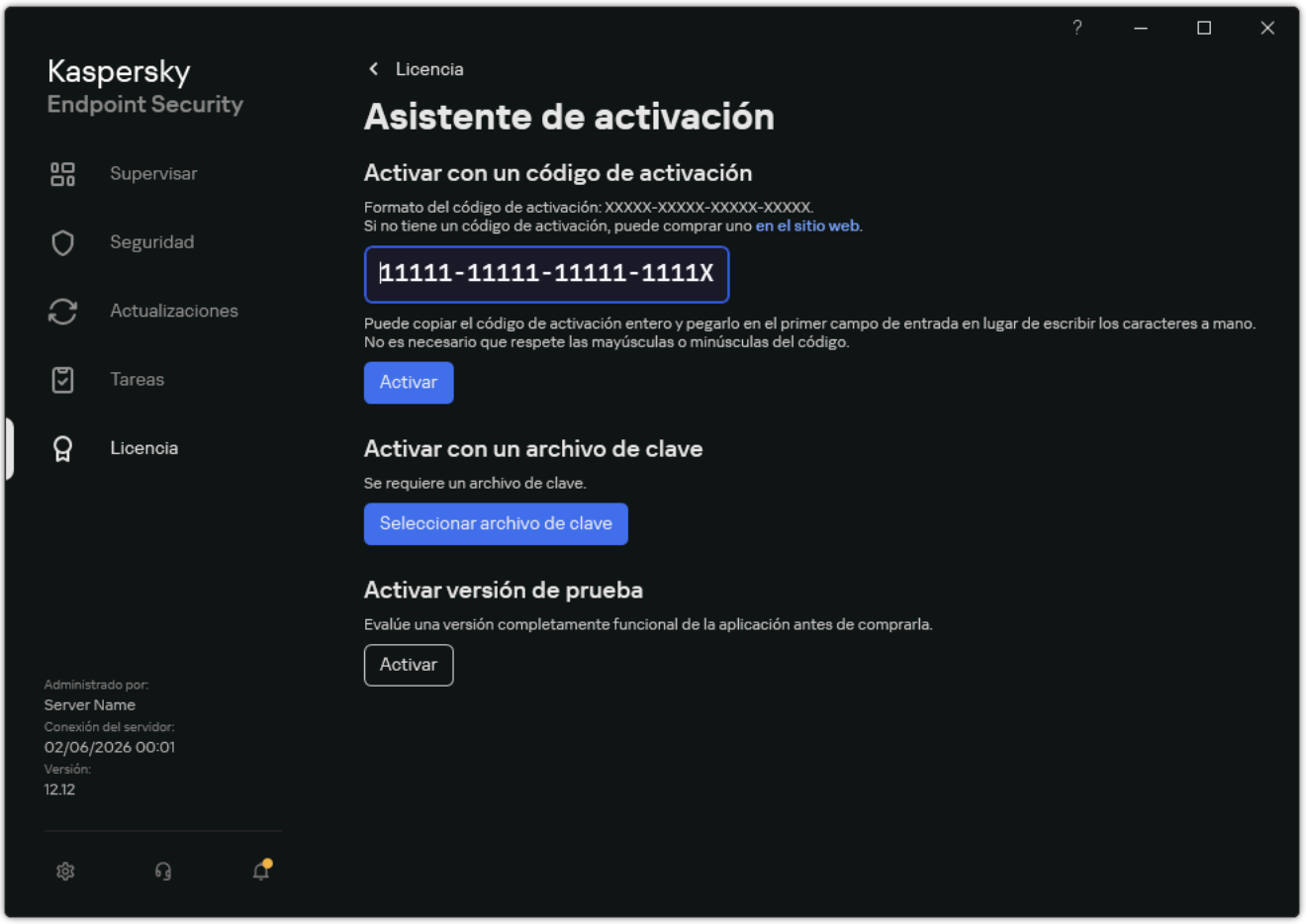
Paso 4. Completar creación de la tarea

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**. 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 nueva licencia**.

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 *Agregar clave*, encontrará una opción para agregar una clave de reserva a los equipos. 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 agregar una clave de licencia en los equipos de forma automática mediante la Consola de administración (MMC)

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

   Se abre una lista de claves de licencia.

2. Abra las propiedades de la clave de licencia.

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

4. Guarde los cambios.

La clave se distribuirá a los equipos adecuados automáticamente. El proceso de distribución de la clave (ya sea que se la vaya a utilizar como clave activa o como clave de reserva) está supeditado al número de equipos definido como límite de la licencia en las propiedades de la clave. En cuanto se alcanza el límite, el proceso de distribución se detiene. Encontrará el número de equipos en los que se agregó la clave, además de otros datos, en la sección **Dispositivos** de las propiedades de la clave.

Cómo agregar una clave de licencia en los equipos de forma automática mediante Web Console y Cloud Console

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

   Se abre una lista de claves de licencia.

2. Abra las propiedades de la clave de licencia.

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

4. Guarde los cambios.

La clave se distribuirá a los equipos adecuados automáticamente. El proceso de distribución de la clave (ya sea que se la vaya a utilizar como clave activa o como clave de reserva) está supeditado al número de equipos definido como límite de la licencia en las propiedades de la clave. En cuanto se alcanza el límite, el proceso de distribución se detiene. Puede ver la cantidad de equipos a las que se agregó la clave y otros datos en las propiedades de la clave en la pestaña **Dispositivos**.

Para activar la aplicación con un *código de activación*, se requiere acceso a Internet para conectarse con los servidores de activación de Kaspersky. Para activar la aplicación con un *archivo de clave*, no se requiere acceso a Internet. Si los equipos se encuentran en un segmento de red aislado 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 obtener acceso 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 correspondiente 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 de verificación **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 ficha **Configuración de la aplicación**.

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

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

6. Guarde los cambios.

Si no se puede activar la aplicación con un *código de activación*, puede intentar obtener un *archivo de clave* usando la solución de Kaspersky e intentar activar la aplicación nuevamente con un método diferente.

Supervisión del uso de licencias

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

- Consulte el *Informe de uso de claves de licencia* para la infraestructura de la organización (**Supervisión** → **Informes**).
- Ver los estados de los equipos en la pestaña **Dispositivos administrados** → **Dispositivos**. Los equipos en los que la aplicación no se haya activado tendrán el estado *La aplicación no está activada*.
- Ver la información de la licencia en las propiedades de los equipos.
- Consulte las propiedades de la clave (**Operaciones** → **Licencias**).

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

Tendrá acceso a una versión de prueba de Kaspersky Security Center Cloud Console. La *versión de prueba* de Kaspersky Security Center Cloud Console es una versión especial, pensada para que el usuario se familiarice con las funciones. La versión de prueba permite realizar acciones en un espacio de trabajo durante 30 días. Todas las aplicaciones administradas, incluida Kaspersky Endpoint Security, se ejecutan automáticamente con una licencia de prueba para Kaspersky Security Center Cloud Console. Cuando la licencia de prueba de Kaspersky Security Center Cloud Console caduque, no podrá activar Kaspersky Endpoint Security con una licencia de prueba específica para esa aplicación. Para encontrar más información acerca de la licencia de Kaspersky Security Center consulte la Ayuda de Kaspersky Security Center Cloud Console.

> La versión de prueba de Kaspersky Security Center Cloud Console no puede convertirse en versión comercial. Pasados los 30 días, el espacio de trabajo de prueba se eliminará, junto con todo lo que contenga.

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 la licencia caduca, Kaspersky Endpoint Security se lo notifica. Si agregó 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 deshacerse de las notificaciones y reparar el estado de su equipo.

La tarea *Eliminar una clave* permite eliminar cualquier clave de licencia del equipo. Puede eliminar claves de licencia activas, así como claves de licencia de reserva. Además de la clave de licencia de activación de Kaspersky Endpoint Security, puede eliminar claves de licencia individuales de soluciones de Kaspersky 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Eliminar una clave**.

Paso 2. Selección de la licencia

Seleccione la clave de licencia que desee 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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Programación de la tarea

Programe la ejecución de la tarea. La tarea puede iniciarse manualmente o cuando el equipo está inactivo, por ejemplo.

Paso 5. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo, *Eliminar clave para beta*.

Paso 6. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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 **Agregar**.

Se inicia el Asistente de tareas. 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 14.2.0**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Eliminar clave**.
3. En el campo **Nombre de la tarea**, escriba una breve descripción (por ejemplo, *Eliminar clave para beta*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea. Vaya al siguiente paso.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Selección de la licencia

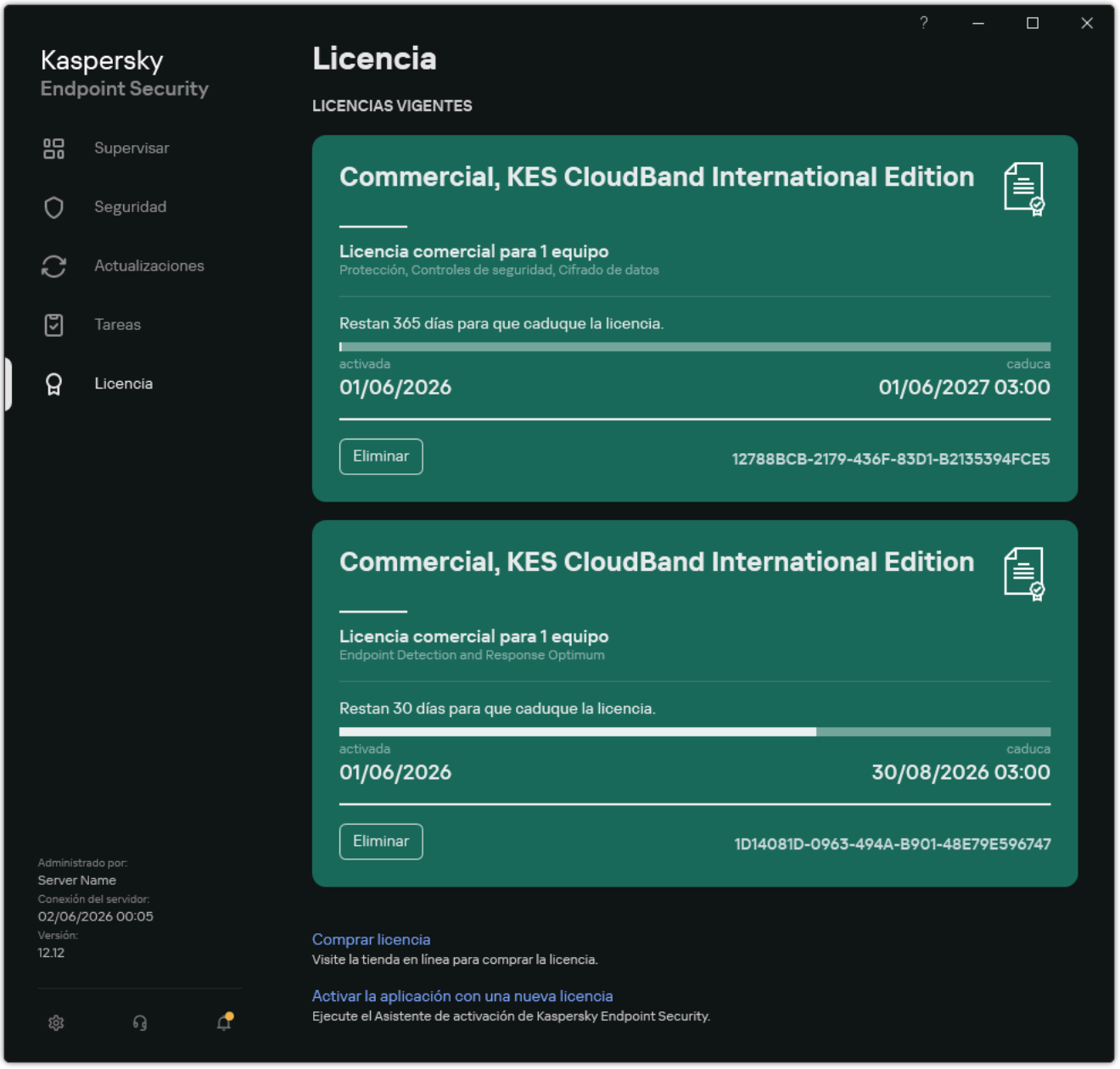
Seleccione la clave de licencia que desee eliminar. Puede seleccionar una clave de licencia del almacén de claves de Kaspersky Security Center o seleccionar un archivo de clave. Vaya al siguiente paso.

Paso 4. Completar creación de la tarea

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 desee eliminar y haga clic en **Eliminar**.



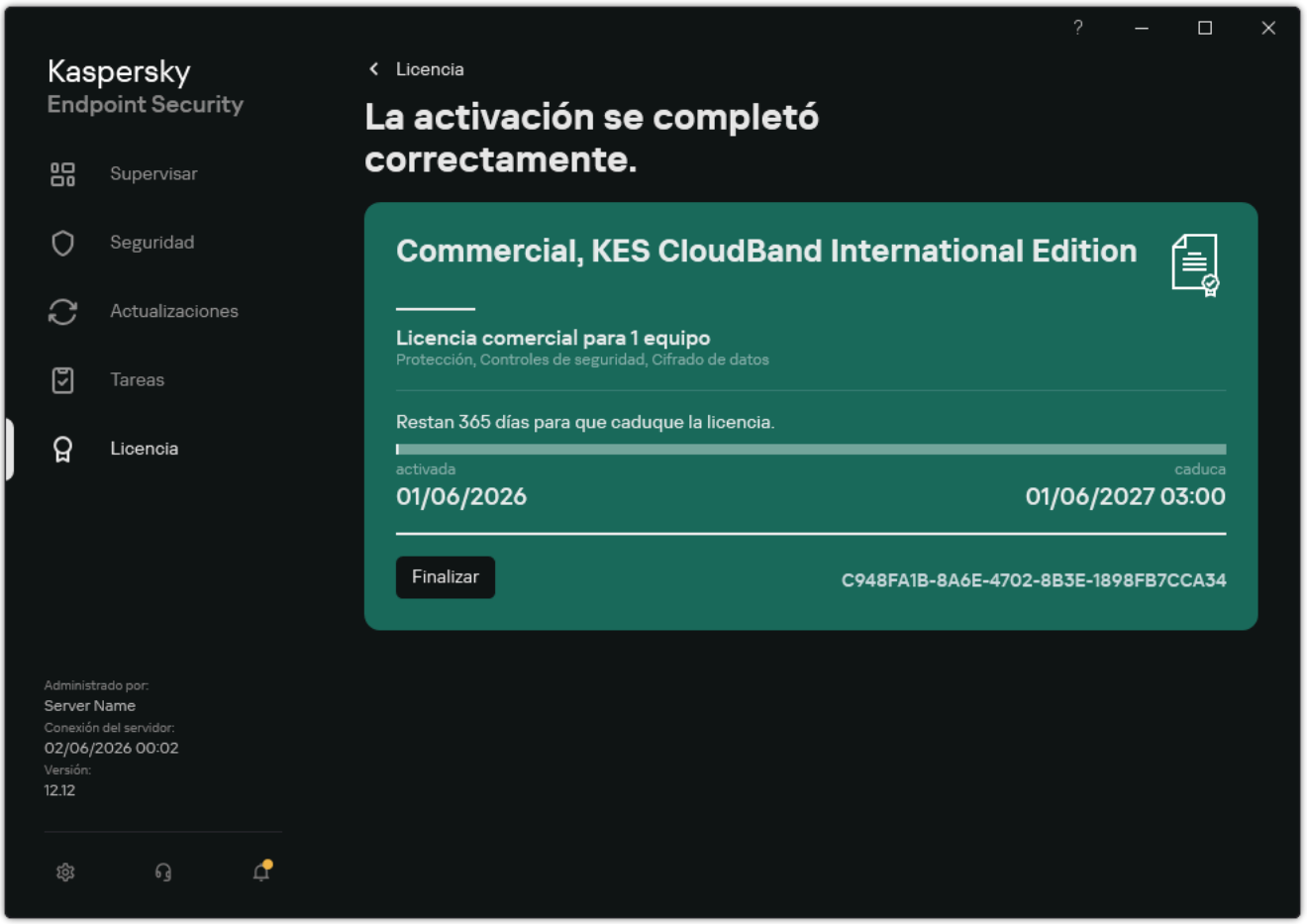
Ventana Licencias

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

Visualización de la información de la licencia

Para ver información sobre la licencia:

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



Ventana Licencias

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 no puede tener más de una clave activa. Para que se active una clave de reserva, es necesario esperar a que la clave activa caduque o eliminar la clave activa haciendo clic en **Eliminar**.
- *Nombre de la aplicación*. Nombre completo de la aplicación de Kaspersky que se ha adquirido.
- *Tipo de licencia*. Los siguientes tipos de licencias están disponibles: de prueba y comercial.
- *Características*. Funciones de la aplicación que la licencia permite utilizar. Entre las funciones se encuentran Protección, Controles de seguridad y Cifrado de datos. 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 plazo de la licencia (solo para la clave activa), duración restante del plazo de la licencia.

  El tiempo 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 nueva licencia**. Abre el Asistente de activación de la aplicación. Use el asistente para agregar una clave con un código de activación o un archivo de clave. A través del Asistente de activación de la aplicación, podrá agregar una clave activa y una única clave de reserva.

Adquisición de una licencia

Puede comprar una licencia después de instalar la aplicación. Cuando adquiera una licencia, recibirá un código de activación o un archivo de 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 agregó ninguna clave o si se agregó una clave para una licencia de prueba, haga clic en el botón **Comprar licencia**.

   - Si se agregó una clave para 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, donde podrá comprar una licencia.

Renovación de una suscripción

Cuando utiliza la aplicación con suscripción, Kaspersky Endpoint Security se contacta en forma automática con el servidor de activación a intervalos específicos hasta que caduque la suscripción.

Si utiliza la aplicación con suscripción ilimitada, Kaspersky Endpoint Security verifica en forma automática el servidor de activación por claves renovadas en modo de segundo. Si una clave está disponible en el servidor de activación, la aplicación la agrega reemplazando la clave anterior. De esta forma, la suscripción ilimitada de Kaspersky Endpoint Security se renueva sin la intervención del usuario.

Si utiliza la aplicación con una suscripción limitada, el día que la suscripción (o el período de gracia una vez que caduca la suscripción durante el que la renovación de la suscripción está disponible) caduca, Kaspersky Endpoint Security muestra la notificación correspondiente y detiene los intentos de renovar la suscripción en forma automática. En este caso, Kaspersky Endpoint Security se comporta del mismo modo que cuando caduca una licencia comercial para la aplicación: la aplicación funciona sin actualizaciones y Kaspersky Security Network no está disponible.

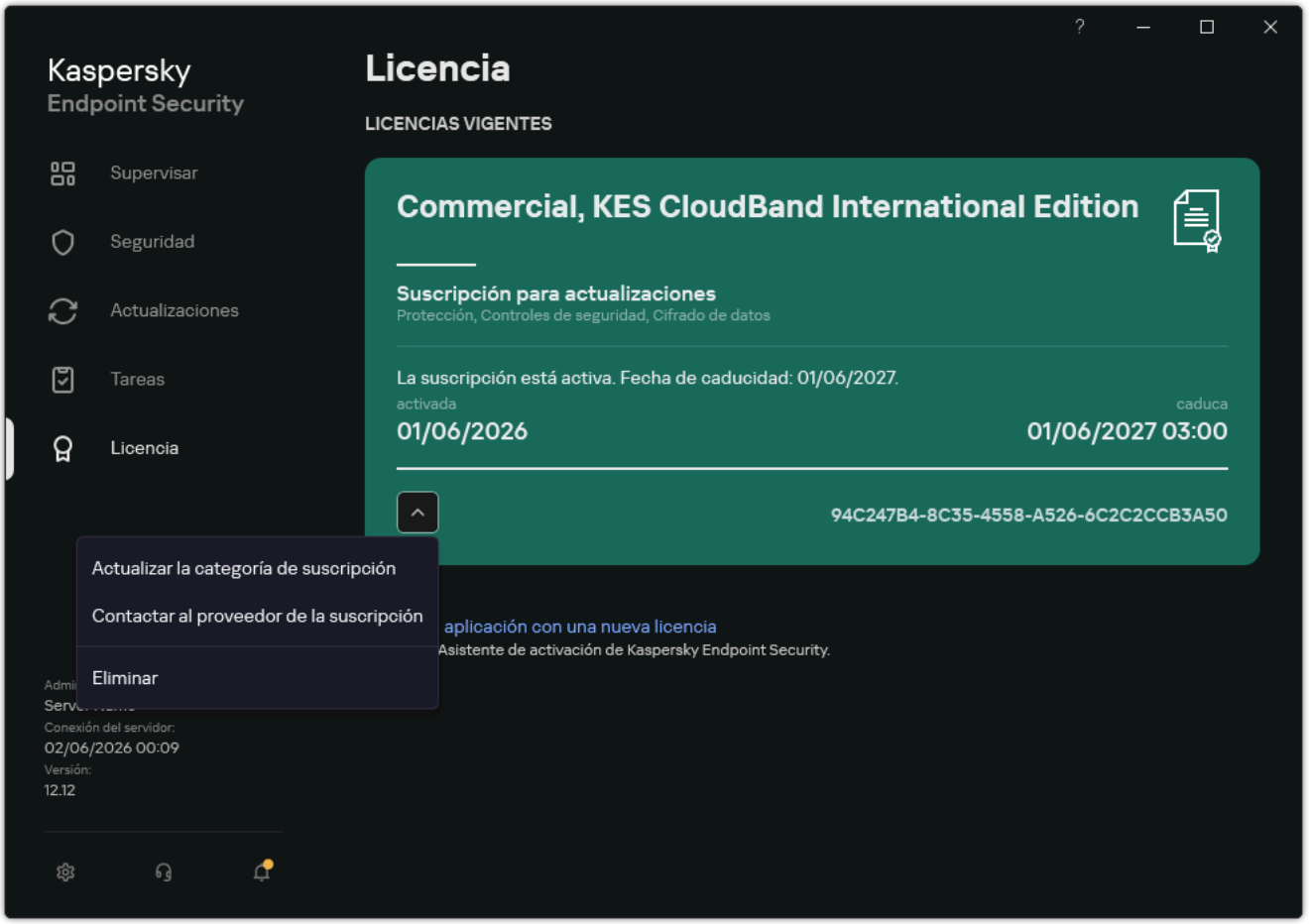
Cuando necesite renovar una suscripción, diríjase al sitio web de su proveedor de servicios.

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

1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.

2. Haga clic en **Contactar al proveedor de la suscripción**.

   Puede actualizar el estado de la suscripción en forma manual. Esto puede ser necesario si la suscripción se ha renovado una vez finalizado el período de gracia y la aplicación no ha actualizado el estado de la suscripción en forma automática.



Renovación de una suscripción

Primeros pasos

Una vez que termine la instalación, podrá administrar Kaspersky Endpoint Security a través de las siguientes interfaces:

- la interfaz local de la aplicación,
- la 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 instalar y desinstalar remotamente, iniciar y suspender Kaspersky Endpoint Security, establecer la configuración de la aplicación, cambiar el conjunto de componentes disponibles de la aplicación, añadir claves e iniciar y detener tareas de actualización y análisis.

La aplicación puede administrarse a través de Kaspersky Security Center con el complemento de administración de Kaspersky Endpoint Security.

Para más detalles 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 lo sucesivo también denominada *Web Console*) es una aplicación web que permite realizar, de manera centralizada, las principales tareas que se requieren para administrar y mantener el sistema de seguridad de la red de una organización. Web Console es un componente de Kaspersky Security Center que proporciona una interfaz de usuario. Para obtener información detallada sobre Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

Kaspersky Security Center Cloud Console (en adelante también llamada "*Cloud Console*") es una solución de nube diseñada para proteger y administrar la red de una organización. Para obtener información detallada sobre Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Puede usar tanto Web Console como Cloud Console para hacer lo siguiente:

- 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.

Web Console, Cloud Console y la Consola de administración de Kaspersky Security Center no ofrecen las mismas capacidades para administrar Kaspersky Endpoint Security. Los componentes y las tareas disponibles también varían según la consola.

Acerca del Complemento de administración para Kaspersky Endpoint Security para Windows

El Complemento de administración para Kaspersky Endpoint Security para Windows es el software que posibilita la interacción entre Kaspersky Endpoint Security y Kaspersky Security Center. Con el complemento, podrá administrar Kaspersky Endpoint Security a través de directivas, tareas y la configuración local de la aplicación. La interacción con Kaspersky Security Center Web Console depende del complemento web.

La versión del complemento de administración puede diferir de la versión 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 faltantes no será controlada por el complemento de administración. Estos parámetros pueden ser modificados por el usuario 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**). Para obtener más información sobre la compatibilidad de Web Console con las distintas versiones de los complementos web, consulte la Ayuda de Kaspersky Security Center.

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 ver los detalles de la alerta. *Detalles de la alerta* es una herramienta para ver la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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 las alertas, necesita el complemento de administración de EDR.

Instalación del complemento web

Puede instalar el complemento web de las siguientes maneras:

- Instale el complemento web utilizando 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 Web Console (**Descubrimiento 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 utilizando la lista de paquetes de distribución disponibles en Web Console.

  Para instalar el complemento web, seleccione el paquete de distribución del complemento web de Kaspersky Endpoint Security en la interfaz de Web Console (**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, agregue el archivo ZIP del 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, se modificó el procedimiento de instalación del complemento web. El paquete de distribución ahora incluye dos complementos web: *Kaspersky Endpoint Security for Windows 14.2.0* y *Unified Protection and Management Plug-in*. Esto se debe a la transición a un único complemento web unificado para administrar las aplicaciones de Kaspersky. El complemento web unificado permite crear una única 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 únicamente el complemento *Unified Protection and Management Plug-in*.

Actualización del complemento de administración

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

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

> Cuando actualice el complemento web, se guardarán los elementos que haya creado anteriormente (las directivas, las tareas, etc.). Los parámetros nuevos de aquellos elementos que implementen nuevas funciones de Kaspersky Endpoint Security aparecerán en los elementos existentes y tendrán los valores predeterminados.

Puede actualizar el complemento web de las siguientes maneras:

- Actualice el complemento web en la lista de complementos web en modo en línea.

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

- Actualice el complemento de web desde un archivo.

  Para actualizar el complemento web, debe seleccionar el archivo ZIP del 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. Solo puede actualizar el complemento web de Kaspersky Endpoint Security a una versión más reciente. El complemento web no puede actualizarse a una versión anterior.

Cuando se abre una directiva, una tarea u otro elemento, el complemento web revisa a información de compatibilidad. Si la versión del complemento web es la que indica la información de compatibilidad o una posterior, se permite cambiar la configuración del elemento abierto. Si esta condición no se cumple, el complemento web no puede usarse para cambiar la configuración del elemento. Se recomienda actualizar el complemento web.

Consideraciones especiales cuando se trabaja con distintas versiones de complementos de administración

Puede administrar Kaspersky Endpoint Security mediante Kaspersky Security Center solo si tiene un complemento de administración de la misma versión (o posterior) que la especificada en la información en cuanto a 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 que se incluye en el kit de distribución.

> Cuando se abre una directiva, una tarea o cualquier otro elemento, el complemento de administración revisa la información de compatibilidad. Si la versión del complemento de administración es la que indica la información de compatibilidad o una posterior, se permite cambiar la configuración del elemento abierto. Si esta condición no se cumple, el complemento de administración no puede usarse para cambiar la configuración del elemento. Se recomienda actualizar el complemento de administración.

Si el Complemento de administración para Kaspersky Endpoint Security está instalado en la Consola de administración, tenga en cuenta lo siguiente al instalar una nueva versión del Complemento de administración

- Se eliminará la versión anterior del Complemento de administración para Kaspersky Endpoint Security.
- La nueva versión del Complemento de administración para Kaspersky Endpoint Security admite la administración de la versión anterior del Kaspersky Endpoint Security para Windows en los equipos de los usuarios.
- Podrá usar la versión nueva para cambiar la configuración de las directivas, tareas y demás elementos que haya creado con la versión anterior.
- 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 que se actualiza el Complemento de administración, se recomienda revisar y guardar los valores de las nuevas configuraciones de las directivas y los perfiles de las directivas. Si no hace esto, los nuevos grupos de configuraciones de Kaspersky Endpoint Security en el equipo del usuario tomarán los valores predeterminados y se pueden modificar (el atributo). Se recomienda revisar las configuraciones comenzando con las directivas y los perfiles de directivas del nivel jerárquico superior. También se recomienda usar la cuenta de usuario que tenga derechos de acceso a todas las áreas funcionales de Kaspersky Security Center.

Para conocer las nuevas funciones de la aplicación, consulte las Notas de la versión o la ayuda de la aplicación.

- Si se ha añadido un nuevo parámetro a un grupo de configuraciones en la nueva versión del Complemento de administración, el estado definido previamente del atributo 🔒/🔓 para este grupo de configuraciones no cambia.

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 bases de datos y módulos de software de la aplicación.
- Activación de la aplicación con un código de activación (activación 2.0).
- Al usar Kaspersky Security Network.

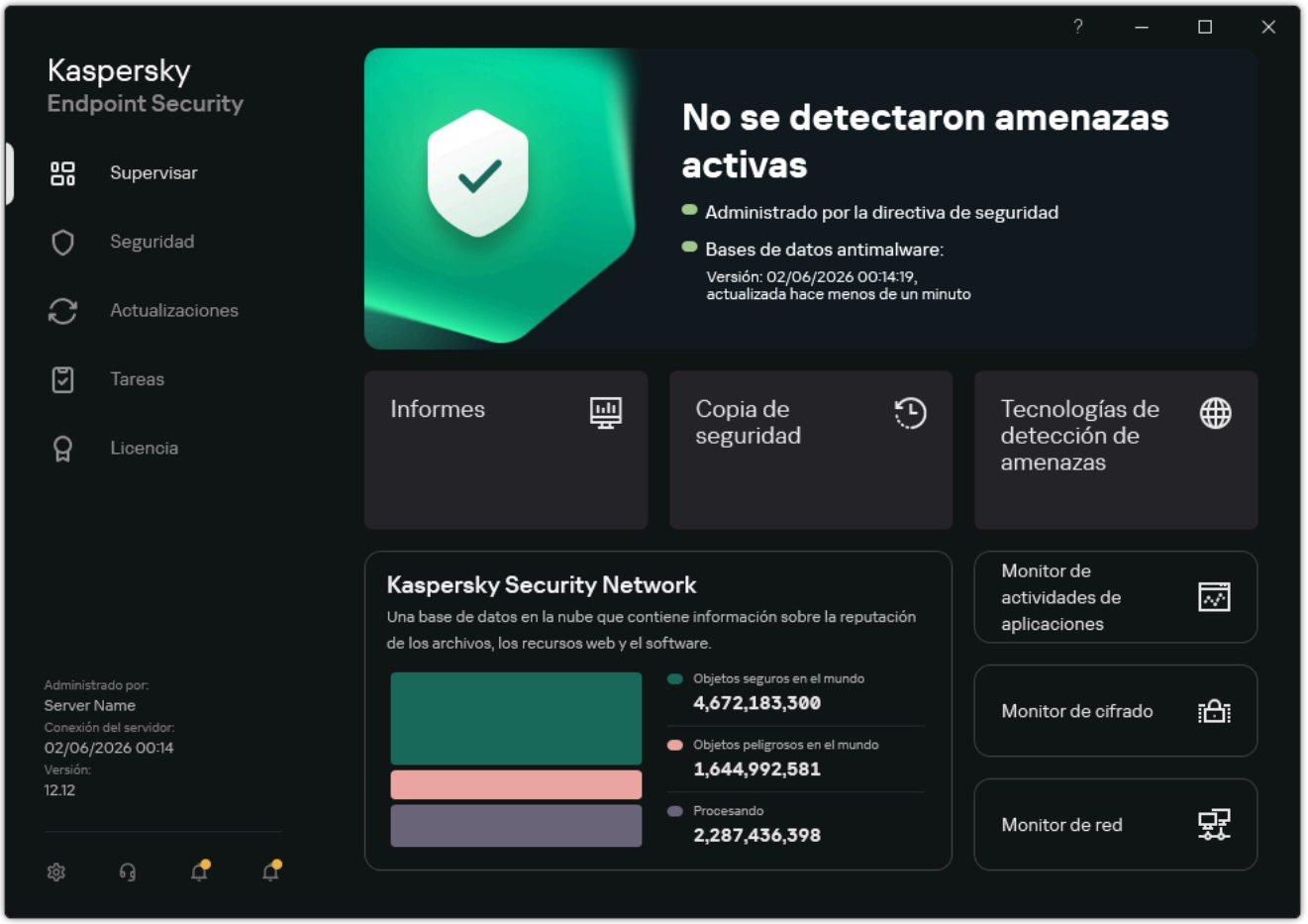
El uso de TLS protege a la aplicación al proporcionar las siguientes características:

- 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 forma parte de una PKI. Kaspersky utiliza su propia autoridad de certificación, ya que los servicios de Kaspersky son altamente técnicos y no tienen carácter público. En este caso, cuando se revocan los certificados raíz de Thawte, VeriSign, GlobalTrust y otros, la PKI de Kaspersky permanece en funcionamiento 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 servicios de Kaspersky. Por ejemplo, puede haber errores relacionados con el uso de Self-Signed Certificate. Estos errores pueden producirse debido a que una herramienta de inspección HTTPS de su entorno no reconoce la PKI de Kaspersky. Para solucionar estos problemas, debe configurar exclusiones para interactuar con servicios externos.

Interfaz de aplicación



Ventana principal de la aplicación

Supervisar	• **Informes**. Visualice eventos que ocurrieron durante el funcionamiento de la aplicación, componentes individuales y tareas. • **Copia de seguridad**. Visualice una lista de copias guardadas de archivos infectados que la aplicación ha eliminado. • **Tecnologías de detección de amenazas**. Visualice 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 de KSN Global. *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 los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, los servicios KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web analizadas, así como información sobre la categoría y la reputación de los archivos analizados . • **Monitor de actividades de aplicaciones**. Visualice información sobre el funcionamiento de las aplicaciones instaladas. El Monitor de actividades de aplicaciones lleva un registro de los eventos de archivos, del registro y del sistema operativo relacionados con la aplicación. • **Monitor de red**. Visualice información sobre la actividad de red del equipo en tiempo real. • **Monitor de cifrado**. Permite monitorear en tiempo real el cifrado o descifrado de una unidad. El componente Monitoreo de Cifrado estará disponible solamente si también se han instalado los componentes Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker.
Seguridad	Estado operativo de los componentes instalados. También puede ir a la configuración de los componentes o a la vista de los informes.
Actualizaciones	Administre las tareas de actualización de Kaspersky Endpoint Security. Puede actualizar las bases de datos antivirus y los módulos de la aplicación, además de revertir la última actualización. Un administrador puede ocultar la sección al usuario o restringir la administración de tareas.
Tareas	Administre las tareas de análisis de Kaspersky Endpoint Security. Puede ejecutar un análisis de malware y una comprobación de integridad de la aplicación. Un administrador puede ocultar tareas a un usuario o restringir la administración 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.
	Ajuste la configuración 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 lanzamiento de la base de datos, clave y otra información. También puede proceder a los recursos de información de Kaspersky, que brindan información útil, recomendaciones y respuestas a las preguntas frecuentes sobre cómo 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 notificación de la barra de tareas

Inmediatamente después de instalar Kaspersky Endpoint Security, aparece el icono de la aplicación en el área de notificación de la barra de tareas de Microsoft Windows.

Si el ícono de la aplicación en el área de notificación de la barra de tareas está oculto, el administrador deshabilitó la visualización de la interfaz de la aplicación en la directiva.

El icono tiene las siguientes finalidades:

- Indica la actividad de la aplicación.
- Funciona como acceso directo al menú contextual y a 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 críticos están habilitados. El icono de advertencia aparece cuando Kaspersky Endpoint Security necesita que el usuario realice alguna acción (por ejemplo, reiniciar el equipo tras una actualización del software).
- El icono indica que uno o más componentes de protección críticos están deshabilitados o han tenido problemas de funcionamiento. Los problemas de funcionamiento pueden deberse a un error en la aplicación, por ejemplo, o al hecho de que la licencia haya caducado. Kaspersky Endpoint Security mostrará una advertencia ( ) junto con una descripción del inconveniente de protección.

El menú contextual del icono de la aplicación contiene los siguientes elementos:

- **Kaspersky Endpoint Security para Windows**. Se abre la ventana principal de la aplicación. En esta ventana, puede ajustar el funcionamiento de las tareas y los componentes de la aplicación, además de mostrar las estadísticas de los archivos procesados y las amenazas detectadas.
- **Suspender protección/Reanudar protección**. Permite poner en pausa todos los componentes de protección y control que no estén marcados con un candado ( ) en la directiva. Recomendamos deshabilitar 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 protección** en el menú contextual de la aplicación.

> Suspender la operación de los componentes de protección y control no afecta el rendimiento de las tareas de actualización y análisis de malware. Tampoco suspende el uso de Kaspersky Security Network por parte de la aplicación.

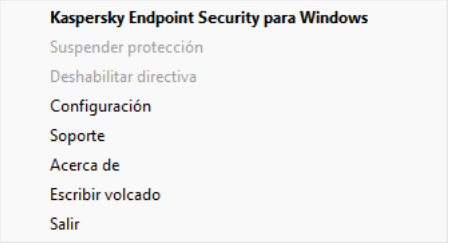
- **Deshabilitar directiva/Habilitar directiva**. Deshabilitar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado ( ) en la directiva, quedarán desbloqueados y podrán configurarse. Si deshabilita la directiva, la aplicación le solicitará 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 **Habilitar 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 Servicio de soporte técnico de Kaspersky.

- **Acerca de**. Este elemento abre una ventana de información con los detalles de la aplicación.

- **Salir**. Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este elemento del menú contextual, la aplicación se descarga de la memoria RAM del equipo.



Menú contextual del icono de la aplicación

Interfaz de la aplicación simplificada

Si se aplica una directiva de Kaspersky Security Center configurada para mostrar la interfaz simplificada de la aplicación a un equipo del cliente en el cual esté instalado Kaspersky Endpoint Security, la ventana principal de la aplicación no estará disponible en este equipo del cliente. Haga clic con el botón derecho del mouse para abrir el menú contextual para el ícono de Kaspersky Endpoint Security (consulte la ilustración a continuación) que contiene los elementos siguientes:

- **Deshabilitar directiva/Habilitar directiva**. Deshabilitar 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 deshabilita la directiva, la aplicación le solicitará 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 **Habilitar directiva** en el menú contextual de la aplicación.

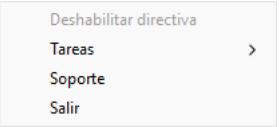
- **Tareas**. La lista desplegable contiene los siguientes elementos:

  - **Comprobación de integridad de la aplicación**.

  - **Reversión de 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 Servicio de soporte técnico de Kaspersky.
- **Salir**. Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este elemento del menú contextual, la aplicación se descarga de la memoria RAM del equipo.



Menú contextual del ícono de la aplicación al mostrar la interfaz simplificada

Configuración de la visualización de la interfaz de la aplicación

Puede determinar qué interfaz verá un usuario al utilizar la aplicación. Los usuarios pueden interactuar con el programa de distintas maneras:

- **Mostrar interfaz simplificada**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un ícono 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, encima del ícono de la aplicación, únicamente las notificaciones que requieren la intervención del usuario.
- **Mostrar interfaz del usuario**. La ventana principal de Kaspersky Endpoint Security y el ícono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. 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 del usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El ícono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

Cómo configurar el modo de presentación de la interfaz 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 correspondiente 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**, elija uno de los siguientes modos de presentación:

   - **Mostrar interfaz del usuario**. La ventana principal de Kaspersky Endpoint Security y el ícono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. 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 habilitar la funcionalidad **Ocultar la sección Monitor de actividades de aplicaciones** para ocultar los datos sobre la actividad de las aplicaciones en la computadora, restringiendo así el acceso de los usuarios a la herramienta Monitor de actividades de aplicaciones.

   - **Mostrar interfaz simplificada**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un ícono 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, encima del ícono de la aplicación, únicamente las notificaciones que requieren la intervención del usuario.

   - **No mostrar interfaz del usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El ícono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

5. Guarde los cambios.

Cómo configurar el modo de presentación de la interfaz a través de 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 ficha **Configuración de la aplicación**.

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

5. En el bloque **Visibilidad de los usuarios**, elija uno de los siguientes modos de presentación:

   - **Mostrar interfaz del usuario**. Si esta funcionalidad está deshabilitada, no se mostrarán indicios del funcionamiento de Kaspersky Endpoint Security en la computadora del cliente. El ícono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

   - **Simplificado**. La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un ícono 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, encima del ícono de la aplicación, únicamente las notificaciones que requieren la intervención del usuario.

   - **Lleno**. La ventana principal de Kaspersky Endpoint Security y el ícono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. 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 Monitor de actividades de aplicaciones**. 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 Monitor de actividades de aplicaciones.

6. Guarde los cambios.

Preparar la aplicación para su uso

Una vez que haya instalado Kaspersky Endpoint Security en los equipos cliente, deberá realizar las siguientes acciones para trabajar con la aplicación a través de Kaspersky Security Center Web Console:

- Crear y configurar una directiva.

  Puede utilizar directivas para aplicar configuraciones idénticas de Kaspersky Endpoint Security en todos los equipos cliente dentro de un grupo de administración. El Asistente de inicio rápido de Kaspersky Security Center crea una directiva para Kaspersky Endpoint Security automáticamente.

- Cree las tareas de *Actualización de bases de datos y módulos de la aplicación* y *Análisis de malware*.

  La tarea *Actualización de 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. El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

  La tarea *Análisis de malware* se requiere para detectar virus y otras clases de malware a tiempo. La tarea *Análisis de malware* se debe crear manualmente.

  Cómo crear una tarea de Análisis de malware 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**.

  Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Análisis de malware**.

Paso 2. Alcance del análisis

Cree una lista con los objetos que Kaspersky Endpoint Security deberá analizar cuando se ejecute la tarea.

Paso 3. Acción de Kaspersky Endpoint Security

Elija la acción que se llevará a cabo si se detecta una amenaza:

- **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

- **Desinfectar; informar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección falla, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.

- **Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.

- **Ejecutar la desinfección avanzada inmediatamente**. Si activa esta casilla, Kaspersky Endpoint Security usará la tecnología de desinfección avanzada para procesar las amenazas activas que se detecten durante el análisis.

  La *tecnología de desinfección avanzada* está diseñada para purgar el sistema operativo de aplicaciones malintencionadas que ya se han ejecutado y se han cargado en la RAM, y que Kaspersky Endpoint Security no puede eliminar por otros medios. Como resultado, se neutraliza la amenaza. Mientras está en curso la desinfección avanzada, se le advierte que no inicie nuevos procesos ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada consume una cantidad significativa de recursos del sistema, lo que puede ralentizar otras aplicaciones. Cuando termina un proceso de desinfección avanzada, Kaspersky Endpoint Security reinicia el equipo sin pedirle autorización al usuario.

- **Ejecutar solo cuando el equipo esté inactivo**. Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando el equipo está en uso.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.

- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 5. Selección de la cuenta con la que se ejecutará la tarea

Seleccione la cuenta con la que se ejecutará la tarea *Análisis de malware*. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local. Si ha incluido unidades de red u objetos de acceso restringido en el alcance del análisis, asegúrese de elegir una cuenta de usuario que tenga los derechos de acceso necesarios.

Paso 6. Programación de la tarea

Programe la tarea. Indique si la tarea deberá iniciarse manualmente, si se ejecutará después de que las bases de datos antivirus se descarguen al repositorio o si se usará otro esquema.

Paso 7. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Análisis completo diario*.

Paso 8. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. Como resultado, la tarea de Análisis de malware se ejecutará en los equipos de los usuarios de acuerdo con la programación especificada.

Cómo crear una tarea de Análisis de malware en Web Console

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Análisis de malware**.

   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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del Asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Para configurar la programación 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 de malware se ejecutará en los equipos de los usuarios de acuerdo con la programación especificada.

- Optimice el rendimiento de Kaspersky Endpoint Security.

Administración 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 de administración puede tener su propia directiva para la aplicación.

Cada configuración de directiva tiene el atributo ("candado"). El estado de este atributo determina si la configuración se pasará a los dispositivos administrados en el grupo de administración:

- Si el "candado" está abierto (), el valor de esta configuración no se transferirá a los dispositivos administrados. La configuración estará disponible para su modificación en la interfaz local de la aplicación. Esas configuraciones se denominan *desbloqueado*.

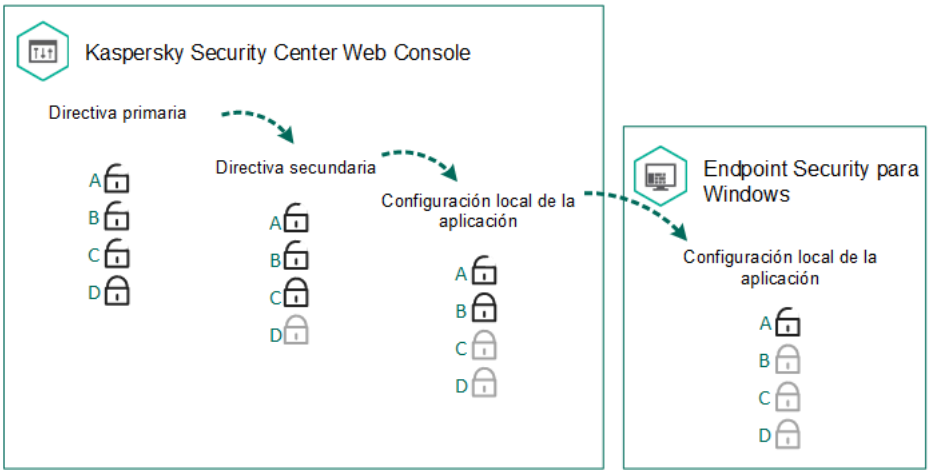
- Si el "candado" está cerrado (), el valor de esta configuración se pasará y se aplicará a los dispositivos administrados. Esas configuraciones se denominan *bloqueado*. Las configuraciones bloqueadas no se pueden modificar en la interfaz local de la aplicación.

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 la sincronización cada 15 minutos por defecto. Si la sincronización falla después de cambiar la configuración de la directiva, el siguiente intento de sincronización se realizará de acuerdo con la programación configurada.

Herencia de configuración

Al igual que los grupos de administración, las directivas se organizan en una jerarquía. Una *directiva secundaria* es una directiva creada para un nivel anidado de una jerarquía; en otras palabras, es una directiva para grupos de administración anidados y Servidores de administración secundarios.

De manera predeterminada, las directivas secundarias heredan la configuración de las directivas primarias. Si la configuración en la directiva principal tiene el atributo ("candado" cerrado), entonces, en las directivas secundarias y en la configuración de la aplicación local, el valor de esa configuración se anulará de acuerdo con la directiva principal. Además, la configuración se bloqueará. Si es necesario, puede deshabilitar la herencia de la configuración de su 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 para la configuración de la directiva de acceso (lectura, escritura y ejecución) se especifican para cada usuario que tiene acceso al Servidor de administración de Kaspersky Security Center y en forma separada para cada alcance 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 forma predeterminada, esta sección está oculta en la interfaz de la consola).

Revisiones de directivas

Kaspersky Security Center realiza un seguimiento de las modificaciones de la directiva 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, el comentario 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 revisiones**. Para obtener más información sobre el funcionamiento de las revisiones, consulte la Ayuda de Kaspersky Security Center.

Creación de una directiva

Al crear una directiva, el asistente sugiere configuraciones que son relevantes para el modo seleccionado. Por ejemplo, para el modo de Light Agent, debe agregar un Servidor de protección (SVM). Cuando utilice la aplicación para proteger un servidor SQL, debe agregar 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. Luego, 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Haga clic en **Nueva directiva**.

   Se inicia el Asistente para directivas.
5. Siga las instrucciones del Asistente para directivas.

Paso 1. Seleccionar la aplicación para crear la directiva de grupo

Seleccione la aplicación **Kaspersky Endpoint Security para Windows (14.1)**.

Paso 2. Asignar un nombre a la directiva de grupo

Escriba un nombre para la directiva de grupo, por ejemplo, *Directiva de la oficina*.

También puede crear directivas nuevas basadas en las directivas existentes con el Asistente de directivas. Para hacerlo, al especificar el nombre de la directiva de grupo, seleccione la casilla de verificación **Usar la configuración de la directiva creada para una versión más antigua 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 para Windows.

Paso 3. Participación en Kaspersky Security Network

Lea y acepte los términos de la Declaración de Kaspersky Security Network (KSN).

Paso 4. Seleccionar el modo de uso de la aplicación en los equipos

Según el uso previsto para 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 directiva con la configuración predeterminada**. Los ajustes predeterminados se consideran óptimos. Esta configuración está recomendada por los expertos de Kaspersky. La configuración predeterminada proporciona el nivel de protección recomendado y el uso óptimo de los recursos.

- **Cambiar los parámetros de la directiva usando el Asistente**. Este método permite administrar la configuración de la directiva paso a paso mediante un asistente. También puede administrar la configuración de la directiva mediante un archivo de configuración de la aplicación (vea el paso siguiente).

- Endpoint Detection and Response Agent para proteger contra amenazas avanzadas y ataques dirigidos.

  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 admitir las soluciones Detection and Response de Kaspersky. En el siguiente paso, debe seleccionar una solución para la integración del EDR Agent.

- Light Agent para proteger entornos virtuales.

  Para usar la aplicación en el modo de Light Agent, debe configurar una conexión con una máquina virtual SVM. Esta configuración es necesaria para que la aplicación funcione en el modo de Light Agent.

Kaspersky Endpoint Security proporciona una directiva común para todos los modos de la aplicación y tipos de SO. 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, cuando se utiliza la aplicación en el modo Endpoint Detection and Response Agent, solo están disponibles las configuraciones 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 sistemas operativos.

Paso 5. Importación de 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 CFG. Al importar un archivo de configuración de la aplicación, no toda la configuración de la directiva está disponible para el asistente. Por ejemplo, los perfiles de directivas no aparecen en la configuración de la aplicación. Si desea transferir toda la configuración y todos los 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 criptocontenedores. Si utiliza la autenticación bidireccional al conectarse a los servidores, debe especificar las contraseñas del criptocontenedor desde cero.

Paso 6 - 10. Configuración de las opciones 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

Configure la zona de confianza. Puede agregar exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en el modo de Light Agent en los entornos virtuales de Citrix y VMware.

Paso 12. Seleccionar el estado de la directiva

- **Activas**. Después de la próxima sincronización, la directiva se usará 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.

- **Inactivas**. 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 con 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 sale del 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 **Agregar**.

   Se inicia el Asistente para directivas.

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 proteger contra amenazas avanzadas y ataques dirigidos.

  Si selecciona este modo, puede crear una directiva para integrar el equipo con las soluciones de Kaspersky Detection and Response. El asistente le pedirá que configure la integración para Kaspersky Managed Detection and Response y luego para 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 el modo de Light Agent.

Kaspersky Endpoint Security proporciona una directiva común para todos los modos de la aplicación y tipos de SO. 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, cuando se utiliza la aplicación en el modo Endpoint Detection and Response Agent, solo están disponibles las configuraciones 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 sistemas operativos.

6. Configure la zona de confianza. Puede agregar exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en el modo de Light Agent en los entornos virtuales de 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 próxima sincronización, la directiva se usará 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 con 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 sale del perímetro de la red de la organización.

- Configurar la herencia de configuración:

  - **Heredar configuración de la directiva primaria**. 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 configuración en las directivas secundarias**. Si el botón de alternar está activado, los valores de la configuración de la directiva se propagan a las directivas secundarias. En las propiedades de la directiva secundaria, el interruptor **Heredar configuración de la directiva primaria** se activará automáticamente y no podrá desactivarse. La configuración de la directiva secundaria se hereda de la directiva principal, excepto la configuración marcada con . La configuración de la directiva secundaria no se puede editar si está establecida 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. Si desea ver información sobre la directiva aplicada al equipo (por ejemplo, el nombre de la directiva), haga clic en el botón en la ventana principal de la interfaz de Kaspersky Endpoint Security. Tenga en cuenta que, para que ver esta información, la opción para que se pueda obtener información adicional sobre la directiva debe estar habilitada en la directiva del Agente de red. Para más detalles sobre la 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. Luego, puede usar la funcionalidad de exportación/importación de directivas para crear copias de seguridad de las directivas, migrar 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.

3. En el espacio de trabajo, seleccione la ficha **Directivas**.

4. Para exportar una directiva:

   a. Haga clic en la directiva que desea exportar.

   b. Haga clic en el vínculo **Exportar directiva a archivo** en la parte derecha de la ventana.

   c. En la ventana que se abre, escriba el nombre del archivo KLP al que quiere exportar la directiva. Seleccione también la carpeta en la que se guardará 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 el archivo de directiva KLP que quiere importar.

   c. Abra el archivo.

   Esto agrega una nueva directiva con el estado *Directiva inactiva*.

Cómo exportar e importar una directiva en Web Console y Cloud Console

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

2. Para exportar una directiva:

   a. Seleccione la casilla ubicada junto a la directiva que desee exportar.

   b. Haga clic en el botón **Exportar**.

   c. En la ventana que se abre, escriba el nombre del archivo KLP al que quiere exportar la directiva. Seleccione también la carpeta en la que se guardará 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 aplicar la directiva.

   d. Haga clic en **Completada** para terminar de importar la política.

   Esto agrega una nueva directiva con el estado *Inactivas*.

Indicador del nivel de seguridad

El indicador del nivel de seguridad se muestra en la parte superior de la ventana de propiedades de la directiva. El indicador puede tener uno de los valores siguientes:

- **Nivel de protección alto**. El indicador indica este valor y se muestra en verde si están habilitados todos los componentes de las siguientes categorías:

  - **Críticos**. Esta categoría incluye los siguientes componentes:

    - Protección contra amenazas de archivo.

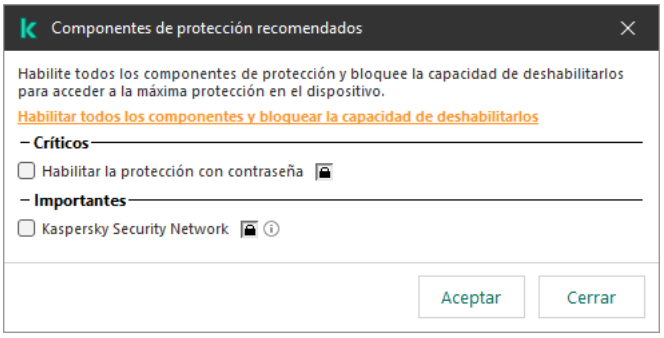
    - Detección de comportamiento.

    - Prevención de exploits.

    - Motor de reparación.
    - Protección de los servicios de aplicación contra la administración externa.
  - **Importantes**. Esta categoría incluye los siguientes componentes:
    - Kaspersky Security Network.
    - Protección contra amenazas web.
    - Protección contra amenazas de correo.
    - Prevención de intrusiones en el host.
    - Protección con contraseña.
- **Nivel de protección medio**. El indicador muestra este valor y en color amarillo si se ha deshabilitado uno de los componentes importantes.
- **Nivel de protección bajo**. El indicador muestra este valor y aparece en color rojo en uno de los siguientes casos:
  - Se han deshabilitado uno o varios componentes críticos.
  - Se han deshabilitado dos o más componentes importantes.

Cuando el valor del indicador sea **Nivel de protección medio** o **Nivel de protección bajo**, habrá un vínculo para abrir la ventana **Componentes de protección recomendados** a la derecha del indicador. En esta ventana, podrá habilitar cualquiera de los componentes de protección recomendados.

Después de actualizar la aplicación, puede que el indicador del nivel de protección indique un nivel de protección menor al que tenía antes de la actualización. Esto ocurre porque la nueva versión de la aplicación contiene componentes o funciones nuevos que son importantes para la seguridad del equipo. Después de actualizar la aplicación, deberá ajustar la nueva configuración para que el nivel de protección se mantenga alto.



Indicador del nivel de seguridad de la directiva

Administración de tareas

Puede crear los siguientes tipos de tareas para administrar Kaspersky Endpoint Security a través de Kaspersky Security Center:

- Tareas locales configuradas para un equipo cliente individual
- Tareas de grupo configuradas para equipos cliente pertenecientes a grupos de administración
- Tareas para una selección de equipos.

Puede crear cuantas tareas locales, de grupo y para selecciones de equipos necesite. Para obtener 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 de malware**. Kaspersky Endpoint Security analiza las áreas del equipo que se especifican en la configuración de la tarea en busca de virus y otras amenazas. La tarea *Análisis de malware*, 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.
- **Agregar clave**. Kaspersky Endpoint Security agrega 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 de equipos permitido por la licencia.
- **Cambiar componentes de la aplicación**. Kaspersky Endpoint Security instala o elimina componentes en equipos cliente conforme a la lista de componentes especificada en la configuración de la tarea. El componente Protección contra archivos peligrosos no puede eliminarse. El conjunto óptimo 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 bases de datos y módulos de la aplicación**. Kaspersky Endpoint Security actualiza sus bases de datos y módulos. La tarea *Actualización de 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 programación 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.
- **Reversión de la 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 parámetros de las cuentas del Agente de autenticación. Estas cuentas se necesitan para utilizar unidades cifradas. El usuario debe autenticarse con el Agente antes de que se cargue el sistema operativo.

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 *Finalizar proceso*.

Las tareas se ejecutarán en un equipo únicamente si Kaspersky Endpoint Security está en funcionamiento.

Crear una tarea

Cómo crear una tarea con 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**.

   Se inicia el Asistente de tareas.
4. Siga las instrucciones del Asistente de tareas.

Cómo crear una tarea con 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 **Agregar**.

   Se inicia el Asistente de tareas.
3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione el tipo de tarea que desee ejecutar en los equipos del usuario.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.
4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.
5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará 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, necesita activar la casilla a su lado y hacer clic en el botón **Iniciar**. Una vez iniciada, podrá pausar y reanudar la tarea cuando lo desee.

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 tareas

Los permisos de acceso a las tareas de Kaspersky Endpoint Security (leer, escribir, ejecutar) se definen individualmente para cada usuario que tiene acceso al Servidor de administración de Kaspersky Security Center, a través de los ajustes de acceso a las distintas áreas funcionales de Kaspersky Endpoint Security. Para configurar el acceso a las áreas funcionales de Kaspersky Endpoint Security, diríjase a la sección **Seguridad** de la ventana de propiedades del Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la administración de tareas a través de Kaspersky Security Center, consulte la ayuda de Kaspersky Security Center.

Puede utilizar una directiva para configurar los derechos de acceso de los usuarios a las tareas (*modo de administración de tareas*). Entre otros aspectos, puede determinar que las tareas de grupo no deberán aparecer en la interfaz de Kaspersky Endpoint Security.

Cómo configurar el modo de administración de tareas de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Tareas locales** → **Administración de tareas**.
4. Configure el modo de administración de tareas (vea la tabla de más abajo).
5. Guarde los cambios.

Cómo configurar el modo de administración de tareas de la interfaz de Kaspersky Endpoint Security a través de 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Interacción del usuario**.
5. En **Acciones permitidas**, configure el modo de administración de tareas (vea la tabla a continuación).
6. Guarde los cambios.

Parámetro	Descripción
Acceder a tareas locales	Si se selecciona la casilla, las tareas locales se muestran en la interfaz local de Kaspersky Endpoint Security. Cuando no haya restricciones adicionales de la directiva, el usuario puede configurar y ejecutar tareas. Sin embargo, la configuración del programa de ejecución de tareas no está disponible para el usuario. El usuario puede ejecutar tareas solo manualmente. Si la casilla de verificación se desactiva, el uso de tareas locales se detiene. En este modo, las tareas locales no se ejecutan según la programación. Las tareas no pueden iniciarse o configurarse en la interfaz local de Kaspersky Endpoint Security, o al funcionar con la línea de comandos. Un usuario puede iniciar un análisis de un archivo o carpeta al seleccionar la opción **Analizar en busca de virus** en el menú contextual del archivo o carpeta. La tarea de análisis se inicia con los valores predeterminados de configuración para la tarea de análisis personalizado.
Ver tareas de grupo	Si se selecciona la casilla, las tareas de grupo se muestran en la interfaz local de Kaspersky Endpoint Security. El usuario podrá ver la lista de tareas completa a través de la interfaz de la aplicación. Si se desactiva esta casilla, Kaspersky Endpoint Security mostrará una lista de tareas vacía.
Administrar tareas de grupo	Si se selecciona esta casilla, los usuarios podrán iniciar y detener las tareas de grupo que se creen en la consola de Kaspersky Security Center. Podrán para ello usar cualquiera de las dos interfaces de la aplicación (completa o simplificada). Si se desactiva esta casilla, Kaspersky Endpoint Security iniciará las tareas programadas automáticamente. El administrador también podrá iniciar estas tareas manualmente a través de la consola de Kaspersky Security Center.

Configuración local de la aplicación

Puede utilizar Kaspersky Security Center para configurar los parámetros de Kaspersky Endpoint Security de un equipo puntual. Tales parámetros se denominan *configuración local de la aplicación*. No siempre es posible modificar todas las configuraciones. Los parámetros que no pueden modificarse tienen el atributo de bloqueo en las propiedades de la directiva.

Cómo modificar la configuración local de la aplicación 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Haga doble clic en un equipo para abrir su ventana de propiedades.
5. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.1)** y haga doble clic para abrir las propiedades de la aplicación.
7. En la sección **Configuración general**, configure Kaspersky Endpoint Security e Informes y repositorios.

   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 la configuración específica, no podrá modificarlos al configurar los parámetros de la aplicación en la sección **Configuración general**.

8. Guarde los cambios.

Cómo modificar la configuración local de la aplicación a través de 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 ficha **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.
5. Seleccione la ficha **Configuración de la aplicación**.
6. Haga los cambios que necesite en la configuración local de la aplicación.
7. Guarde los cambios.

La configuración de la aplicación local es igual que la configuración de la directiva, excepto la configuración de cifrado.

Iniciar y detener 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 es posible configurar la autoejecución de la aplicación en el sistema operativo.

Dependiendo de las prestaciones del equipo, las bases de datos antivirus de Kaspersky Endpoint Security pueden tardar hasta dos minutos en descargarse tras el inicio del sistema operativo. Durante este tiempo, 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 definir si Kaspersky Endpoint Security se ejecutará automáticamente 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 correspondiente 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 **Iniciar la aplicación al arrancar el equipo (recomendado)** para configurar el inicio de la aplicación.
5. Guarde los cambios.

Cómo definir si Kaspersky Endpoint Security se ejecutará automáticamente a través de 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 ficha **Configuración de la aplicación**.

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

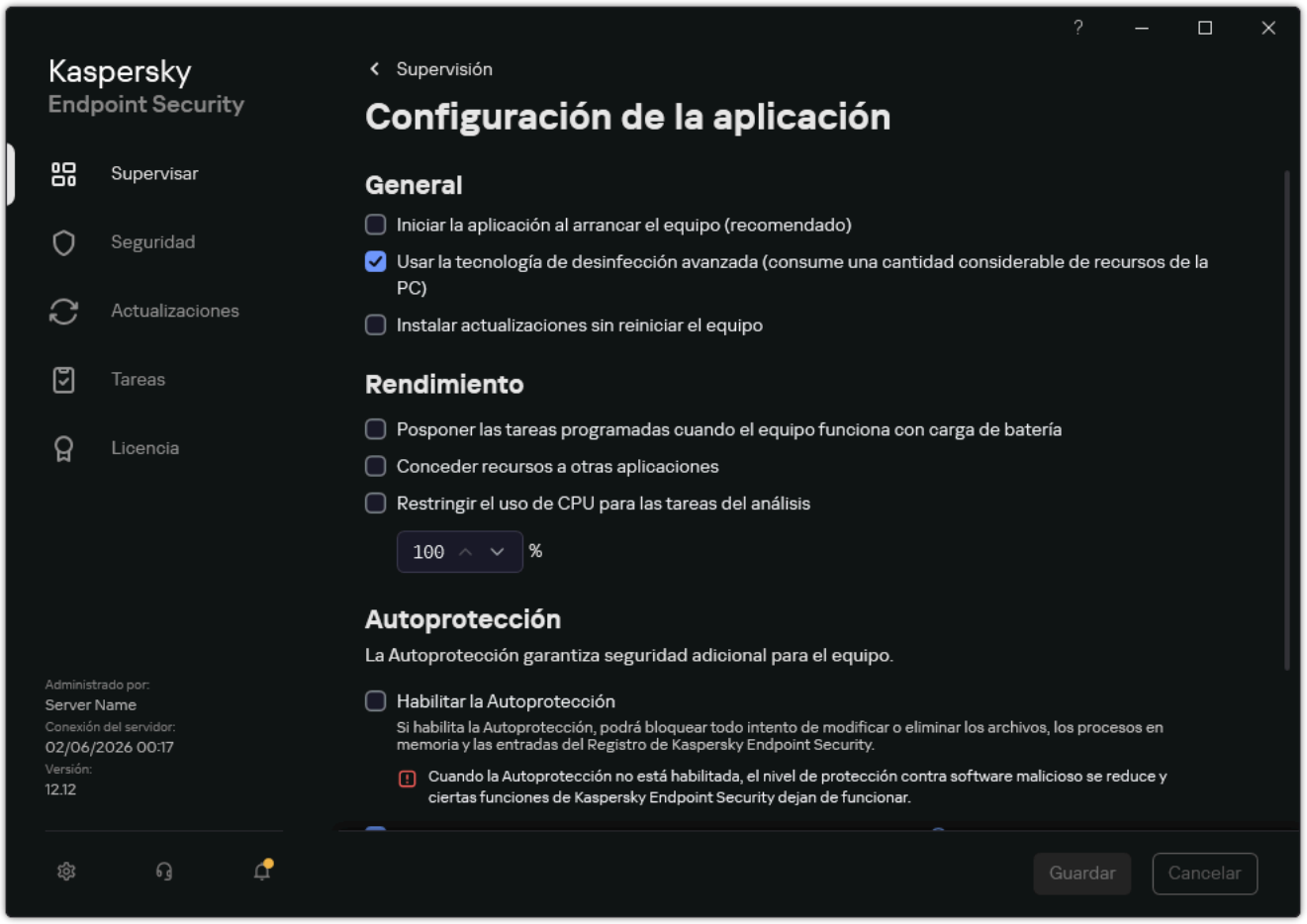
5. Use la casilla **Iniciar Kaspersky Endpoint Security en el arranque del equipo (recomendado)** para configurar el inicio de la aplicación.

6. Guarde los cambios.

Cómo definir si Kaspersky Endpoint Security se ejecutará automáticamente a través de la interfaz local

1. En la ventana principal de la aplicación 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 **Iniciar la aplicación al arrancar 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 es necesario, puede suspender la protección del equipo mientras tenga que hacerlo, sin detener la aplicación.

Podrá controlar el estado de la aplicación a través del widget **Estado de protección**.

Cómo iniciar o detener Kaspersky Endpoint Security 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Haga doble clic en un equipo para abrir su ventana de propiedades.
5. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.1)** 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 , que encontrará a la derecha de la lista de aplicaciones de Kaspersky.
   - Para detener la aplicación, haga clic en el botón , que encontrará a la derecha de la lista de aplicaciones de Kaspersky.

Cómo iniciar o detener Kaspersky Endpoint Security a través de 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 ficha **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. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta donde se encuentra el archivo ejecutable klpsm.exe.
3. Para iniciar la aplicación mediante la línea de comandos, use el comando `klpsm.exe start_avp_service`.
4. Para detener la aplicación mediante la línea de comandos, use el comando `klpsm.exe stop_avp_service`.

Para detener la aplicación desde la línea de comandos, habilite la administración externa de los servicios del sistema.

Inicio y detención de la aplicación desde la línea de comandos

Suspensión y reanudación de la protección y control del equipo

Suspender la protección y control del equipo significa deshabilitar todos los componentes de protección y control de Kaspersky Endpoint Security durante un tiempo.

El estado de aplicación se muestra por medio del icono de la aplicación en el área de notificación de la barra de tareas.

- El icono significa que la protección y control del equipo están suspendidos.
- El icono significa que la protección y control del equipo están habilitados.

Suspender o reanudar el control y la protección del equipo no afecta las tareas de análisis o actualización.

Si hay conexiones de red ya establecidas cuando suspende o reanuda la protección y control del equipo, se muestra una notificación que informa que estas conexiones de red se han interrumpido.

Para pausar la protección y control del equipo:

1. Haga clic con el botón derecho para mostrar el menú contextual del icono de la aplicación que se encuentra en el área de notificación de la barra de tareas.
2. En el menú contextual, seleccione **Suspender protección** (vea la siguiente imagen).

   Este elemento del menú contextual está disponible si la protección con contraseña está habilitada.

3. Seleccione una de las siguientes opciones:

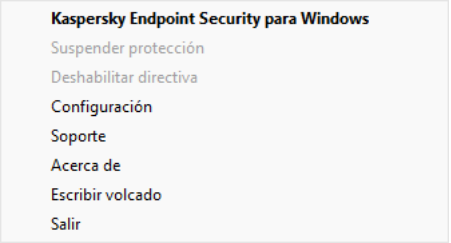
   - **Suspender durante <periodo>**: las funciones de protección y control del equipo se reactivarán cuando haya transcurrido el tiempo que indique en la lista desplegable de abajo.

   - **Suspender hasta reiniciar la aplicación**: las funciones de protección y control del equipo se reactivarán luego de que cierre y vuelva a abrir la aplicación, o bien cuando se reinicie el sistema operativo. Para utilizar esta opción, debe habilitarse el inicio automático de la aplicación.

   - **Suspender**: las funciones de protección y control del equipo se reactivarán cuando usted lo decida.

4. Haga clic en **Suspender protección**.

   Kaspersky Endpoint Security pausará todos los componentes de protección y control que no estén marcados con un candado (🔒) en la directiva. Recomendamos deshabilitar la directiva de Kaspersky Security Center antes de realizar esta operación.



Menú contextual del icono de la aplicación

Para reanudar la protección y control del equipo:

1. Haga clic con el botón derecho para mostrar el menú contextual del icono de la aplicación que se encuentra en el área de notificación de la barra de tareas.

2. En el menú contextual, seleccione **Reanudar protección**.

Puede reanudar la protección y control del equipo en cualquier momento, sin importar la opción que seleccionó previamente para suspender la protección y control.

Crear y utilizar un archivo de configuración

Un archivo de configuración con parámetros de Kaspersky Endpoint Security le permite realizar las siguientes tareas:

- Realizar la instalación local de Kaspersky Endpoint Security mediante la línea de comandos con la configuración predefinida.

- Realizar 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 a otro (consulte las instrucciones a continuación).

Exportar un archivo de configuración

Para crear un archivo de configuración:

1. En la ventana principal de la aplicación 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. En la ventana que se abre, especifique la ruta en la cual desea guardar el archivo de configuración e ingrese su nombre.

   Para usar el archivo de configuración con el objetivo de instalar Kaspersky Endpoint Security de forma local o remota, debe llamarlo install.cfg.

5. Si es necesario, ingrese una contraseña para exportar la configuración de la aplicación en un archivo.

   Para guardar el archivo de configuración, debe habilitar la protección con contraseña. El usuario debe tener el permiso **Exportar configuración**.

6. Guarde el archivo.

De esta forma, la aplicación crea un archivo de configuración. Es posible que el archivo de configuración contenga datos de la cuenta del usuario, por este motivo, Kaspersky Endpoint Security cifra el archivo. Un archivo de configuración no es editable. Cualquier intento de modificar un archivo de configuración lo dañará.

Importar un archivo de configuración

Es posible que los archivos de configuración contengan datos de las cuentas de usuario agregadas a la aplicación. Si importa un archivo de configuración en el mismo equipo donde se creó, Kaspersky Endpoint Security importa las contraseñas de las cuentas de usuario. Si importa el archivo en un equipo diferente, debe ingresar las contraseñas de forma manual.

Al importar un archivo de configuración, Kaspersky Endpoint Security no transfiere contraseñas de criptocontenedores. Si utiliza la autenticación bidireccional al conectarse a los servidores, debe especificar las contraseñas del criptocontenedor desde cero.

Para importar parámetros de Kaspersky Endpoint Security desde un archivo de configuración:

1. En la ventana principal de la aplicación 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, escriba la ruta de acceso al archivo de configuración.

5. Abra el archivo.

Todos los valores de los parámetros de Kaspersky Endpoint Security se definirán conforme al archivo de configuración seleccionado.

Administración de la configuración de la aplicación

Restauración de la configuración predeterminada de la aplicación

Puede restaurar la configuración de la aplicación recomendada por Kaspersky en cualquier momento. Después de restaurar 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 principal de la aplicación 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.

Administración de la configuración de la aplicación

Rendimiento de Kaspersky Endpoint Security y su compatibilidad con otras aplicaciones

El rendimiento de Kaspersky Endpoint Security se refiere a la cantidad de tipos de objetos que pueden dañar el equipo y se pueden detectar, así como también al consumo energético y el uso de los recursos del equipo.

Selección de tipos de objetos detectables

Kaspersky Endpoint Security le permite personalizar la protección de su equipo y seleccionar los tipos de objetos que detecta la aplicación durante su funcionamiento. Kaspersky Endpoint Security siempre analiza el sistema operativo en busca de virus, gusanos y troyanos. No puede deshabilitar el análisis en busca de estos tipos de objetos. Este tipo de malware puede causar daños significativos al equipo. Para lograr una mayor seguridad del equipo, puede expandir la gama de tipos de objetos detectables habilitando la supervisión de software legal que los delincuentes pueden usar para dañar el equipo o los datos personales.

Uso del modo de ahorro de energía

El consumo energético de las aplicaciones es un aspecto de gran importancia en el caso de los equipos portátiles. Las tareas programadas de Kaspersky Endpoint Security consumen habitualmente una cantidad significativa de recursos. Cuando el equipo funciona con carga de batería, se puede utilizar el modo de ahorro de energía para moderar el consumo.

En el modo de ahorro de energía, las siguientes tareas programadas se posponen automáticamente:

- Tarea de Análisis completo.
- Tarea de Análisis de áreas críticas.
- Tarea de Análisis personalizado.
- Tarea de Comprobación de integridad.

Dependiendo de si el modo de ahorro de energía está o no habilitado, Kaspersky Endpoint Security detiene las tareas de cifrado cuando un equipo portátil se pasa a funcionar con carga de batería. La aplicación reanuda las tareas de cifrado cuando el equipo portátil pasa de alimentación por batería a la alimentación por la red eléctrica.

Dispensación de recursos del equipo a otras aplicaciones

Es posible que el consumo de recursos del equipo al analizarlo aumente la carga de la CPU y de los subsistemas del disco duro. Para resolver el problema del funcionamiento simultáneo durante períodos de mayor carga en la CPU y en los subsistemas del disco duro, Kaspersky Endpoint Security puede conceder recursos a otras aplicaciones.

Uso de tecnología de desinfección avanzada

Las aplicaciones malintencionadas modernas pueden penetrar los niveles más bajos del sistema operativo. Ello las hace casi imposibles de eliminar. Cuando detecta actividades malintencionadas en el sistema operativo, Kaspersky Endpoint Security realiza un procedimiento de desinfección exhaustivo con una tecnología especial. La *tecnología de desinfección avanzada* está diseñada para purgar el sistema operativo de aplicaciones malintencionadas que ya se han ejecutado y se han cargado en la RAM, y que Kaspersky Endpoint Security no puede eliminar por otros medios. Como resultado, se neutraliza la amenaza. Mientras está en curso la desinfección avanzada, se le advierte que no inicie nuevos procesos ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada consume una cantidad significativa de recursos del sistema, lo que puede ralentizar otras aplicaciones.

Una vez completado el proceso de desinfección avanzada en un equipo 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 una análisis completo "ligero" del equipo.

Por motivos inherentes al diseño de Kaspersky Endpoint Security, no es posible mostrar una solicitud de reinicio en equipos con Microsoft Windows para servidores. El reinicio no planificado de un servidor de archivos puede generar problemas relacionados con la no disponibilidad temporal de los datos del servidor de archivos o la pérdida de los datos sin guardar. Se recomienda reiniciar un servidor de archivos estrictamente de acuerdo con lo programado. Por este motivo, la tecnología de desinfección avanzada está desactivada de forma predeterminada para servidores de archivos.

Si se detecta una infección activa en un servidor de archivos, se envía un evento a Kaspersky Security Center en el que se indica que se necesita una desinfección avanzada. Para atacar una infección activa en un servidor, habilite la tecnología de desinfección avanzada para servidores y, cuando resulte conveniente para los usuarios del servidor, inicie una tarea de grupo *Análisis de malware*.

Activación o desactivación del modo de ahorro de energía

El *Modo de ahorro de energía* es una funcionalidad que reduce la carga sobre los recursos del equipo portátil y prolonga la duración de la batería sin comprometer significativamente el nivel de seguridad. En el modo de ahorro de energía, la aplicación limita la ejecución de tareas programadas. De esta manera, el modo de ahorro de energía garantiza un equilibrio entre el nivel de seguridad y la duración de la batería del equipo portátil.

Cuando el modo de ahorro de energía está activado y el equipo está funcionando con alimentación de la batería, las siguientes tareas no se ejecutan, incluso si estuvieran programadas:

- *Análisis completo*.
- *Análisis de áreas críticas*.
- *Análisis personalizado*.
- *Comprobación de integridad de la aplicación*.
- *Análisis de IOC*.
- *Actualización de bases de datos y módulos de la aplicación* (solo parches)

La aplicación omite las actualizaciones programadas de la base de datos únicamente cuando el equipo portátil funciona con batería y el nivel de carga es inferior al 30 %. En todos los demás casos, Kaspersky Endpoint Security actualiza las bases de datos según lo programado, independientemente de si el equipo portátil está conectado a la corriente o funciona con batería, o de si la aplicación se encuentra en modo de ahorro de energía.

Cómo habilitar o deshabilitar 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 correspondiente 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 **Posponer las tareas programadas cuando el equipo funciona con carga de batería** para habilitar o deshabilitar el modo de ahorro de energía.

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

Cómo habilitar o deshabilitar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Rendimiento**.

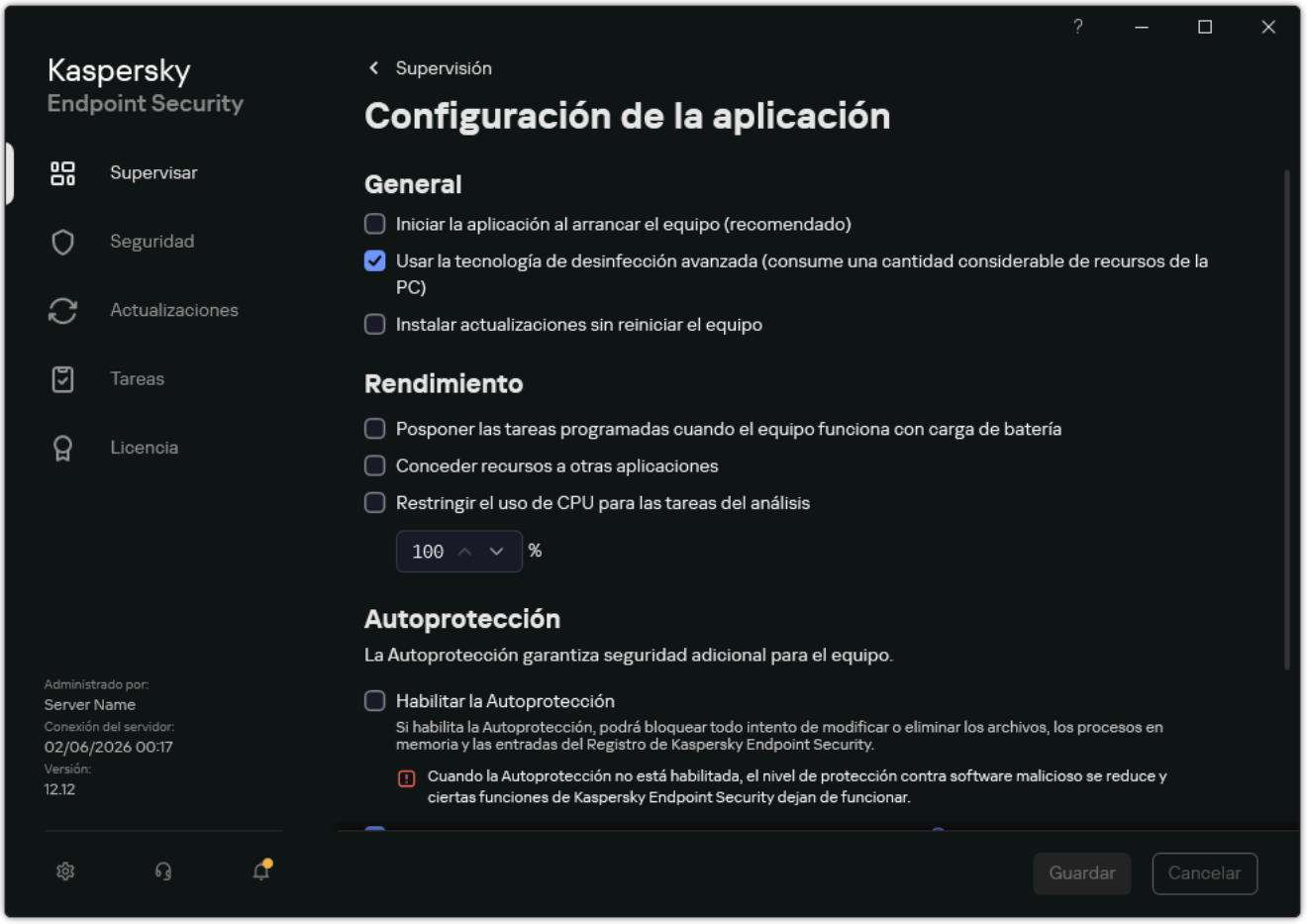
5. En el bloque **Posponer u omitir las tareas programadas cuando el equipo funciona con carga de batería**, use la casilla **Posponer u omitir las tareas programadas cuando el equipo funciona con carga de batería (según el SO)** para habilitar o deshabilitar el modo de ahorro de energía.

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

Cómo habilitar o deshabilitar el modo de ahorro de energía en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 **Posponer las tareas programadas cuando el equipo funciona con carga de batería** para habilitar o deshabilitar el modo de ahorro de energía.

4. Guarde los cambios.

Activación o desactivación de la dispensación de recursos para otras aplicaciones

Es posible que el consumo de recursos del equipo por parte de Kaspersky Endpoint Security al analizar el equipo aumente la carga de la CPU y de los subsistemas del disco duro. Esto puede ralentizar otras aplicaciones. Para optimizar el rendimiento, Kaspersky Endpoint Security proporciona un *modo para transferir recursos a otras aplicaciones*. En este modo, el sistema operativo puede dar menos prioridad a los subprocesos de la tarea de análisis de Kaspersky Endpoint Security cuando la carga de la CPU sea alta. Esto permite redistribuir los recursos del sistema operativo a otras aplicaciones. De este modo, las tareas de análisis recibirán menos tiempo de CPU. Por consiguiente, Kaspersky Endpoint Security tardará más tiempo en analizar el equipo. Por defecto, la aplicación está configurada para dispensar recursos para otras aplicaciones.

Cómo habilitar o deshabilitar 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 correspondiente 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 **Conceder recursos a otras aplicaciones** para habilitar o deshabilitar la concesión de recursos a otras aplicaciones.

5. Guarde los cambios.

Cómo habilitar o deshabilitar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Rendimiento**.

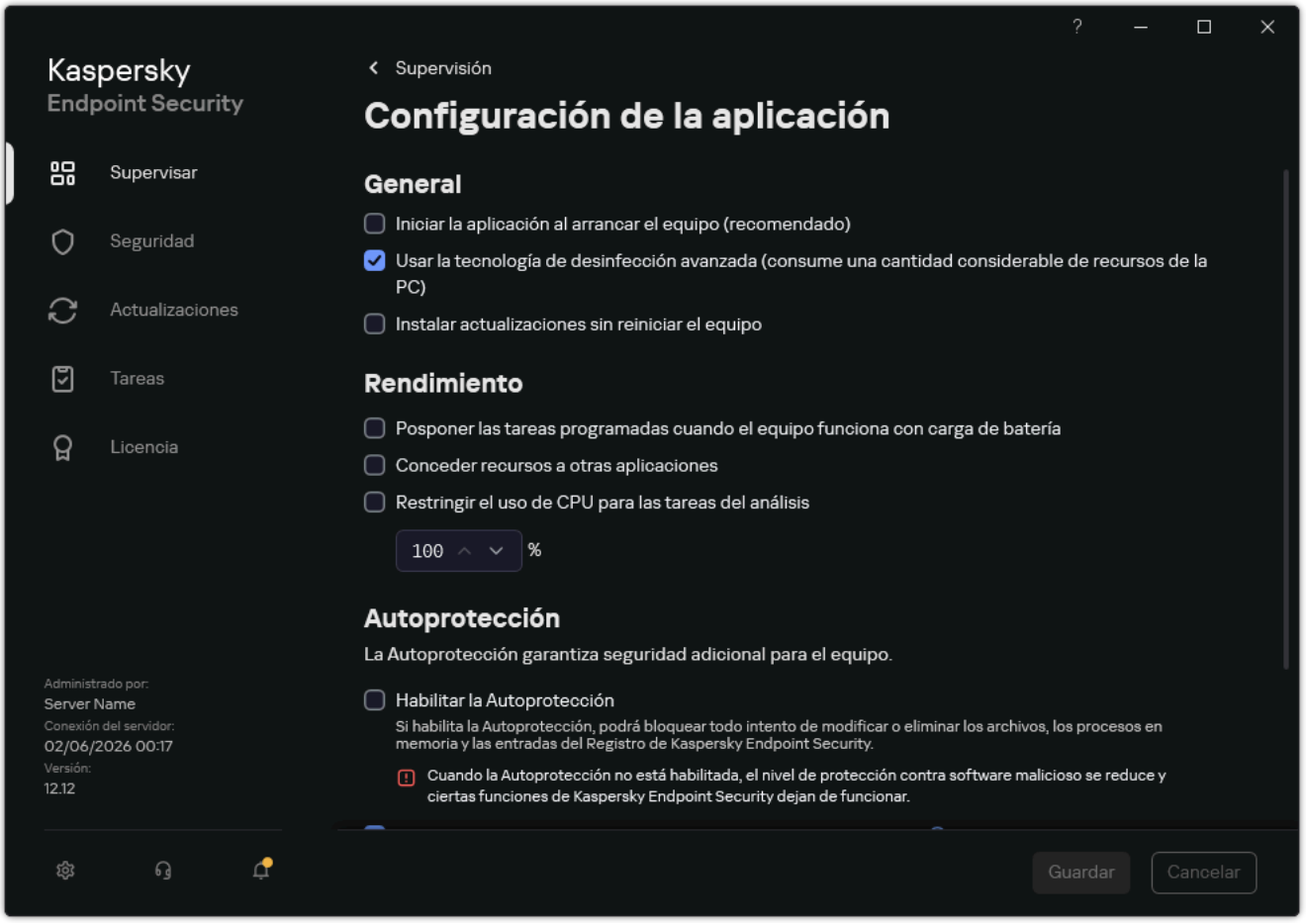
5. En el bloque **Conceder recursos a otras aplicaciones**, utilice el interruptor **Conceder recursos a otras aplicaciones** para habilitar o deshabilitar la concesión de recursos a otras aplicaciones.

6. Guarde los cambios.

Cómo habilitar o deshabilitar la concesión de recursos a otras aplicaciones en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 **Conceder recursos a otras aplicaciones** para habilitar o deshabilitar la concesión de recursos a otras aplicaciones.

4. Guarde los cambios.

Prácticas recomendadas para optimizar el rendimiento de Kaspersky Endpoint Security

Al desplegar Kaspersky Endpoint Security para Windows, puede utilizar las siguientes recomendaciones para configurar la protección y optimizar el rendimiento del equipo. Para obtener más información sobre cómo solucionar problemas de rendimiento del equipo, consulte la Base de conocimientos del Servicio de soporte técnico.

General

Configure los ajustes generales de la aplicación de acuerdo con las siguientes recomendaciones:

1. Actualice Kaspersky Endpoint Security a la última versión.

   Las versiones más recientes de la aplicación tienen errores corregidos, estabilidad mejorada y rendimiento optimizado.

2. Habilite los componentes de protección con la configuración predeterminada.

   Los ajustes predeterminados se consideran óptimos. Esta configuración está recomendada por los expertos de Kaspersky. 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. Habilite 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 habilitadas.

Análisis de malware en estaciones de trabajo

Se recomienda habilitar el Análisis en segundo plano para el análisis de malware en estaciones de trabajo. *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 Análisis completo, 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 inicio, la memoria del sistema y la partición del sistema. La configuración del análisis en segundo plano se considera óptima. Esta configuración está recomendada por los expertos de Kaspersky. Por lo tanto, para realizar un Análisis de malware en el 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 de *Análisis de malware* de acuerdo con las siguientes recomendaciones:

1. Establecer un límite en el consumo de recursos de la CPU al analizar el equipo.

   Puede limitar el uso de la CPU al ejecutar la tarea *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 mientras se analiza el equipo. Esto puede aumentar el tiempo que toma analizar el equipo.

2. Configurar el programa de análisis del equipo óptimo.

   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 de atención, puede habilitar la función Wake-on-LAN. La característica Wake-on-LAN permite encender el equipo de forma remota mediante el envío de una señal especial a través de la red local. Para utilizarla, debe habilitar Wake-on-LAN en la configuración del BIOS. También puede hacer que el equipo se apague automáticamente después de que 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 el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió.

3. Definir un alcance del análisis.

   Seleccione los siguientes objetos para el análisis (conjunto mínimo de alcances del análisis):

   - Memoria del núcleo
   - Procesos en ejecución y objetos de inicio
   - Sectores de inicio
   - %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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

   Solo puede activar las tecnologías iSwift y 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. Deshabilitar el análisis de archivos de almacenamiento protegidos con contraseña.

   Si el análisis de archivos de almacenamiento protegidos con contraseña está habilitado, se muestra una solicitud de contraseña antes de analizar el archivo de almacenamiento. Debido a que se recomienda programar la tarea fuera del horario de oficina, el usuario no puede ingresar la contraseña. Puede analizar archivos de almacenamiento protegidos con contraseña manualmente.

6. Deshabilitar el inicio simultáneo de varias tareas de análisis.

   Kaspersky Endpoint Security pondrá en cola las nuevas tareas de análisis si continúa el análisis actual. Esto permite optimizar la carga en el equipo.

Análisis de malware en los servidores

Configurar la tarea de *Análisis de malware* de acuerdo con las siguientes recomendaciones:

1. Establecer un límite en el consumo de recursos de la CPU al analizar el equipo.

   Puede limitar el uso de la CPU al ejecutar la tarea *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 mientras se analiza el equipo. Esto puede aumentar el tiempo que toma analizar el equipo.

2. Configurar el programa de análisis del equipo óptimo.

   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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

   Solo puede activar las tecnologías iSwift y 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. Deshabilitar el análisis de archivos de almacenamiento protegidos con contraseña.

   Si el análisis de archivos de almacenamiento protegidos con contraseña está habilitado, se muestra una solicitud de contraseña antes de analizar el archivo de almacenamiento. Debido a que se recomienda programar la tarea fuera del horario de oficina, el usuario no puede ingresar la contraseña. Puede analizar archivos de almacenamiento protegidos con contraseña manualmente.

5. Deshabilitar el inicio simultáneo de varias tareas de análisis.

   Kaspersky Endpoint Security pondrá en cola las nuevas tareas de análisis si continúa el análisis actual. Esto permite 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 los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, los servicios KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web analizadas, así como información sobre la categoría y la reputación de los archivos analizados.

Edite la configuración de Kaspersky Security Network de acuerdo con las siguientes recomendaciones:

1. Deshabilite el modo KSN extendido.

   El *modo KSN extendido* es un modo por el cual Kaspersky Endpoint Security remite información adicional a Kaspersky.

2. Configurar Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN). A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky.

3. Habilite el 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 de malware

Un análisis de malware es vital para la seguridad de su equipo. Ejecutados en forma regular, los análisis de malware descartan la posibilidad de que se distribuya el malware que no hayan detectado los componentes de protección debido a que se configuró un nivel de seguridad bajo o por otros motivos.

Si el contenido de un archivo está almacenado en la nube de OneDrive, Kaspersky Endpoint Security no lo analizará y creará una entrada en el registro para indicar que el archivo no fue analizado.

Análisis completo

Análisis detallado de todo el equipo. Kaspersky Endpoint Security analiza los siguientes objetos:

- Memoria del núcleo
- Objetos cargados al iniciar el sistema operativo
- Sectores de inicio
- Copia de seguridad del sistema operativo
- Todos los discos rígidos y discos extraíbles

Los especialistas de Kaspersky recomiendan no modificar el alcance 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 un 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 kernel, los procesos en ejecución y los sectores de inicio del disco.

Los especialistas de Kaspersky recomiendan no modificar el alcance del análisis de la tarea *Análisis de áreas críticas*.

Análisis personalizado

Kaspersky Endpoint Security analiza los objetos que selecciona el usuario. Puede analizar cualquier objeto de la siguiente lista:

- Memoria del sistema
- Objetos cargados al iniciar el sistema operativo
- Copia de seguridad del sistema operativo
- los discos duros, las unidades extraíbles y las unidades de red
- Cualquier archivo seleccionado

Análisis en segundo plano

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 Análisis completo, 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 inicio, la memoria del sistema y la partición del sistema.

Comprobación de integridad de la aplicación

Kaspersky Endpoint Security comprueba si los módulos de la aplicación presentan fallas o modificaciones.

Análisis del equipo

Un análisis es vital para la seguridad de su equipo. Ejecutados en forma regular, los análisis de malware descartan la posibilidad de que se distribuya el malware que no hayan detectado los componentes de protección debido a que se configuró un nivel de seguridad bajo o por otros motivos. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Kaspersky Endpoint Security tiene las siguientes tareas estándar predefinidas: *Análisis completo*, *Análisis de áreas críticas*, *Análisis personalizado*. Si su organización tiene implementado el sistema de administración de Kaspersky Security Center, puede crear una tarea *Análisis de malware* 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 *Análisis de malware*.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.

5. Configure la tarea de análisis (vea la tabla de más abajo).

   Si es necesario, configure la programación de la tarea de análisis.

6. Guarde los cambios.

7. Ejecute la tarea de análisis.

Kaspersky Endpoint Security comenzará a analizar el equipo. Si el usuario interrumpió la ejecución de la tarea (por ejemplo, apagando el equipo), Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió el análisis.

Cómo ejecutar una tarea de análisis con 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 de propiedades de la tarea.

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

4. Configure la tarea de análisis (vea la tabla de más abajo).

   Si es necesario, configure la programación de la tarea de análisis.

5. Guarde los cambios.

6. Ejecute la tarea de análisis.

Kaspersky Endpoint Security comenzará a analizar el equipo. Si el usuario interrumpió la ejecución de la tarea (por ejemplo, apagando el equipo), Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa 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 ⚙.

3. Configure la tarea de análisis (vea la tabla de más abajo).

   Si es necesario, configure la programación de la tarea de análisis.

4. Guarde los cambios.

5. Ejecute la tarea de análisis.

Kaspersky Endpoint Security comenzará a analizar el equipo. La aplicación mostrará el progreso del análisis, la cantidad de archivos analizados y el tiempo de análisis restante. Para detener la tarea en cualquier momento, haga clic en el botón **Detener**. Si no se muestra la tarea de análisis, significa que el administrador prohibió el uso de tareas locales en la directiva.

Para optimizar el rendimiento de Kaspersky Endpoint Security mientras analiza 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 usar 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 pudo desinfectar. La aplicación elimina el archivo infectado después de reiniciar el equipo.
- **Registrado**. El archivo infectado no se pudo desinfectar. La aplicación agrega información sobre los archivos infectados detectados a la lista de amenazas activas.
- **Escritura no admitida** o **Error de escritura**. El archivo infectado no se pudo desinfectar. La aplicación no tiene acceso de escritura.
- **Ya se procesó**. La aplicación detectó un archivo infectado antes. 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 configuraciones para ejecutar un análisis. Estos grupos de configuraciones que se almacenan 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 de almacenamiento, paquetes de distribución, archivos en formatos de oficina, pero no analiza los archivos de almacenamiento protegidos con contraseña. Al establecer 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 de almacenamiento, paquetes de distribución, archivos en formatos de oficina, pero no analiza los archivos de almacenamiento protegidos con contraseña. Al establecer 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 de almacenamiento, paquetes de distribución, archivos en formatos de oficina, pero no analiza los archivos de almacenamiento protegidos con contraseña. Al establecer 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 del nivel de seguridad recomendada.

Parámetro	Descripción
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo. **Desinfectar; informar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección falla, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas. **Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos. 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 si se puede desinfectar en el futuro. Si se detectan archivos infectados que forman parte de la aplicación Windows Store, Kaspersky Endpoint Security intenta eliminarlos.
Ejecutar la desinfección avanzada inmediatamente *(disponible solo en la Consola de Kaspersky Security Center)*	La Desinfección avanzada durante una tarea de análisis antivirus en un equipo solo se realiza si la función Desinfección avanzada está habilitada en las propiedades de la directiva que se aplica al equipo. Si la casilla está seleccionada, 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 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 activa 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.
Alcance del análisis	Lista de objetos que analiza Kaspersky Endpoint Security cuando realiza una tarea de análisis. Los objetos dentro del alcance del análisis pueden incluir la memoria Kernel, procesos en ejecución, sectores de arranque, almacenamiento de copias de seguridad del sistema, discos duros, unidades extraíbles o unidades de red, una carpeta o un archivo. En Kaspersky Endpoint Security para Windows 12.12, se excluye el correo electrónico del alcance del análisis de la aplicación. El análisis de los mensajes de correo electrónico entrantes y salientes lo realiza el componente Protección contra amenazas de correo. Si está utilizando una versión anterior del complemento de administración, la aplicación excluye el correo electrónico del alcance del análisis, aunque la directiva lo incluya.
Programar análisis	**Manualmente**. Modo de ejecución en el que puede iniciar el análisis manualmente en el momento que sea conveniente para usted. **Mediante programación**. En este modo de ejecución de la tarea de análisis, la aplicación inicia la tarea de análisis de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de análisis, también puede iniciar manualmente la tarea de análisis.
Posponer la ejecución después del inicio de la aplicación durante N minutes	Inicio pospuesto de la tarea de análisis después de iniciar la aplicación. Al iniciar el sistema operativo, se ejecutan muchos procesos, por lo que es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después de iniciar Kaspersky Endpoint Security.
Ejecutar tareas omitidas	Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea omitida tan pronto como sea posible. La tarea puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas no realizadas, las ejecuta aleatoriamente dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si la casilla está desactivada, Kaspersky Endpoint Security no ejecuta las tareas omitidas. En lugar de eso, ejecuta la siguiente tarea según la programación actual.

Parámetro	Descripción
Ejecutar solo cuando el equipo esté inactivo	Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando el equipo está en uso.
Ejecutar el análisis como	De forma predeterminada, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. El alcance de la protección puede incluir unidades de red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que posea los derechos requeridos en la configuración de la aplicación y ejecutar la tarea de análisis con la cuenta de este 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 archivo que seleccione para analizar. **Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones). **Archivos analizados según su formato**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, 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 según su extensión**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión. De forma predeterminada, Kaspersky Endpoint Security analiza los archivos por 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 archivos potencialmente infectables (por ejemplo, `.123`).
Analizar solo 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 compuestos.
Omitir archivo que se analice durante más de N segundo(s)	Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.
No ejecutar varias tareas de análisis al mismo tiempo	Inicio pospuesto de tareas de análisis si ya se está ejecutando un análisis. Kaspersky Endpoint Security pondrá en cola las nuevas tareas de análisis si continúa el análisis actual. Esto permite optimizar la carga en el equipo. Por ejemplo, supongamos que la aplicación inició una tarea Análisis completo según la programación. Si un usuario intenta iniciar un análisis rápido desde la interfaz de la aplicación, Kaspersky Endpoint Security pondrá en cola esta tarea de análisis rápido y la iniciará automáticamente una vez finalizada la tarea de análisis completo. Sin embargo, Kaspersky Endpoint Security inicia de inmediato una tarea de análisis incluso si se está ejecutando una de las siguientes tareas de análisis: • Análisis de unidades extraíbles en la conexión. • Análisis desde el menú contextual. • Análisis de áreas críticas que se inició durante la detección de un indicador de compromiso (IoC). Si esta casilla de verificación está desactivada, Kaspersky Endpoint Security le permite ejecutar varias tareas de análisis al mismo tiempo. La ejecución de varias tareas de análisis requiere más recursos de procesamiento.
Analizar archivos de almacenamiento	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos de Microsoft Office	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.

Parámetro	Descripción
Analizar archivos de formato de correo electrónico	Análisis de archivos de 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 de cliente de correo Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de Microsoft Outlook (archivos PST y OST) si está instalada una versión de Microsoft Outlook de 64 bits en el equipo, incluso si el correo está incluido en el alcance del análisis. Si la casilla está seleccionada, Kaspersky Endpoint Security divide el archivo de formato de correo en sus componentes (encabezado, cuerpo, archivos adjuntos) y lo analiza en busca de amenazas. Si se desactiva la casilla, Kaspersky Endpoint Security analiza el archivo de formato de correo como si fuera un único archivo. Si se descubre un objeto malicioso en archivos PST u OST, Kaspersky Endpoint Security lo convierte en un archivo inofensivo según la acción seleccionada (por ejemplo, mediante la desinfección o eliminación del archivo). Si se detecta un archivo malicioso en archivos de otros clientes de correo (por ejemplo, Mozilla Thunderbird), Kaspersky Endpoint Security solo marca el mensaje infectado. Debe eliminar el mensaje que contiene el archivo adjunto infectado de forma manual.
Analizar archivos de almacenamiento con contraseña	Si la casilla está seleccionada, la aplicación analiza los archivos de almacenamiento con contraseña. Para analizar los archivos de un archivo de almacenamiento, se le solicitará que escriba la contraseña. Si se desactiva la casilla de verificación, la aplicación ignorará el análisis de los archivos de almacenamiento protegidos con contraseña.
No desempaquetar archivos compuestos de gran tamaño	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada o no.
Aprendizaje automático y análisis de firmas	El método aprendizaje automático y análisis de firmas usa las bases de datos de Kaspersky Endpoint Security que contienen descripciones de las amenazas conocidas y las formas para neutralizarlas. La protección que usa este método proporciona el nivel de seguridad mínimo aceptable. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado.
Análisis heurístico	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Análisis de unidades extraíbles cuando se conectan al equipo

Kaspersky Endpoint Security analiza todos los archivos que ejecuta o copia, incluso si el archivo está ubicado en una unidad extraíble (componente Protección contra archivos peligrosos). Para evitar la propagación de virus y otros programas malintencionados, puede configurar análisis automáticos de unidades extraíbles cuando están conectadas al equipo. Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos. El componente mantiene un equipo seguro mediante la ejecución de análisis que implementan aprendizaje automático, análisis heurístico (nivel alto) y análisis de firmas. Kaspersky Endpoint Security también utiliza las tecnologías de optimización de análisis iSwift e iChecker. Estas tecnologías están siempre activas y no se pueden deshabilitar.

Cómo configurar la ejecución del análisis de unidades extraíbles 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 correspondiente 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 en una conexión de unidad extraíble**, seleccione **Análisis detallado** o **Análisis rápido**.
5. Configure las opciones avanzadas para el análisis de unidades extraíbles (vea la tabla de más abajo).
6. Guarde los cambios.

Cómo configurar la ejecución del análisis de unidades extraíbles a través de 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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Análisis de unidades extraíbles**.
5. Use el interruptor **Análisis de unidades extraíbles HABILITADO** para habilitar o deshabilitar 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 (vea la tabla de más abajo).
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 el interruptor **Análisis de unidades extraíbles** para habilitar o deshabilitar los análisis de unidades extraíbles al conectarse al equipo.

4. Configure las opciones avanzadas para el análisis de unidades extraíbles (vea la tabla de más abajo).

5. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security ejecuta un análisis de unidades extraíbles en busca de unidades extraíbles que no superen el tamaño máximo especificado. Si no se muestra la tarea *Análisis de unidades extraíbles*, significa que el administrador prohibió 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 cuando se conecta una unidad extraíble, incluidos los archivos dentro de objetos compuestos, los archivos de almacenamiento, los paquetes de distribución y los archivos con formato de Office. Kaspersky Endpoint Security no analiza archivos en formatos de correo o archivos protegidos con contraseña. **Análisis rápido**. Si esta opción está seleccionada, cuando se conecte una unidad extraíble, Kaspersky Endpoint Security analizará únicamente los archivos de formatos específicos que sean los más propensos a estar infectados. Los objetos compuestos no se desempaquetarán.
Tamaño máximo de la unidad (MB)	Si se selecciona esta casilla, Kaspersky Endpoint Security realiza la acción seleccionada en unidades extraíbles cuyo tamaño no supere el tamaño máximo de unidad especificado. 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 se selecciona la casilla, Kaspersky Endpoint Security muestra el progreso de análisis de las unidades extraíbles en una ventana independiente y en la sección **Tareas**. Si la casilla se desactiva, Kaspersky Endpoint Security realiza los análisis de las unidades extraíbles en segundo plano.
Evitar que los usuarios detengan el análisis	Si esta casilla está seleccionada, entonces el botón **Detener** en la sección **Tareas** y el botón **Detener** en la ventana de análisis de unidades extraíbles no están disponibles para la tarea de análisis de unidades extraíbles en la interfaz local de Kaspersky Endpoint Security.

Análisis en segundo plano

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 Análisis completo, 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 inicio, 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 un análisis completo. El nivel de seguridad del equipo no se verá afectado. Estas tareas tienen el mismo alcance de análisis. Para optimizar la carga en el equipo, la aplicación no ejecuta una tarea Análisis completo y una tarea Análisis en segundo plano al mismo tiempo. Si ya ejecutó una tarea Análisis completo, Kaspersky Endpoint Security no iniciará una tarea Análisis en segundo plano hasta siete días después de que se complete la tarea Análisis completo.

La aplicación inicia un análisis en segundo plano en los siguientes casos:

- Después de que se actualizan las bases de datos antivirus.
- Cuando Kaspersky Endpoint Security se ha estado ejecutando por treinta 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).

Si se inicia un análisis en segundo plano porque el equipo ha quedado inactivo, pero ocurre cualquiera de las siguientes situaciones, el análisis se interrumpirá:

- el equipo pasa al modo activo;

  El análisis en segundo plano no se interrumpirá si es la primera vez en más de diez días que se lo ejecuta.

- el equipo (portátil) comienza a funcionar con 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 habilitar el análisis en segundo plano 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 correspondiente 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. Use la casilla **Habilitar Análisis en segundo plano** para habilitar o deshabilitar esta característica.
5. Guarde los cambios.

Cómo habilitar el análisis en segundo plano con 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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Protección contra amenazas de archivo**.
5. En **Análisis en segundo plano**, use el interruptor **Análisis en segundo plano HABILITADO** para habilitar o deshabilitar el análisis en segundo plano.
6. Guarde los cambios.

Cómo habilitar el análisis en segundo plano mediante 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 habilitar o deshabilitar esta característica.

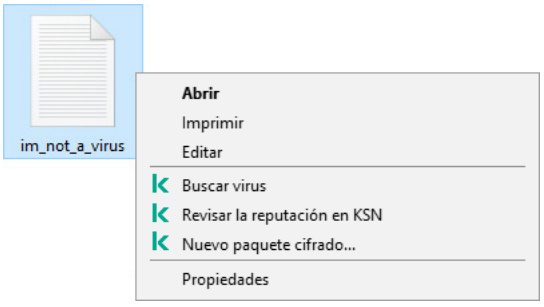
4. Guarde los cambios.

Si no se muestra *Análisis en segundo plano*, significa que el administrador prohibió el uso de tareas locales en la directiva.

Análisis 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.



Análisis desde el menú contextual

Cómo configurar Análisis 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 correspondiente 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 Análisis desde el menú contextual (vea la tabla de más abajo).

5. Guarde los cambios.

Cómo configurar Análisis desde el menú contextual a través de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Protección contra amenazas de archivo**.

5. En **Análisis desde el menú contextual**, configure Análisis desde el menú contextual (consulte la tabla a continuación).

6. Guarde los cambios.

Cómo configurar Análisis 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 Análisis desde el menú contextual (vea la tabla de más abajo).

4. Guarde los cambios.

Si no se muestra la tarea *Análisis desde el menú contextual*, significa que el administrador prohibió el uso de tareas locales en la directiva.

Analizar desde la configuración de tareas del menú contextual

Parámetro	Descripción
Nivel de seguridad	Kaspersky Endpoint Security puede usar diferentes grupos de configuraciones para ejecutar un análisis. Estos grupos de configuraciones que se almacenan 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 de almacenamiento, paquetes de distribución, archivos en formatos de oficina, pero no analiza los archivos de almacenamiento protegidos con contraseña. Al establecer 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 de almacenamiento, paquetes de distribución, archivos en formatos de oficina, pero no analiza los archivos de almacenamiento protegidos con contraseña. Al establecer 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 de almacenamiento, paquetes de distribución, archivos en formatos de oficina, pero no analiza los archivos de almacenamiento protegidos con contraseña. Al establecer 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 falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo. **Desinfectar; informar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección falla, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas. **Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.
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 archivo que seleccione para analizar. **Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones). **Archivos analizados según su formato**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, 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 según su extensión**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión. De forma predeterminada, Kaspersky Endpoint Security analiza los archivos por 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 archivos potencialmente infectables (por ejemplo, `.123`).
Analizar solo 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 compuestos.
Omitir archivo que se analice durante más de N segundo(s)	Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.

Parámetro	Descripción
Analizar archivos de almacenamiento	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar paquetes de distribución	La casilla habilita o deshabilita el análisis de los paquetes de distribución.
Analizar archivos de Microsoft Office	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.
Analizar archivos de formato de correo electrónico	Análisis de archivos de 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 de cliente de correo Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de Microsoft Outlook (archivos PST y OST) si está instalada una versión de Microsoft Outlook de 64 bits en el equipo, incluso si el correo está incluido en el alcance del análisis. Si la casilla está seleccionada, Kaspersky Endpoint Security divide el archivo de formato de correo en sus componentes (encabezado, cuerpo, archivos adjuntos) y lo analiza en busca de amenazas. Si se desactiva la casilla, Kaspersky Endpoint Security analiza el archivo de formato de correo como si fuera un único archivo. Si se descubre un objeto malicioso en archivos PST u OST, Kaspersky Endpoint Security lo convierte en un archivo inofensivo según la acción seleccionada (por ejemplo, mediante la desinfección o eliminación del archivo). Si se detecta un archivo malicioso en archivos de otros clientes de correo (por ejemplo, Mozilla Thunderbird), Kaspersky Endpoint Security solo marca el mensaje infectado. Debe eliminar el mensaje que contiene el archivo adjunto infectado de forma manual.
Analizar archivos de almacenamiento con contraseña	Si la casilla está seleccionada, la aplicación analiza los archivos de almacenamiento con contraseña. Para analizar los archivos de un archivo de almacenamiento, se le solicitará que escriba la contraseña. Si se desactiva la casilla de verificación, la aplicación ignorará el análisis de los archivos de almacenamiento protegidos con contraseña.
No desempaquetar archivos compuestos de gran tamaño	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada o no.
Aprendizaje automático y análisis de firmas	El método aprendizaje automático y análisis de firmas usa las bases de datos de Kaspersky Endpoint Security que contienen descripciones de las amenazas conocidas y las formas para neutralizarlas. La protección que usa este método proporciona el nivel de seguridad mínimo aceptable. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado.
Análisis heurístico	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.
Tecnología iSwift	Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Comprobación de integridad de la aplicación

Kaspersky Endpoint Security comprueba si los módulos de la aplicación presentan fallas 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* con Kaspersky Security Center Web Console o mediante la Consola de administración. No es posible crear esta tarea con 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 la aplicación a través de 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Programación de la tarea

Programe la ejecución de la tarea. Puede hacer que la tarea se inicie manualmente o cuando se detecte un brote de virus, por ejemplo.

Paso 4. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Comprobar la integridad de la aplicación tras una infección*.

Paso 5. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. 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 compruebe en forma programada (vea la tabla de más abajo).

Cómo ejecutar una comprobación de integridad de la aplicación a través de Web Console

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del 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 compruebe en forma programada (vea la tabla de más abajo).

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 compruebe en forma programada (vea la tabla de más abajo). Si no se muestra la tarea *Comprobación de integridad de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

Configuración de la tarea Comprobación de integridad

Parámetro	Descripción
Programar análisis	**Manualmente**. Modo de ejecución en el que puede iniciar el análisis manualmente en el momento que sea conveniente para usted. **Mediante programación**. En este modo de ejecución de la tarea de análisis, la aplicación inicia la tarea de análisis de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de análisis, también puede iniciar manualmente la tarea de análisis.
Ejecutar tareas omitidas	Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea omitida tan pronto como sea posible. La tarea puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas no realizadas, las ejecuta aleatoriamente dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si la casilla está desactivada, Kaspersky Endpoint Security no ejecuta las tareas omitidas. En lugar de eso, ejecuta la siguiente tarea según la programación actual.
Ejecutar solo cuando el equipo esté inactivo	Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando el equipo está en uso.

Editar el alcance del análisis

El *Alcance 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 ingresar una máscara.

> Para editar el alcance del análisis, recomendamos usar la tarea *Análisis personalizado*. Los especialistas de Kaspersky recomiendan no modificar el alcance del análisis de las tareas *Análisis completo* y *Análisis de áreas críticas*.

Kaspersky Endpoint Security cuenta con los siguientes objetos predefinidos como parte del alcance del análisis:

- **Memoria del sistema**.
- **Procesos en ejecución y Objetos de inicio**.

  Memoria ocupada por procesos y archivos ejecutables de aplicaciones que se ejecutan al iniciar el sistema.
- **Sectores de inicio del disco**.

  Sectores de inicio 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, se excluye el correo electrónico del alcance del análisis de la aplicación. El análisis de los mensajes de correo electrónico entrantes y salientes lo realiza el componente Protección contra amenazas de correo. Si está utilizando una versión anterior del complemento de administración, la aplicación excluye el correo electrónico del alcance del análisis, aunque la directiva lo incluya.

  > Recomendamos crear una tarea de análisis separada para las analizar unidades de red o carpetas compartidas. En la configuración de la tarea *Análisis de malware*, 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, evitará comprobar el objeto dos veces y mejorará el rendimiento del servidor.

Para excluir carpetas o archivos del alcance del análisis, agregue la carpeta o el archivo a la zona de confianza.

Cómo editar un alcance 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 *Análisis de malware*.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.

5. En la sección **Alcance del análisis**, haga clic en **Configuración**.

6. En la ventana que se abre, seleccione los objetos que desea agregar al alcance del análisis o excluir de este.

7. Si quiere agregar un objeto nuevo al alcance del análisis:

   a. Haga clic en **Agregar**.

   b. En el campo **Objeto**, escriba la ruta del archivo o la carpeta.

      Usar máscaras:

      - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

      - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras en cualquier parte de la ruta de acceso a una carpeta o un archivo. Por ejemplo, si desea que el alcance del análisis incluya la carpeta Descargas para todas las cuentas de usuario del equipo, escriba la máscara `C:\Users\*\Downloads\`.

      El objeto **Este equipo** en la lista de recursos de la computadora 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 el alcance del análisis. Para hacerlo, desactive la casilla ubicada junto al objeto.

8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo editar un alcance del análisis con 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 de propiedades de la tarea. Si es necesario, cree la tarea *Análisis de malware*.

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

4. En la sección **Alcance del análisis**, seleccione los objetos que desea agregar al alcance del análisis o excluir de él.

5. Si quiere agregar un objeto nuevo al alcance del análisis:

   a. Haga clic en **Agregar**.

   b. Contiene la ruta a la carpeta o al archivo.

      Usar máscaras:

      - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

      - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras en cualquier parte de la ruta de acceso a una carpeta o un archivo. Por ejemplo, si desea que el alcance del análisis incluya la carpeta Descargas para todas las cuentas de usuario del equipo, escriba la máscara `C:\Users\*\Downloads\`.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en el alcance del análisis. Para hacerlo, habilite el conmutador del interruptor junto a este en la posición de apagado.

6. Guarde los cambios.

Cómo editar un alcance 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 el alcance del análisis para otras tareas. Los especialistas de Kaspersky recomiendan no modificar el alcance del análisis de las tareas *Análisis completo* y *Análisis de áreas críticas*.

3. En la ventana que se abre, seleccione los objetos que desea agregar al alcance del análisis.

4. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador prohibió el uso de tareas locales en la directiva.

Ejecutar un análisis programado

La búsqueda de malware con la tarea *Análisis de malware* puede llevar mucho tiempo y aumentar el uso de los recursos del equipo por parte de Kaspersky Endpoint Security. 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 con un horario fijo, puede configurar un análisis del equipo que se ejecute por la noche o los fines de semana. Si no es posible ejecutar la tarea por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha ignorado para que se inicie automáticamente tan pronto como sea posible. Esta función debe usarse con precaución, ya que puede ralentizar las aplicaciones en el equipo del usuario cuando el equipo se enciende por la mañana.

Si no puede determinar una programación de análisis óptima que se adapte a sus necesidades, puede configurar el análisis para que se ejecute 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 del inicio de la aplicación.

  Kaspersky Endpoint Security ejecuta un análisis del equipo cuando haya transcurrido un período de tiempo especificado después del inicio de la aplicación. Al iniciar el sistema operativo, se ejecutan muchos procesos, por lo que es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después de iniciar Kaspersky Endpoint Security.

- Característica 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 característica Wake-on-LAN del sistema operativo. La característica Wake-on-LAN permite encender el equipo de forma remota mediante el envío de una señal especial a través de la red local. Para utilizarla, debe habilitar Wake-on-LAN en la configuración del BIOS.

  Puede configurar la ejecución del análisis mediante el uso de la característica Wake-on-LAN solo para la tarea *Análisis de malware* en Kaspersky Security Center. No puede habilitar la característica 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 pone el análisis en pausa. En este caso, el Análisis completo puede tardar varios días en completarse.

- Cuando se omitió la tarea.

  Kaspersky Endpoint Security ejecuta la tarea omitida tan pronto como sea posible. La tarea puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas no realizadas, las ejecuta aleatoriamente dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo.

Cómo configurar el programa de análisis con 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 de propiedades de la tarea.

3. En la ventana de propiedades de la tarea, seleccione la pestaña **Programación**.

4. Configure la programación de la tarea de análisis.

5. Según la frecuencia seleccionada, defina configuraciones avanzadas que especifiquen la programación de ejecución de la tarea (vea la tabla de más abajo).

6. Guarde los cambios.

Cómo configurar el programa de análisis en la interfaz de la aplicación

Puede configurar el programa de análisis solo si no se aplica una directiva al equipo. Para los equipos conforme a la directiva, puede configurar la programación de la tarea *Análisis de malware* 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 **Programar análisis**.

4. En la ventana que se abre, configure la programación de la ejecución de la tarea de análisis.

5. Según la frecuencia seleccionada, defina configuraciones avanzadas que especifiquen la programación de ejecución de la tarea (vea la tabla de más abajo).

6. Guarde los cambios.

Configuración de la programación del análisis

Parámetro	Descripción
Programar análisis	**Manualmente**. Modo de ejecución en el que puede iniciar el análisis manualmente en el momento que sea conveniente para usted. **Mediante programación**. En este modo de ejecución de la tarea de análisis, la aplicación inicia la tarea de análisis de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de análisis, también puede iniciar manualmente la tarea de análisis.
Posponer la ejecución después del inicio de la aplicación durante N minutes	Inicio pospuesto de la tarea de análisis después de iniciar la aplicación. Al iniciar el sistema operativo, se ejecutan muchos procesos, por lo que es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después de iniciar Kaspersky Endpoint Security.
Ejecutar tareas omitidas	Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea omitida tan pronto como sea posible. La tarea puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas no realizadas, las ejecuta aleatoriamente dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si la casilla está desactivada, Kaspersky Endpoint Security no ejecuta las tareas omitidas. En lugar de eso, ejecuta la siguiente tarea según la programación actual.
Ejecutar solo cuando el equipo esté inactivo	Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando el equipo está en uso.

Parámetro	Descripción
Esperar un tiempo definido al azar antes de iniciar la tarea *(disponible solo en la Consola de Kaspersky Security Center)*	Si se selecciona la casilla, la tarea no se ejecuta estrictamente según lo programado, sino aleatoriamente dentro de un cierto intervalo, 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 tengan acceso simultáneamente al Servidor de administración cuando la tarea se ejecuta según lo programado. El rango de horas de inicio aleatorias se calcula automáticamente cuando se crea la tarea, según la cantidad de equipos que tienen asignada la tarea. 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 está desactivada, la tarea se ejecuta exactamente a la hora programada.
Limitar el tiempo de espera a esta cantidad de minutos	Si se selecciona esta casilla, la tarea se ejecuta en los equipos en un momento aleatorio dentro de un período determinado. Las horas de inicio aleatorias ayudan a evitar que una gran cantidad de equipos tengan acceso simultáneamente al Servidor de administración cuando la tarea se ejecuta según lo programado. Si la casilla 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)*	Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo 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, 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 si desea ejecutar la tarea en todos los equipos, incluidos los equipos apagados.
Apagar dispositivos cuando se complete la tarea *(disponible solo en la Consola de Kaspersky Security Center)*	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 suspenderá la ejecución de una tarea programada previamente. Una vez transcurrido 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 del equipo durante los períodos de mayor uso.
Deshabilitar el programa de	Si se selecciona la casilla, Kaspersky Endpoint Security dejará de ejecutar la tarea programada a partir de la fecha especificada. La tarea se establecerá en el modo **Manualmente**.

Ejecutar un análisis como un usuario diferente

De forma predeterminada, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. El alcance de la protección puede incluir unidades de red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que posea los derechos requeridos en la configuración de la aplicación y ejecutar la tarea de análisis con la cuenta de este usuario.

Puede ejecutar los siguientes análisis como un usuario diferente:

- Análisis de áreas críticas.
- Análisis completo.
- Análisis personalizado.
- Análisis desde el menú contextual.

No puede configurar los derechos de usuario para ejecutar un Análisis de unidades extraíbles, un Análisis en segundo plano o 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **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. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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 de propiedades de la tarea.
3. Seleccione la ficha **Configuración**.
4. En el bloque **Cuenta**, haga clic en el botón **Configuración**.
5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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, ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar una tarea de análisis.
5. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador prohibió el uso de tareas locales en la directiva.

Optimización de análisis

Limitar el uso de la CPU al analizar el equipo

Puede limitar el uso de la CPU al ejecutar la tarea *Análisis de malware*. Esto puede aumentar el tiempo que toma analizar el equipo.

Cómo limitar el uso de la CPU durante el análisis del 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 correspondiente 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 **Restringir el uso de CPU para las tareas del análisis** e ingrese el valor promedio de consumo de recursos de la CPU en porcentaje.
5. Guarde los cambios.

Cómo limitar el uso de la CPU durante el análisis del equipo en Web Console y Cloud Console

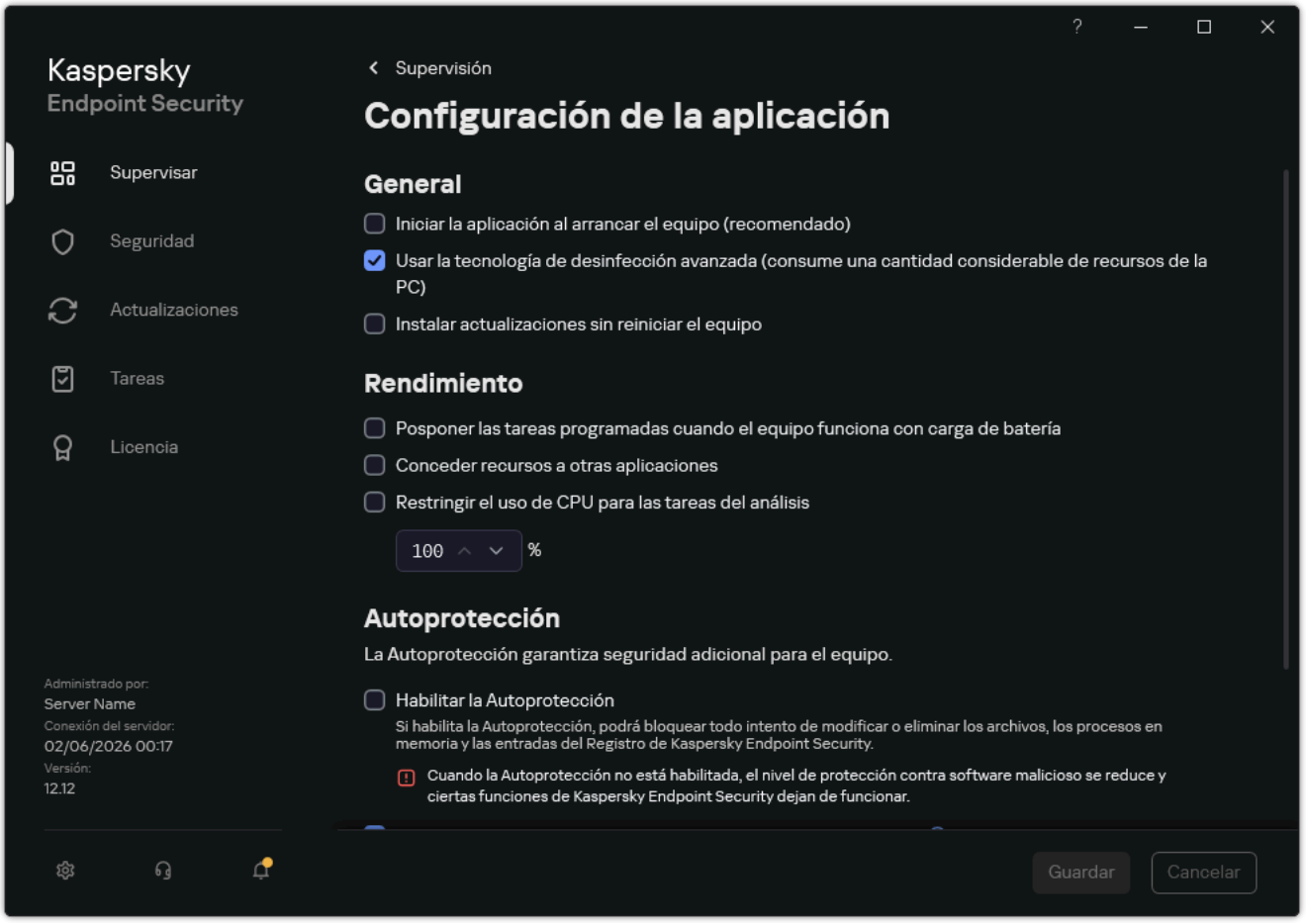
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Rendimiento**.
5. En **Restringir el uso de CPU para las tareas del análisis**, active el interruptor **Restringir el uso de CPU para las tareas del análisis** e ingrese el valor promedio del consumo de recursos de la CPU en porcentaje.
6. Guarde los cambios.

Cómo limitar el uso de la CPU durante el análisis del equipo en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 **Restringir el uso de CPU para las tareas del análisis** e ingrese el valor promedio de consumo de recursos de la CPU en porcentaje.

4. Guarde los cambios.

Establecer la configuración avanzada de Análisis de malware.

Puede optimizar el análisis de archivos: reducir la duración del análisis y aumentar la velocidad operativa de Kaspersky Endpoint Security. Esto se puede lograr analizando solamente los archivos nuevos y aquellos que se han modificado desde el análisis anterior. Este modo se aplica tanto a archivos simples como compuestos. También puede establecer un límite para el análisis de un único archivo. Cuando termina el intervalo de tiempo especificado, Kaspersky Endpoint Security excluye el archivo del análisis actual (excepto los archivos de almacenamiento y objetos que incluyen varios archivos).

Una técnica común para ocultar virus u otro malware es implantarlo en archivos compuestos, como archivos de almacenamiento o bases de datos. Para detectar virus u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

También puede habilitar las tecnologías iChecker y iSwift. Estas tecnologías reducen el tiempo de análisis al asegurarse de que los archivos que no hayan cambiado desde el último análisis no se vuelvan a controlar.

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 *Análisis de malware*.
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**.

   Se abre la ventana de configuración de la tarea de análisis.
6. En el bloque **Optimización**, ajuste la configuración del análisis:

   - **Analizar solo 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 compuestos.

     También puede configurar el análisis de nuevos archivos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo los archivos de almacenamiento nuevos y los archivos de Office.
   - **Omitir archivos que se analicen durante más de N s**. Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.
   - **No ejecutar varias tareas de análisis al mismo tiempo**. Inicio pospuesto de tareas de análisis si ya se está ejecutando un análisis. Kaspersky Endpoint Security pondrá en cola las nuevas tareas de análisis si continúa el análisis actual. Esto permite optimizar la carga en el equipo. Por ejemplo, supongamos que la aplicación inició una tarea Análisis completo según la programación. Si un usuario intenta iniciar un análisis rápido desde la interfaz de la aplicación, Kaspersky Endpoint Security pondrá en cola esta tarea de análisis rápido y la iniciará automáticamente una vez finalizada la tarea de análisis completo.
7. Haga clic en **Adicional**.

   Se abre la ventana de configuración de análisis de archivos compuestos.
8. En el bloque **Límite de tamaño**, seleccione la casilla **No desempaquetar archivos compuestos grandes**. Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.

   > Kaspersky Endpoint Security analiza los archivos de gran tamaño que se extraen de archivos comprimidos, independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.
9. Haga clic en **Aceptar**.
10. Vaya a la pestaña **Adicional**.

11. En el bloque **Tecnologías de análisis**, seleccione las casillas junto a los nombres de las tecnologías que desea utilizar durante un análisis:

    - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

12. Guarde los cambios.

Cómo optimizar un análisis con 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 de propiedades de la tarea. Si es necesario, cree la tarea *Análisis de malware*.

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

4. En el bloque **Acción al detectar una amenaza**, seleccione la casilla **Analizar solo 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 compuestos.

   También puede configurar el análisis de nuevos archivos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo los archivos de almacenamiento nuevos y los archivos de Office.

5. En el bloque **Optimización de análisis**, seleccione la casilla **No desempaquetar archivos compuestos grandes**. Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.

   > Kaspersky Endpoint Security analiza los archivos de gran tamaño que se extraen de archivos comprimidos, independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

6. Seleccione la casilla de verificación **No ejecutar varias tareas de análisis al mismo tiempo**. Inicio pospuesto de tareas de análisis si ya se está ejecutando un análisis. Kaspersky Endpoint Security pondrá en cola las nuevas tareas de análisis si continúa el análisis actual. Esto permite optimizar la carga en el equipo. Por ejemplo, supongamos que la aplicación inició una tarea Análisis completo según la programación. Si un usuario intenta iniciar un análisis rápido desde la interfaz de la aplicación, Kaspersky Endpoint Security pondrá en cola esta tarea de análisis rápido y la iniciará automáticamente una vez finalizada la tarea de análisis completo.

7. En el bloque **Configuración avanzada**, seleccione la casilla **Omitir archivo que se analice durante más de (s)**. Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.

8. Guarde los cambios.

Cómo optimizar el análisis mediante 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**, ajuste la configuración del análisis:

   - **Analizar solo 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 compuestos.

     También puede configurar el análisis de nuevos archivos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo los archivos de almacenamiento nuevos y los archivos de Office.

   - **Omitir archivo que se analice durante más de N segundo(s)**. Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.

   - **No ejecutar varias tareas de análisis al mismo tiempo**. Inicio pospuesto de tareas de análisis si ya se está ejecutando un análisis. Kaspersky Endpoint Security pondrá en cola las nuevas tareas de análisis si continúa el análisis actual. Esto permite optimizar la carga en el equipo. Por ejemplo, supongamos que la aplicación inició una tarea Análisis completo según la programación. Si un usuario intenta iniciar un análisis rápido desde la interfaz de la aplicación, Kaspersky Endpoint Security pondrá en cola esta tarea de análisis rápido y la iniciará automáticamente una vez finalizada la tarea de análisis completo.

5. En el bloque **Límite de tamaño**, seleccione la casilla **No desempaquetar archivos compuestos de gran tamaño**. Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.

   Kaspersky Endpoint Security analiza los archivos de gran tamaño que se extraen de archivos comprimidos, independientemente de si la casilla **No desempaquetar archivos compuestos de gran tamaño** está seleccionada.

6. En el bloque **Tecnologías de análisis**, seleccione las casillas junto a los nombres de las tecnologías que desea utilizar durante un análisis:

   - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

7. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador prohibió el uso de tareas locales en la directiva.

Actualización de bases de datos y módulos de software de la aplicación

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Endpoint Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antivirus y de la base de código) dejar de estar disponible en el software en el territorio de EE. UU.

Las actualizaciones regulares requieren una licencia en vigencia. Si no hay una licencia actual, se podrá realizar una única actualización.

Su equipo debe estar conectado a Internet para descargar correctamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. Por defecto, la configuración de la conexión a Internet se determina automáticamente. Si utiliza un servidor proxy, debe definir su configuración.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTP.

Al realizar una actualización, se descargan e instalan en el equipo los siguientes objetos:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se brinda con bases de datos que contienen firmas de virus y otras amenazas e información sobre maneras de neutralizarlas. Los componentes de protección utilizan esta información al realizar búsquedas de archivos infectados en el equipo y neutralizarlos. Las bases de datos se actualizan constantemente con registros de amenazas nuevas y métodos para contrarrestarlas. Por lo tanto, le recomendamos actualizar las bases de datos con regularidad.

  Además de las bases de datos de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de la aplicación interceptar el tráfico de la red.

- Módulos de la aplicación. Además de las bases de datos de Kaspersky Endpoint Security, también se pueden actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación repara vulnerabilidades en Kaspersky Endpoint Security y agrega funciones nuevas o mejora funciones existentes.

Durante la actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con la versión actualizada en el origen de actualizaciones. Si las bases de datos y los módulos de la aplicación actuales difieren de las respectivas versiones actualizadas, la parte faltante de las actualizaciones se instala en el equipo.

Si las bases de datos están obsoletas, es posible que el tamaño del paquete de actualización sea considerable, lo que puede ocasionar un mayor tráfico web (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 ícono de la aplicación en el área de notificaciones.

La información sobre los resultados de la actualización y sobre todos los eventos que ocurren durante la ejecución de la tarea de actualización se registra en el informe de Kaspersky Endpoint Security.

Si la aplicación funciona en el modo de Light Agent, se aplican consideraciones especiales en la actualización de las bases de datos y los módulos de la aplicación.

Modalidades de actualización para las bases de datos y los módulos

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Endpoint Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

Los objetos que se actualizan en los equipos de los usuarios son los siguientes:

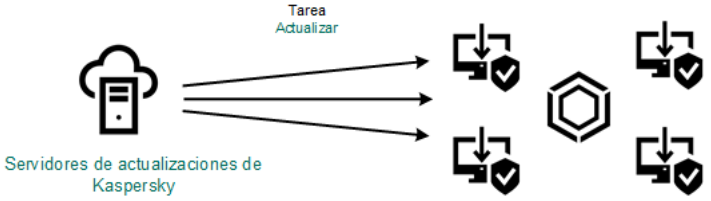
- Bases de datos antivirus. Las bases de datos antivirus contienen bases de datos con firmas de malware, descripciones de ataques de red, bases de datos de direcciones web fraudulentas y malintencionadas, bases de datos de banners, bases de datos de spam y otras clases de información.

- 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 se encuentran 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*.

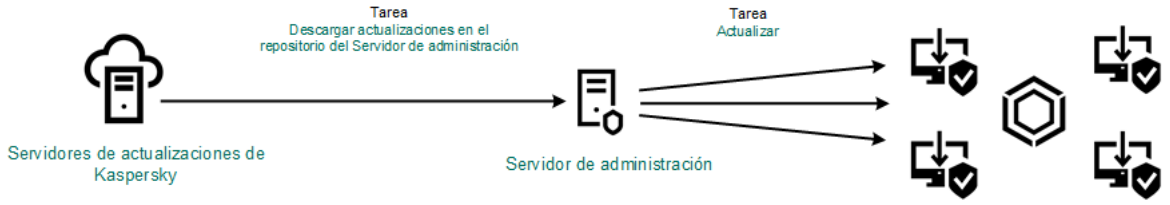
  2. Descargar el paquete de actualización a una carpeta compartida (opcional).

Para descargar el paquete de actualización a una carpeta compartida, puede usar los siguientes métodos:

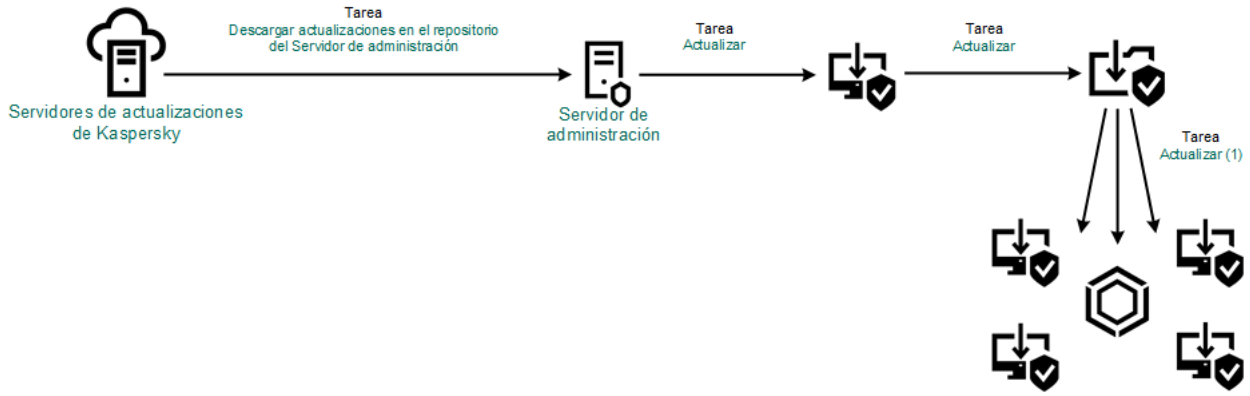
- Utilizar la tarea de *Actualización de bases de datos y módulos de la aplicación* de Kaspersky Endpoint Security. La tarea está diseñada para uno de los equipos en la red de la compañía local.
- Usar la herramienta Kaspersky Update Utility. Para obtener información detallada sobre el uso de Kaspersky Update Utility, consulte la Base de conocimientos de Kaspersky.

3. Distribuir el paquete de actualización a los equipos cliente.

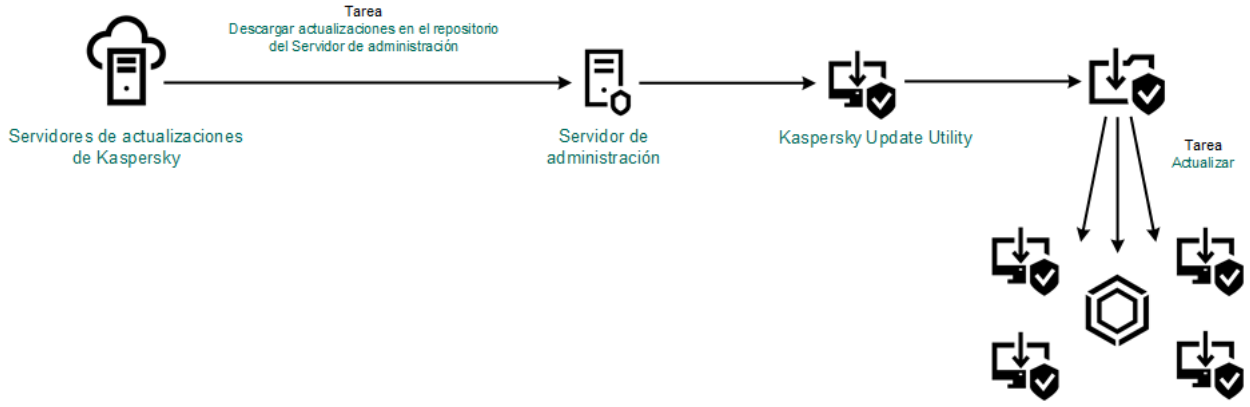
   Para distribuir el paquete a los equipos cliente, utilice la tarea *Actualización de bases de datos y módulos de la aplicación* de Kaspersky Endpoint Security. Podrá crear cuantas tareas de actualización necesite para cada grupo de administración.



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 el Servidor de administración de Kaspersky Security Center y los servidores de actualizaciones de Kaspersky. En Kaspersky Security Center Cloud Console, los orígenes por defecto son los puntos de distribución y los servidores de actualizaciones de Kaspersky. Para obtener más información sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center Cloud Console. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las 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 la configuración de la 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 (la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*).

   La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* se crea automáticamente al usar el asistente de inicio rápido del Servidor de administración. Solo puede existir una instancia de esta tarea. De manera predeterminada, Kaspersky Security Center copia el paquete de actualización en la carpeta `\\<server name>\KLSHARE\Updates`. Si necesita más información sobre la tarea Descargar actualizaciones en el 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 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.

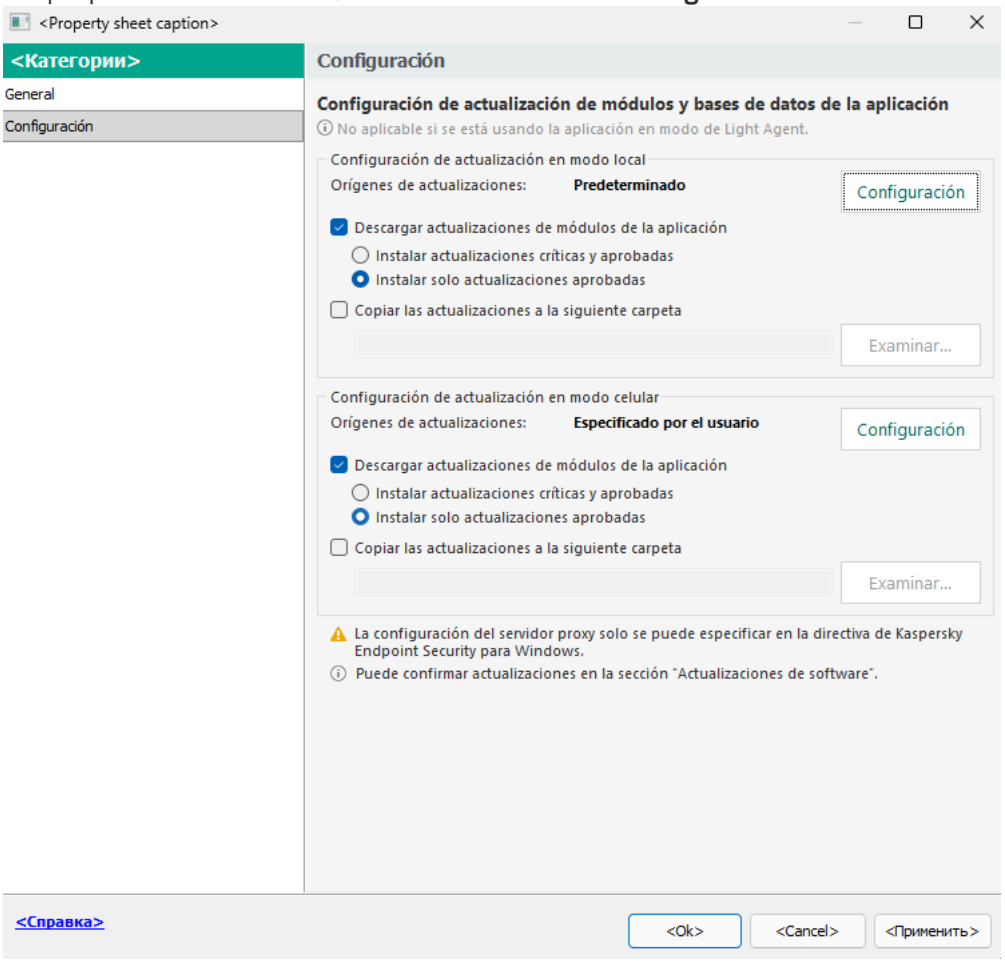
      En el árbol de la consola, seleccione **Tareas**.

   2. Seleccione la tarea **Actualización de bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

      Se abre la ventana de propiedades de la tarea.

      El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de bases de datos y módulos de la aplicación

4. En el bloque **Configuración de actualización en modo local**, haga clic en el botón **Configuración**.

5. En la lista de orígenes de actualizaciones, asegúrese de que la actualización del origen **Kaspersky Security Center** esté habilitada. Además, el origen **Kaspersky Security Center** debe tener la prioridad más alta.

6. Si es necesario, agregue los orígenes de actualizaciones:

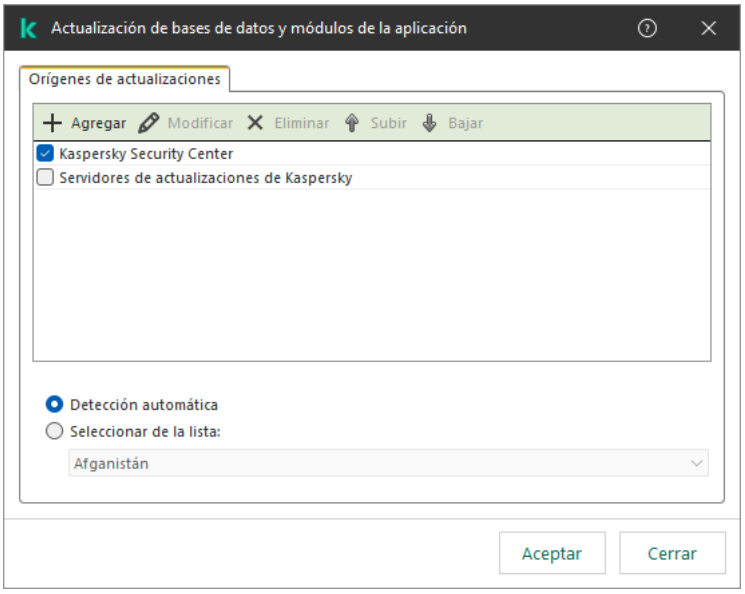
   a. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.

   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 del origen de actualizaciones 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 el origen de actualizaciones sin eliminarlo de la lista de orígenes de actualizaciones. Para hacerlo, desactive la casilla ubicada junto al objeto.



Orígenes de actualizaciones

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 manera 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 de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización*. Para crear la tarea *Actualización*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. Seleccione la ficha **Configuración de la aplicación** → **Modo local**.

4. En la lista de orígenes de actualizaciones, asegúrese de que la actualización del origen **Kaspersky Security Center** esté habilitada. Además, el origen **Kaspersky Security Center** debe tener la prioridad más alta.

5. Si es necesario, agregue los orígenes de actualizaciones:

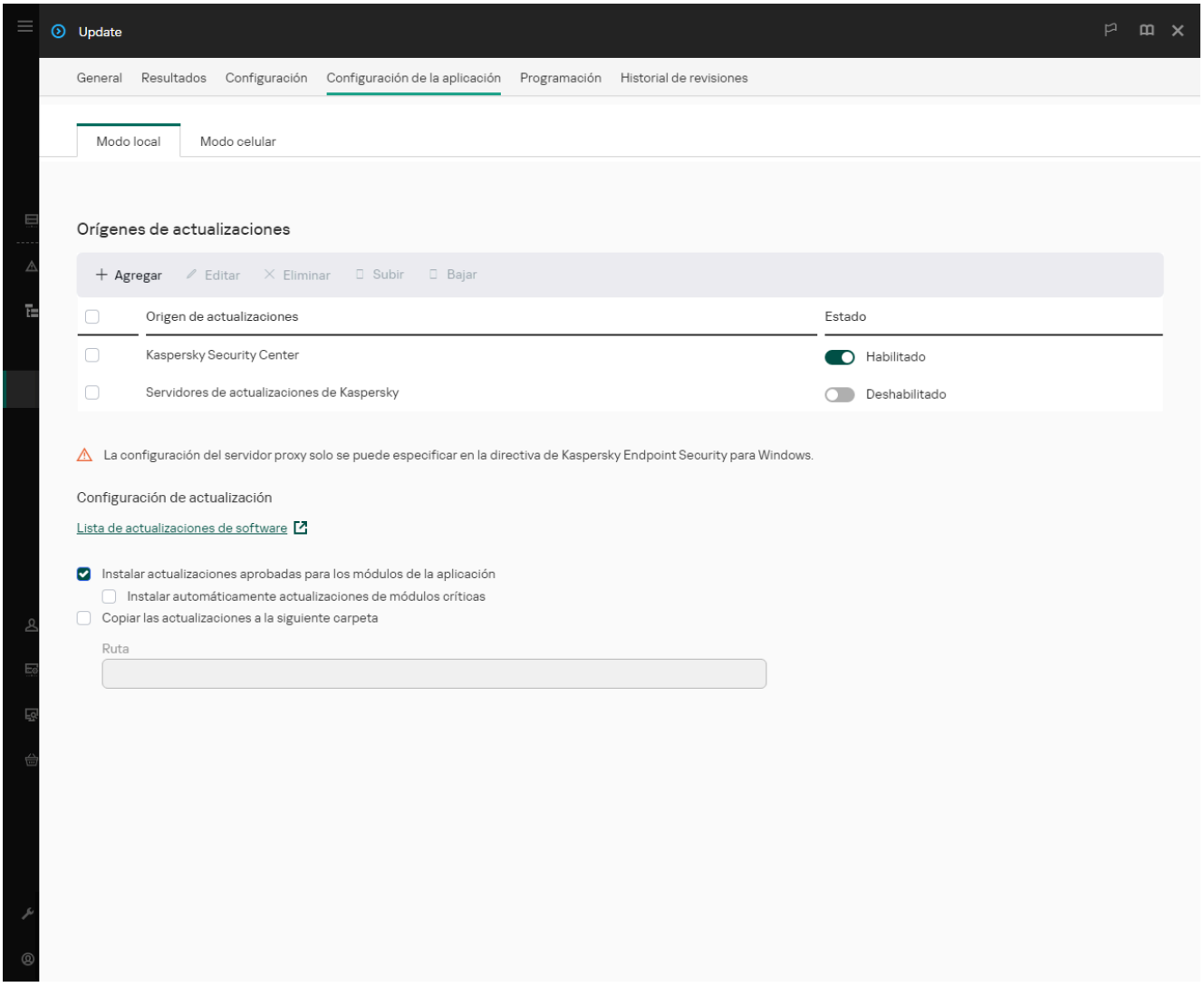
   a. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.

   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 del origen de actualizaciones 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 el origen de actualizaciones sin eliminarlo de la lista de orígenes de actualizaciones. Para hacerlo, habilite el conmutador del interruptor junto a este en la posición de apagado.



Orígenes de actualizaciones

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 manera 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 de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

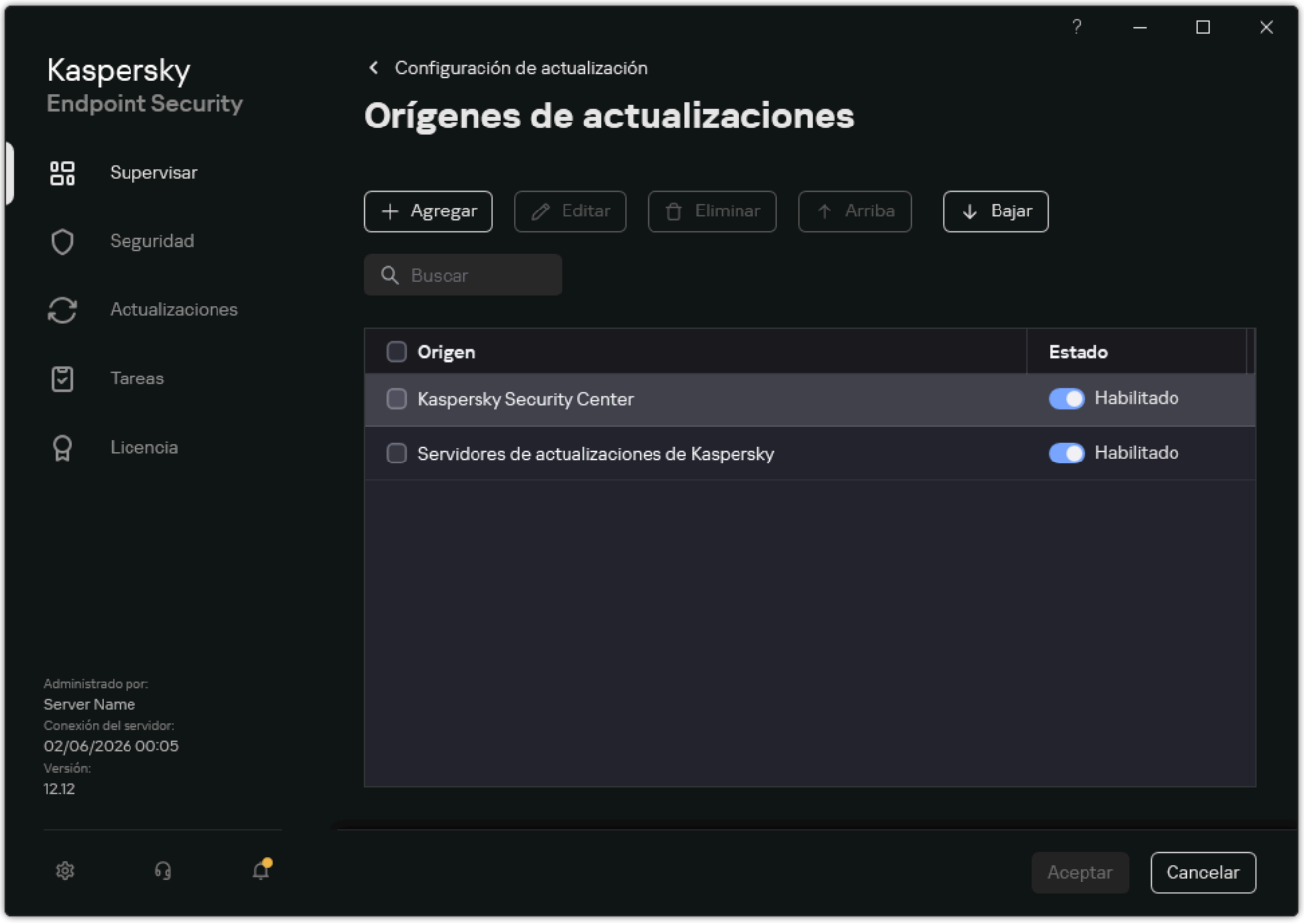
   Se abre la ventana de propiedades de la tarea.

3. En la ventana de propiedades de la tarea, haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la lista de orígenes de actualizaciones, asegúrese de que la actualización del origen **Kaspersky Security Center** esté habilitada. Además, el origen **Kaspersky Security Center** debe tener la prioridad más alta.

5. Si es necesario, agregue los orígenes de actualizaciones:

   a. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.



Orígenes de actualizaciones

   a. Especifique la dirección del servidor FTP/HTTP, la carpeta local o la carpeta de red donde Kaspersky Security Center guardará el paquete de actualización que reciba de los servidores de actualizaciones de Kaspersky.

   > La dirección del origen de actualizaciones 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**.

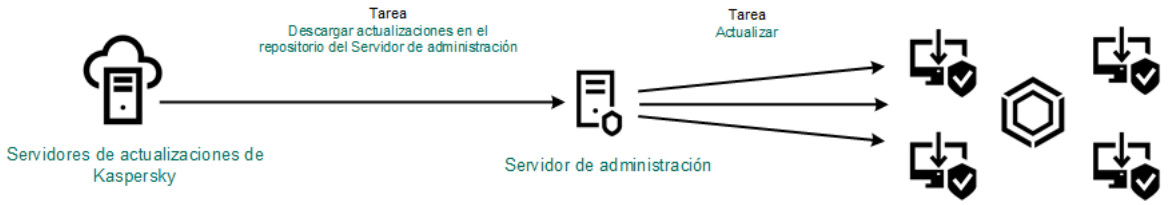
   Puede excluir el origen de actualizaciones sin eliminarlo de la lista de orígenes de actualizaciones. Para hacerlo, habilite el conmutador del interruptor junto a este en la posición de apagado.

6. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Bajar**.

   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 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 la localización de la aplicación Kaspersky Endpoint Security que copia el paquete de actualización a una carpeta compartida debe coincidir con la versión y la localización de la aplicación que actualiza las bases de datos desde la carpeta compartida. Si las versiones o las localizaciones de las aplicaciones no coinciden, la actualización de la base de datos puede mostrar un mensaje de 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. Configurar el uso de un repositorio alojado en un servidor para actualizar las bases de datos y los módulos de la aplicación.

2. Habilitar la opción para que el paquete de actualización se copie a una carpeta compartida en uno de los equipos de la red de área local.

   Cómo habilitar la copia del paquete de actualización a 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**.

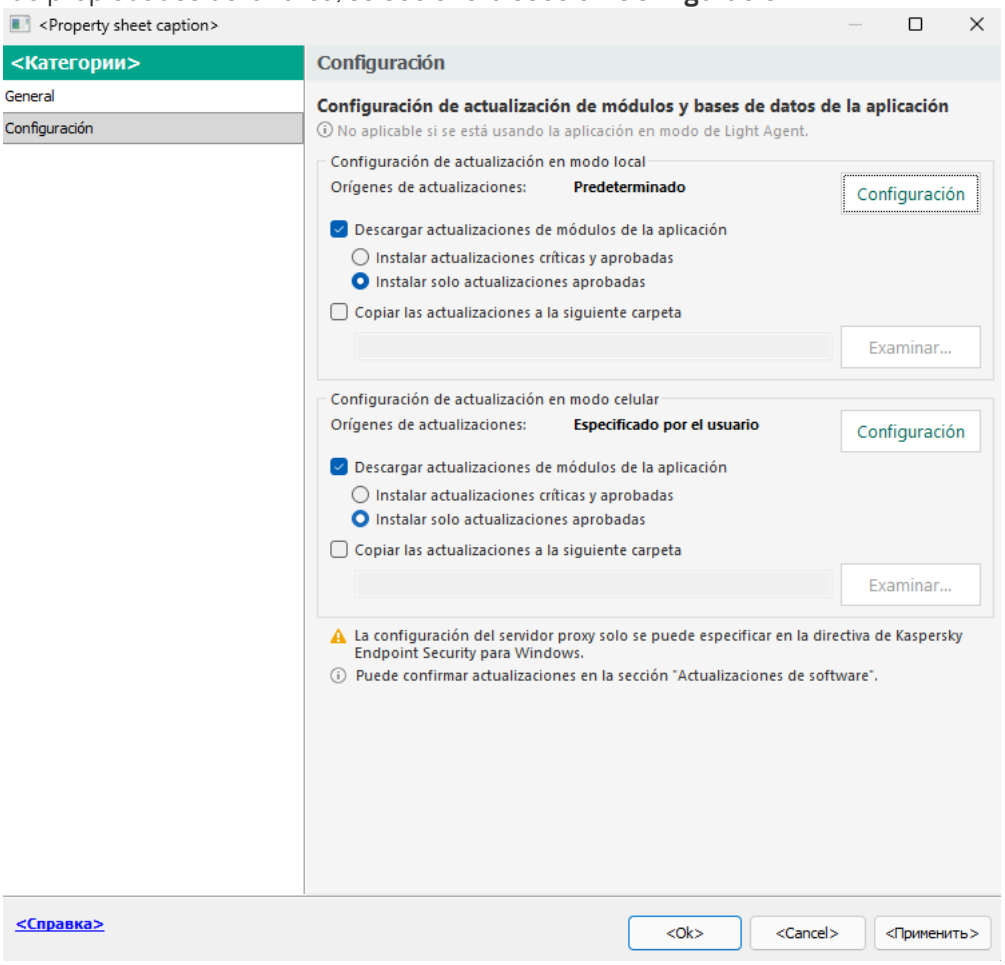
   La tarea *Actualización de bases de datos y módulos de la aplicación* debe asignarse al equipo que actuará como origen de actualizaciones.

   3. Seleccione la tarea **Actualización de bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

      Se abre la ventana de propiedades de la tarea.

El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de bases de datos y módulos de la aplicación

5. En el bloque **Configuración de actualización en 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 de verificación **Copiar las actualizaciones a la siguiente carpeta**.

8. En el campo **Ruta de acceso a carpeta**, escriba la ruta UNC de 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 habilitar 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 de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización*. Para crear la tarea *Actualización*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. Seleccione la ficha **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 de verificación **Copiar las actualizaciones a la siguiente carpeta**.

6. En el campo **Ruta**, escriba la ruta UNC de 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 habilitar la copia del paquete de actualización en la carpeta compartida en la interfaz de la aplicación

> No puede configurar la tarea de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de propiedades de la tarea.

3. En el bloque **Distribuyendo actualizaciones**, seleccione la casilla **Copiar las actualizaciones a la siguiente carpeta**.

4. Escriba la ruta UNC de la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

5. Guarde los cambios.

3. Configurar el proceso de actualización para que los demás equipos conectados a la LAN de la organización obtengan las bases de datos y los módulos más recientes de la carpeta compartida.

Cómo configurar la actualización 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Actualización de 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Actualización de bases de datos y módulos de la aplicación**.

Paso 2. Cómo elegir 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 acceso a carpeta** al configurar la copia del paquete de actualización en 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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

La tarea *Actualización de 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 con la que se ejecutará la tarea

Seleccione la cuenta con la que se ejecutará la tarea *Actualización de bases de datos y módulos de la aplicación*. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

Paso 5. Programación de la tarea

Programe la tarea. Indique si la tarea deberá iniciarse manualmente, si se ejecutará después de que las bases de datos antivirus se descarguen al repositorio o si se usará otro esquema.

Paso 6. Nombre de la tarea

Ingrese el nombre de la tarea, por ejemplo, *Actualizar desde una carpeta compartida*.

Paso 7. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. Como consecuencia, la tarea de actualización se ejecutará en las computadoras de los usuarios de acuerdo con la programación especificada.

Cómo configurar las 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Actualización**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve, por ejemplo, *Actualizar desde una carpeta compartida*.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione 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 alcance de la tarea que haya elegido y vaya al siguiente paso.

5. Salga del Asistente.

   La nueva tarea aparecerá en la tabla de tareas.

6. Haga clic en la tarea *Actualización* que acaba de crear.

   Se abre la ventana de propiedades de la tarea.

7. Seleccione la ficha **Configuración de la aplicación** → **Modo local**.

8. En el bloque **Orígenes de actualizaciones**, haga clic en el botón **Agregar**.

9. En la ventana que se abre, escriba la ruta de acceso a 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 en 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 de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de propiedades de la tarea.

3. Haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la ventana que se abre, haga clic en el botón **Agregar**.

5. En la ventana que se abre, escriba la ruta de acceso a la carpeta compartida.

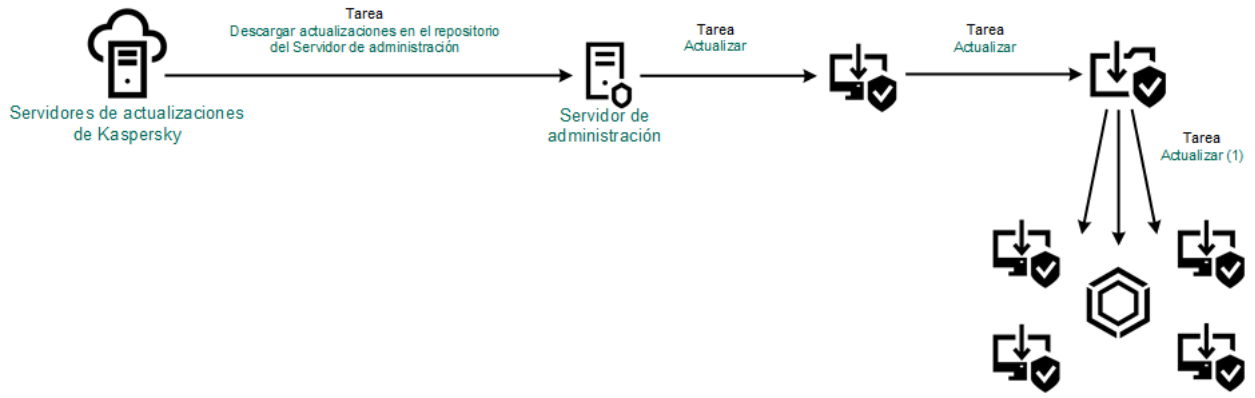
   La dirección del origen debe ser la que haya especificado al configurar la copia del paquete de actualización en la carpeta compartida (consulte las instrucciones de más arriba).

6. Haga clic en **Seleccionar**.

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Bajar**.

   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 la localización de la aplicación Kaspersky Endpoint Security que copia el paquete de actualización a una carpeta compartida debe coincidir con la versión y la localización de la aplicación que actualiza las bases de datos desde la carpeta compartida. Si las versiones o las localizaciones de las aplicaciones no coinciden, la actualización de la base de datos puede mostrar un mensaje de 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. Configurar el uso de un repositorio alojado en un 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 del Servicio 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. Configurar el proceso de actualización para que los demás equipos conectados a la LAN de la organización obtengan las bases de datos y los módulos más recientes de la carpeta compartida.

Cómo configurar la actualización desde la carpeta compartida en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

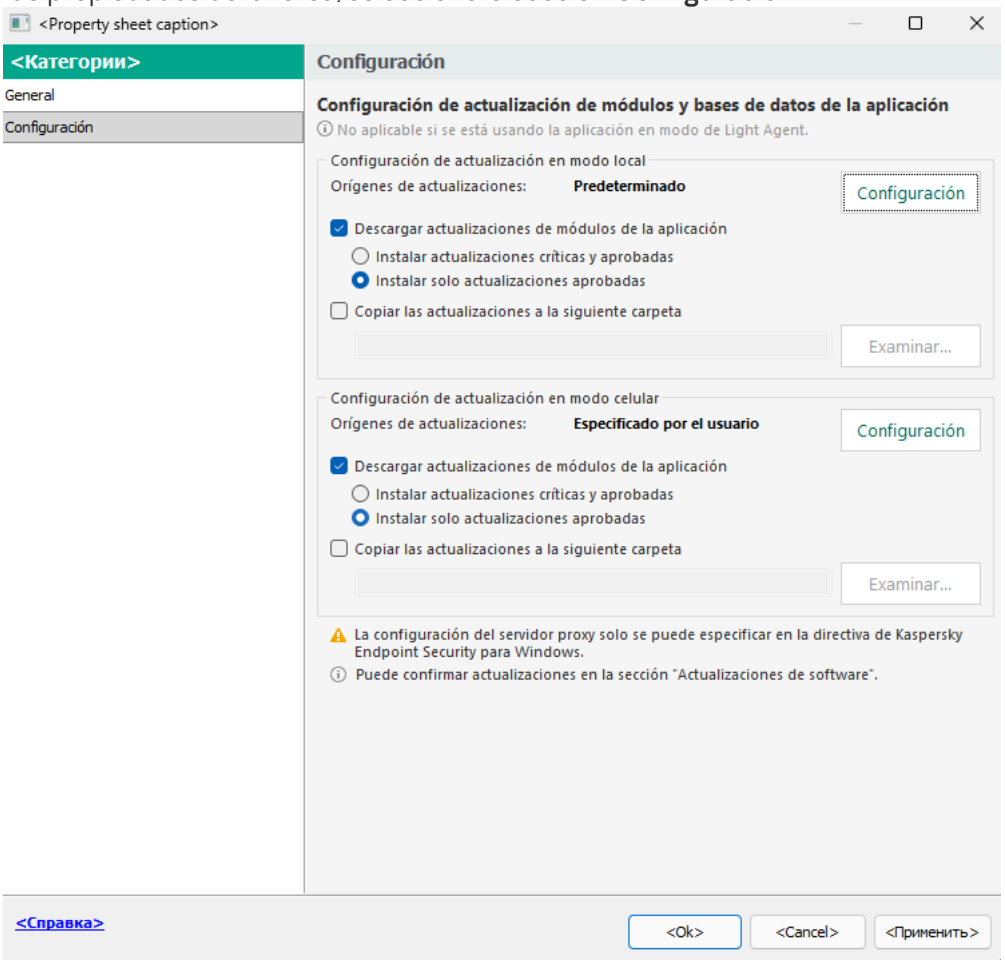
2. En el árbol de la consola, seleccione **Tareas**.

3. Seleccione la tarea **Actualización de bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de bases de datos y módulos de la aplicación

5. En el bloque **Configuración de actualización en modo local**, haga clic en el botón **Configuración**.

6. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.

7. En la ventana que se abre, escriba la ruta UNC de 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 las 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 de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización*. Para crear la tarea *Actualización*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. Seleccione la ficha **Configuración de la aplicación** → **Modo local**.

4. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.

5. En la ventana que se abre, escriba la ruta UNC de 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 de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

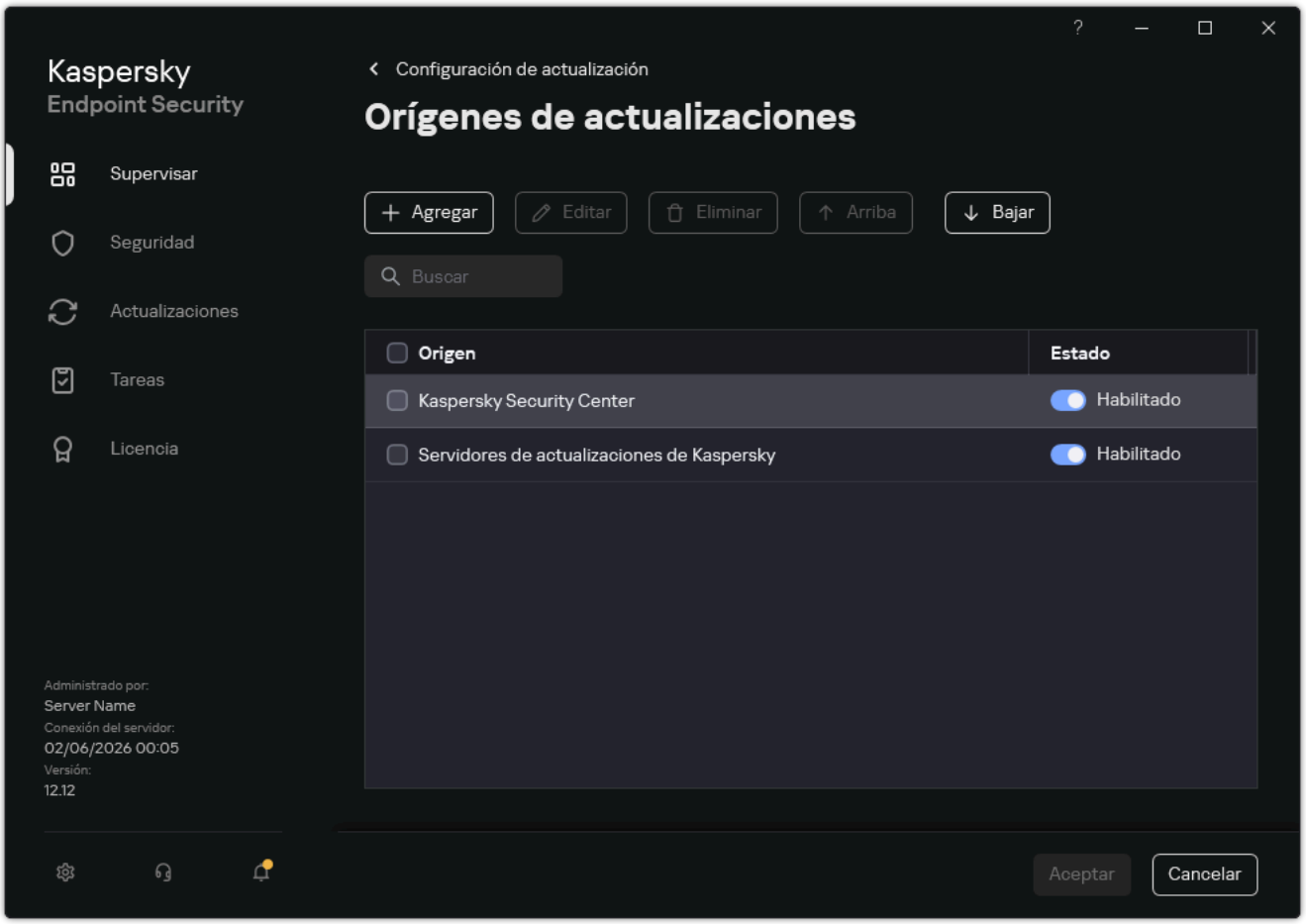
Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de 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 **Agregar**.



Orígenes de actualizaciones

5. Escriba la ruta UNC de la carpeta compartida (por ejemplo, `\\<server name>\KLSHARE\Updates`).

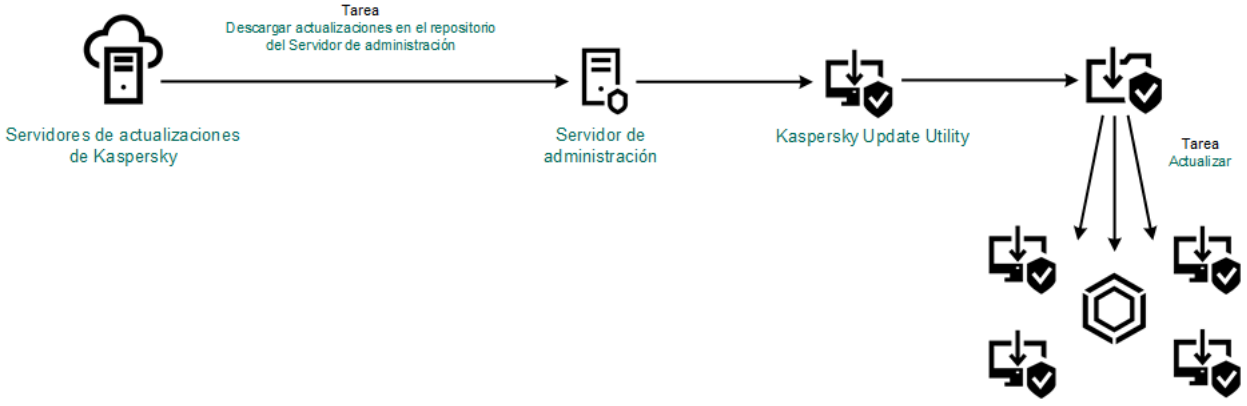
> La dirección del origen debe coincidir con la indicada en la configuración de Kaspersky Update Utility.

6. Haga clic en **Seleccionar**.

7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Bajar**.

   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

El *modo móvil* es el modo de operación de Kaspersky Endpoint Security, cuando un equipo sale del perímetro de la red de organización (*equipo desconectado*). 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, solo los servidores de actualización de Kaspersky se utilizan como fuente de actualización para actualizar bases de datos y módulos de aplicaciones en el modo móvil. 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 establecer la configuración de actualización para el modo móvil en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

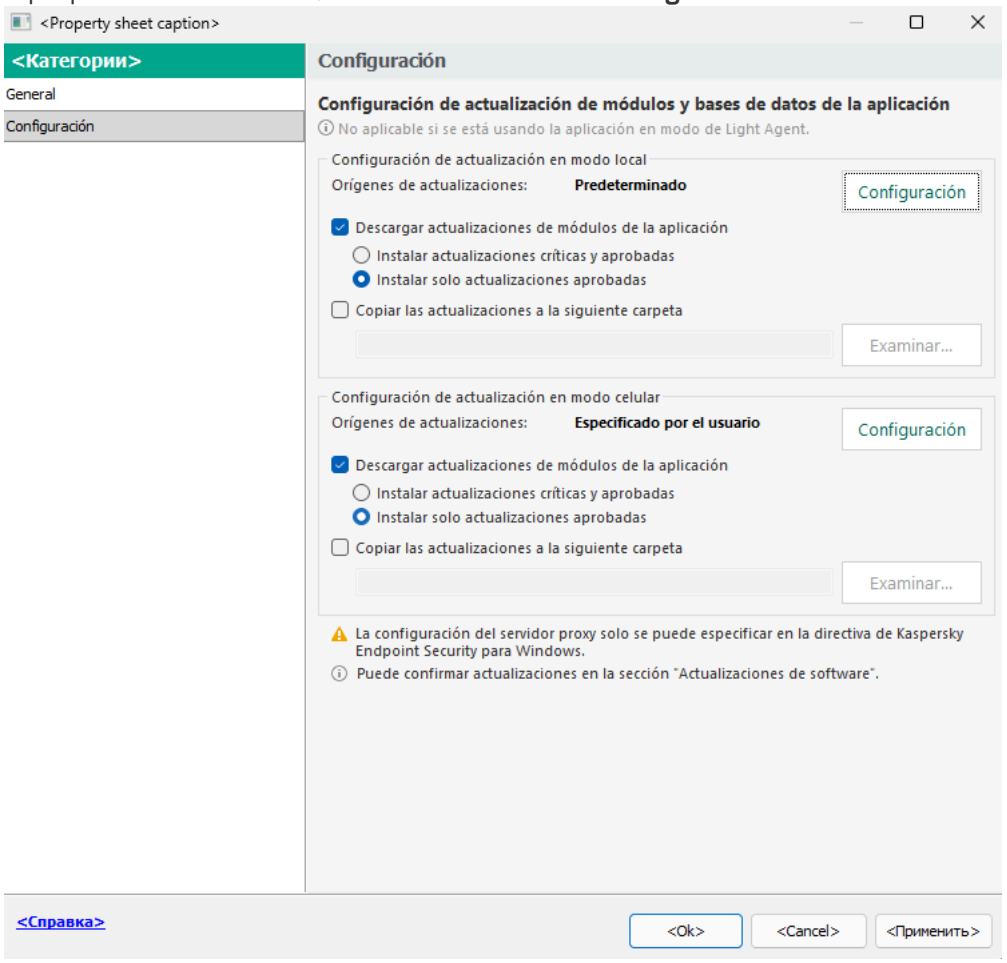
2. En el árbol de la consola, seleccione **Tareas**.

3. Seleccione la tarea **Actualización de bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de bases de datos y módulos de la aplicación

5. En el bloque **Configuración de actualización en modo celular**, 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 establecer la configuración de actualización para el 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 de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización*. Para crear la tarea *Actualización*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. Seleccione la ficha **Configuración de la aplicación** → **Modo celular**.

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.

Una vez que complete estos pasos, los equipos del usuario estarán en condiciones de actualizar las bases de datos y los módulos de la aplicación cuando pasen al modo móvil.

Inicio y detención de una tarea de actualización

Independientemente del modo de ejecución seleccionado para la tarea de actualización, puede iniciar o detener una tarea de actualización de Kaspersky Endpoint Security en cualquier momento.

Para iniciar o detener una tarea de actualización:

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

2. En el ícono **Actualización de 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 las bases de datos y módulos de aplicación. La aplicación mostrará el progreso de la tarea, el tamaño de los archivos descargados y el origen de actualizaciones. Para detener la tarea en cualquier momento, haga clic en el botón **Detener actualización**.

Para iniciar o detener una tarea de actualización cuando se muestra la interfaz simplificada de la aplicación, haga lo siguiente:

1. Haga clic con el botón derecho para mostrar el menú contextual del icono de la aplicación que se encuentra en el área de notificación de la barra de tareas.

2. En la lista desplegable **Tareas** en el menú contextual, realice una de las siguientes opciones:

   - seleccione una tarea de actualización que no se esté ejecutando para iniciarla

   - seleccione una tarea de actualización en ejecución para detenerla

   - seleccione una tarea de actualización suspendida de reanudarla o reiniciarla

Inicio de una tarea de actualización según los derechos de una cuenta de usuario distinta

Por defecto, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta ha usado para iniciar sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security puede actualizarse desde un origen de actualizaciones al cual el usuario que inició sesión no puede acceder debido a la falta de permisos exigidos (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o una fuente de actualización para la cual no se ha configurado la autenticación del servidor proxy. En la configuración de la aplicación, puede especificar un usuario que tenga dichos derechos y comenzar la tarea de actualización de Kaspersky Endpoint Security de la cuenta de este usuario.

Para iniciar una tarea de actualización con una cuenta de usuario distinta:

No puede configurar la tarea de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de propiedades de la tarea.

3. Haga clic en **Ejecutar las actualizaciones de bases de datos con derechos de usuario**.

4. En la ventana que se abre, seleccione **Otro usuario**.

5. Ingrese 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 ejecutar la tarea de actualización por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha ignorado para que se inicie automáticamente tan pronto como sea posible.

Puede posponer la ejecución de la tarea de actualización después del inicio de la aplicación si seleccionó el modo de ejecución de la tarea de actualización **Mediante programación** y si la hora de inicio de Kaspersky Endpoint Security coincide con la planificación del inicio de la tarea de actualización. La tarea de actualización sólo se puede ejecutar una vez transcurrido el intervalo de tiempo especificado después del inicio de Kaspersky Endpoint Security.

Para seleccionar el modo de ejecución de la tarea de actualización:

No puede configurar la tarea de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de 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 desea que Kaspersky Endpoint Security ejecute la tarea de actualización según si existe o no un paquete de actualizaciones disponible en el origen de las actualizaciones, seleccione **Automáticamente**. La frecuencia de las comprobaciones de Kaspersky Endpoint Security para detectar paquetes de actualizaciones aumenta durante las epidemias de virus y disminuye en otros momentos.

   - Si desea iniciar una tarea de actualización manualmente, seleccione **Manualmente**.

   - Si desea configurar una programación para la ejecución de la tarea de actualización, seleccione otras opciones. Defina la configuración avanzada para iniciar la tarea de actualización:

     - En el campo **Posponer la ejecución después del inicio de la aplicación durante N minutos**, ingrese el intervalo de tiempo en el que desea posponer el inicio de la tarea de actualización después del inicio de Kaspersky Endpoint Security.

     - Seleccione **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 no realizadas, las ejecuta aleatoriamente 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.

Como origen de actualizaciones, puede utilizar el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky o una carpeta local o de red dispuesta para tal fin.

> Si los servidores de actualizaciones de Kaspersky no están disponibles, Kaspersky Endpoint Security puede usar dominios alternativos para actualizar sus bases de datos y módulos de software de la aplicación. Para obtener más información, consulte la Base de conocimientos del Servicio de soporte técnico.

La lista por defecto de orígenes de actualizaciones incluye a los servidores de actualización de Kaspersky Security Center y de Kaspersky. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las actualizaciones.

> Kaspersky Endpoint Security no admite actualizaciones que provengan de servidores HTTPS, a menos que sean servidores de actualización de Kaspersky.

Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno tras otro, comenzando por el principio de la lista, y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible.

De manera predeterminada, Kaspersky Endpoint Security usa el servidor de Kaspersky Security Center como el primer origen de actualizaciones. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una directiva a la computadora, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de *Actualización de bases de datos y módulos de la aplicación* de la tarea local, ya que es posible que la aplicación no tenga acceso al servidor de Kaspersky Security Center.

Si la aplicación se ejecuta en el modo de Light Agent, se selecciona una carpeta en la SVM como origen de actualizaciones.

Cómo agregar un origen de actualizaciones en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

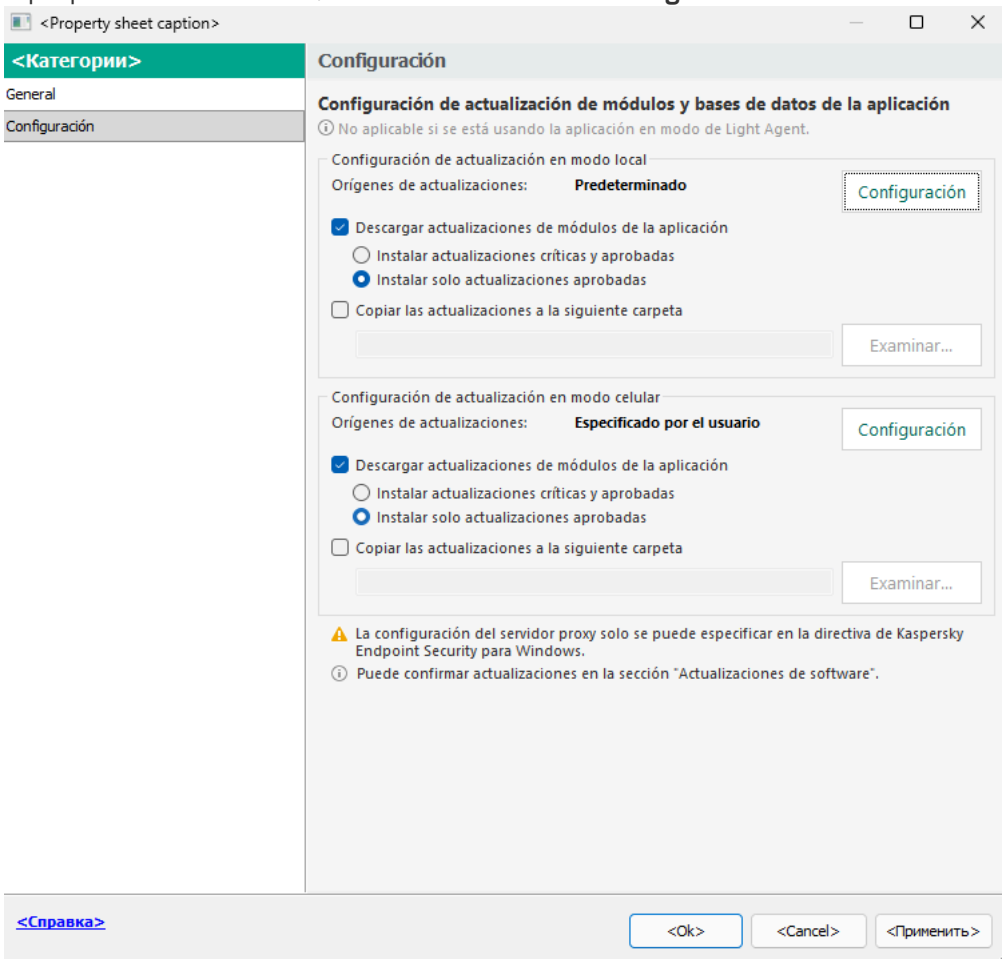
   En el árbol de la consola, seleccione **Tareas**.

2. Seleccione la tarea **Actualización de bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

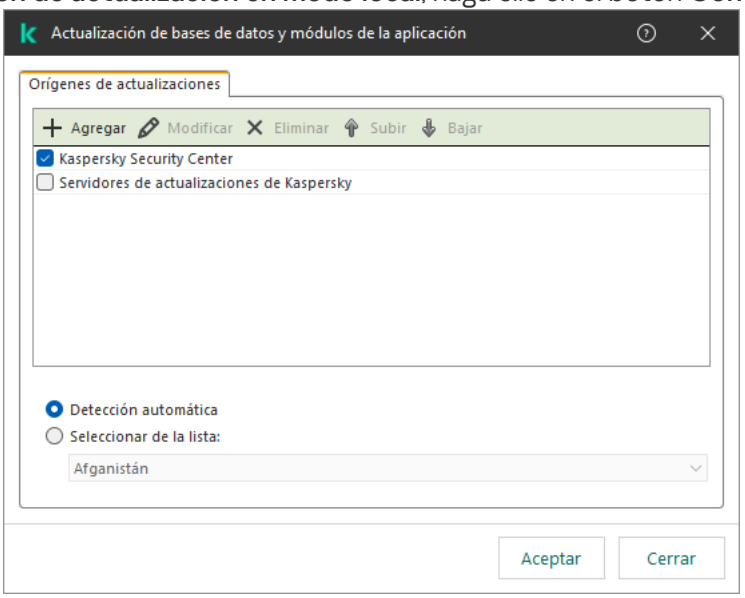
   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de bases de datos y módulos de la aplicación

4. En el bloque **Configuración de actualización en modo local**, haga clic en el botón **Configuración**.



Orígenes de actualizaciones

5. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.

6. En el campo **Orígenes de actualizaciones**, escriba la dirección del servidor FTP o HTTP, de la carpeta de red o de la carpeta local en la que se encuentre el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Si el origen es un servidor FTP o HTTP, escriba la dirección web o la 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>`.

   - Si el origen es una carpeta de red, escriba la ruta UNC.

     Por ejemplo, `\\Server\Share\Update distribution`.

   - Si el origen es una carpeta local o de red, escriba la ruta completa de la carpeta.

     Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Puede excluir el origen de actualizaciones sin eliminarlo de la lista de orígenes de actualizaciones. Para hacerlo, desactive la casilla ubicada 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 es necesario, agregue un origen de actualizaciones para el modo móvil. El *modo móvil* es el modo de operación de Kaspersky Endpoint Security, cuando un equipo sale del perímetro de la red de organización (*equipo desconectado*).

10. Guarde los cambios.

Cómo agregar un origen de actualizaciones en Web Console y Cloud Console

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

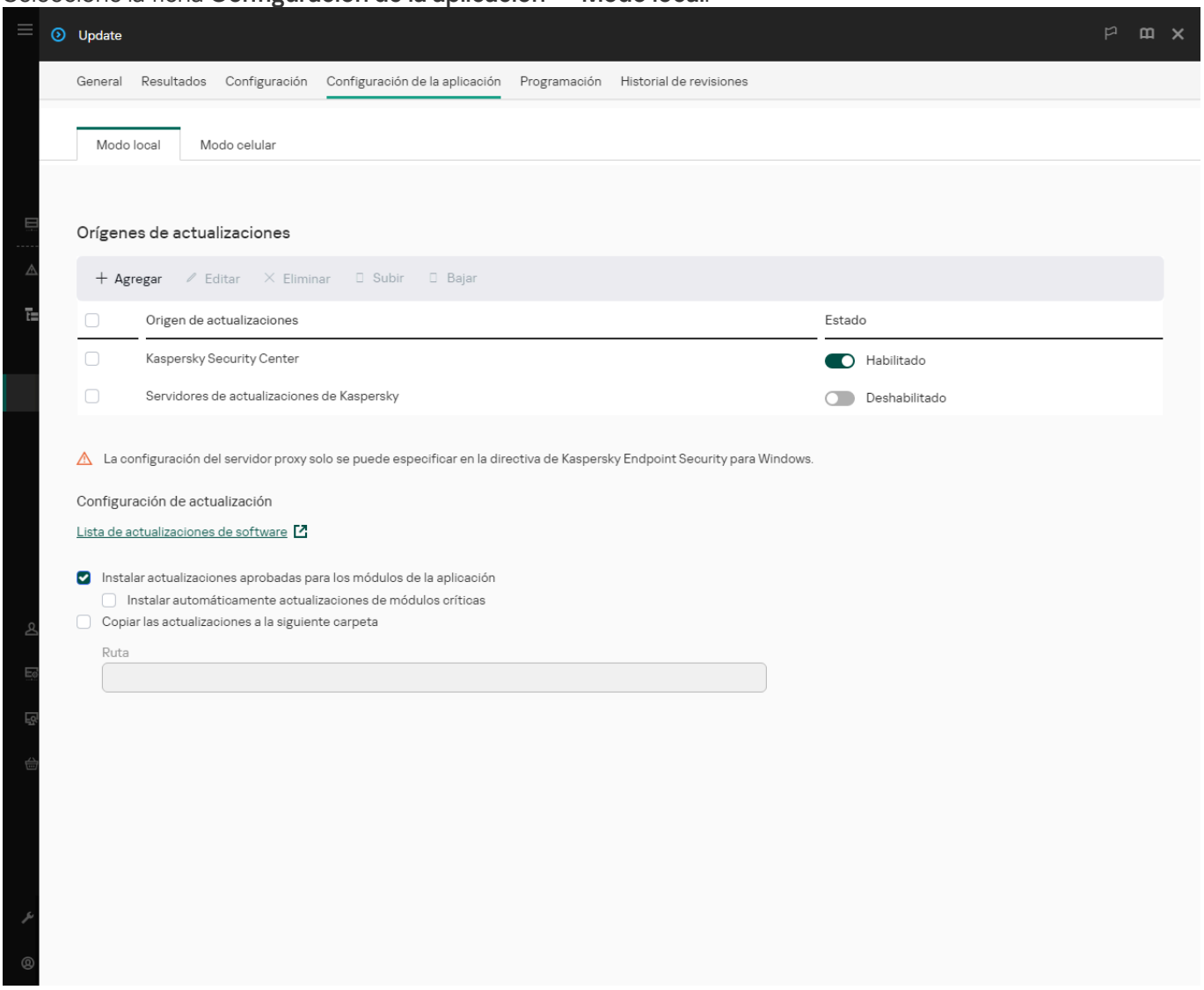
   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización*. Para crear la tarea *Actualización*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. Seleccione la ficha **Configuración de la aplicación** → **Modo local**.



Orígenes de actualizaciones

4. En la lista de orígenes de actualizaciones, haga clic en el botón **Agregar**.

5. En la ventana que se abre, escriba la dirección del servidor FTP o HTTP, de la carpeta de red o de la carpeta local en la que se encuentre el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Si el origen es un servidor FTP o HTTP, escriba la dirección web o la 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>`.

- Si el origen es una carpeta de red, escriba la ruta UNC.

  Por ejemplo, `\\Server\Share\Update distribution`.

- Si el origen es una carpeta local o de red, escriba la ruta completa de la carpeta.

  Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Puede excluir el origen de actualizaciones sin eliminarlo de la lista de orígenes de actualizaciones. Para hacerlo, habilite el conmutador del interruptor junto a este 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 es necesario, agregue un origen de actualizaciones para el modo móvil. El *modo móvil* es el modo de operación de Kaspersky Endpoint Security, cuando un equipo sale del perímetro de la red de organización (*equipo desconectado*).

9. Guarde los cambios.

Cómo agregar un origen de actualizaciones en la interfaz de la aplicación

No puede configurar la tarea de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

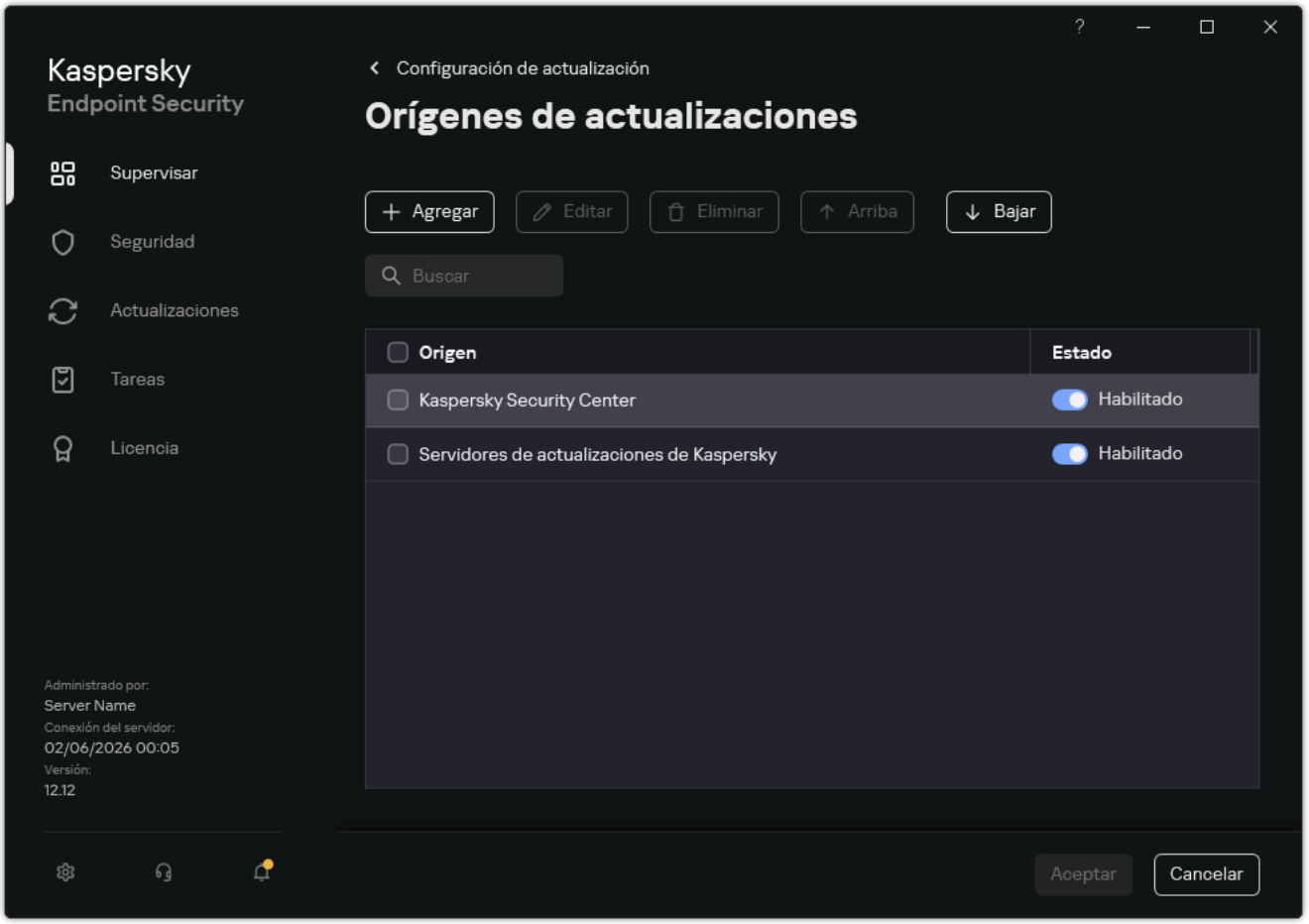
Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de propiedades de la tarea.

3. Haga clic en **Seleccionar orígenes de actualizaciones**.

4. En la ventana que se abre, haga clic en el botón **Agregar**.



Orígenes de actualizaciones

5. En la ventana que se abre, escriba la dirección del servidor FTP o HTTP, de la carpeta de red o de la carpeta local en la que se encuentre el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Si el origen es un servidor FTP o HTTP, escriba la dirección web o la 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>`.

   - Si el origen es una carpeta de red, escriba la ruta UNC.

     Por ejemplo, `\\Server\Share\Update distribution`.

   - Si el origen es una carpeta local o de red, escriba la ruta completa de la 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 **Bajar**.

8. Guarde los cambios.

Actualización de los módulos de la aplicación

Las actualizaciones del módulo de la aplicación corrigen errores, mejoran el rendimiento y agregan nuevas características. 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 para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final.

Después de instalar una actualización de la aplicación, es posible que deba reiniciar el equipo.

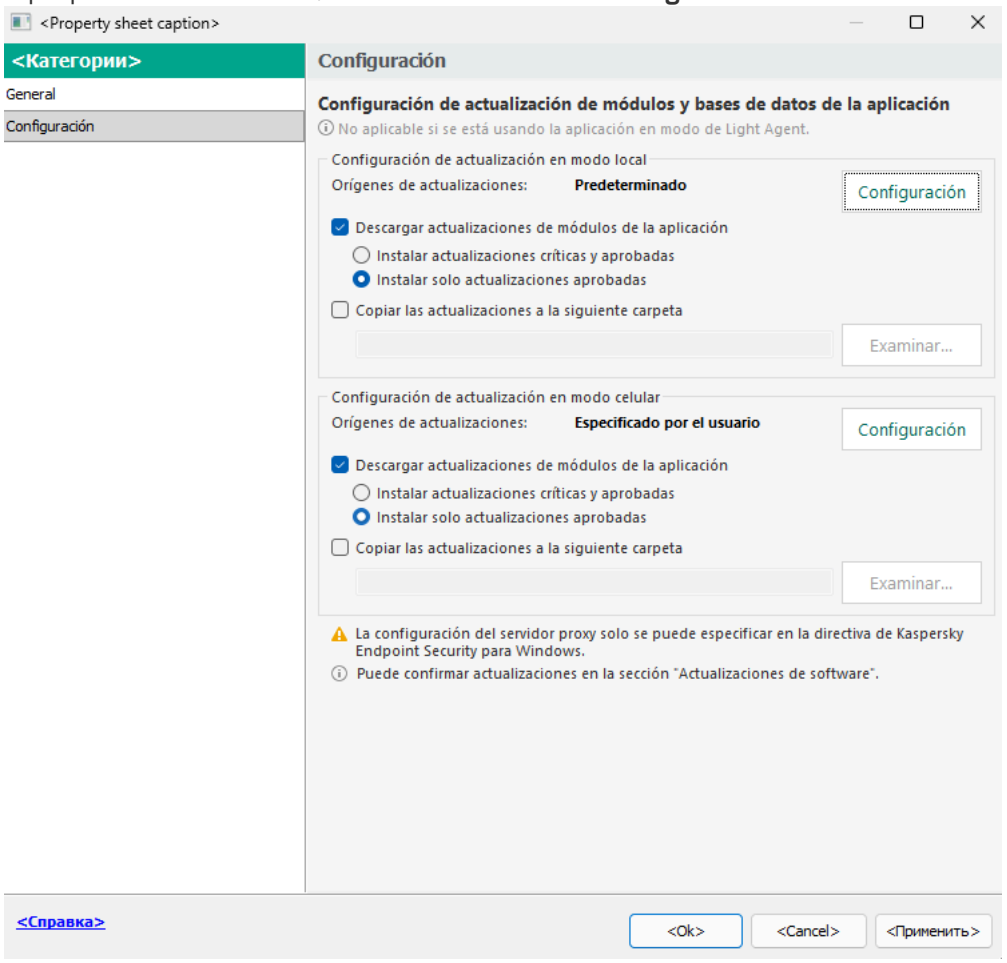
Cómo configurar las actualizaciones del módulo de la aplicación en la Consola de administración (MMC)

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 bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

4. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.



Configuración de la tarea Actualización de bases de datos y módulos de la aplicación

5. En el bloque **Configuración de actualización en modo local**, seleccione la casilla **Descargar actualizaciones de módulos de la aplicación**.

   Si desea evitar que se descarguen las actualizaciones del módulo de la aplicación, desactive la casilla de verificación **Descargar actualizaciones de módulos de la aplicación** y prohíba que el usuario use tareas locales.

6. Seleccione las actualizaciones del módulo de la aplicación que desea instalar.

   - **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.

   - **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.

7. Si es necesario, configure las actualizaciones del módulo de la aplicación para el modo celular. El *modo móvil* es el modo de operación de Kaspersky Endpoint Security, cuando un equipo sale del perímetro de la red de organización (*equipo desconectado*).

8. Guarde los cambios.

Cómo configurar las actualizaciones del módulo de la aplicación en Web Console y Cloud Console

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

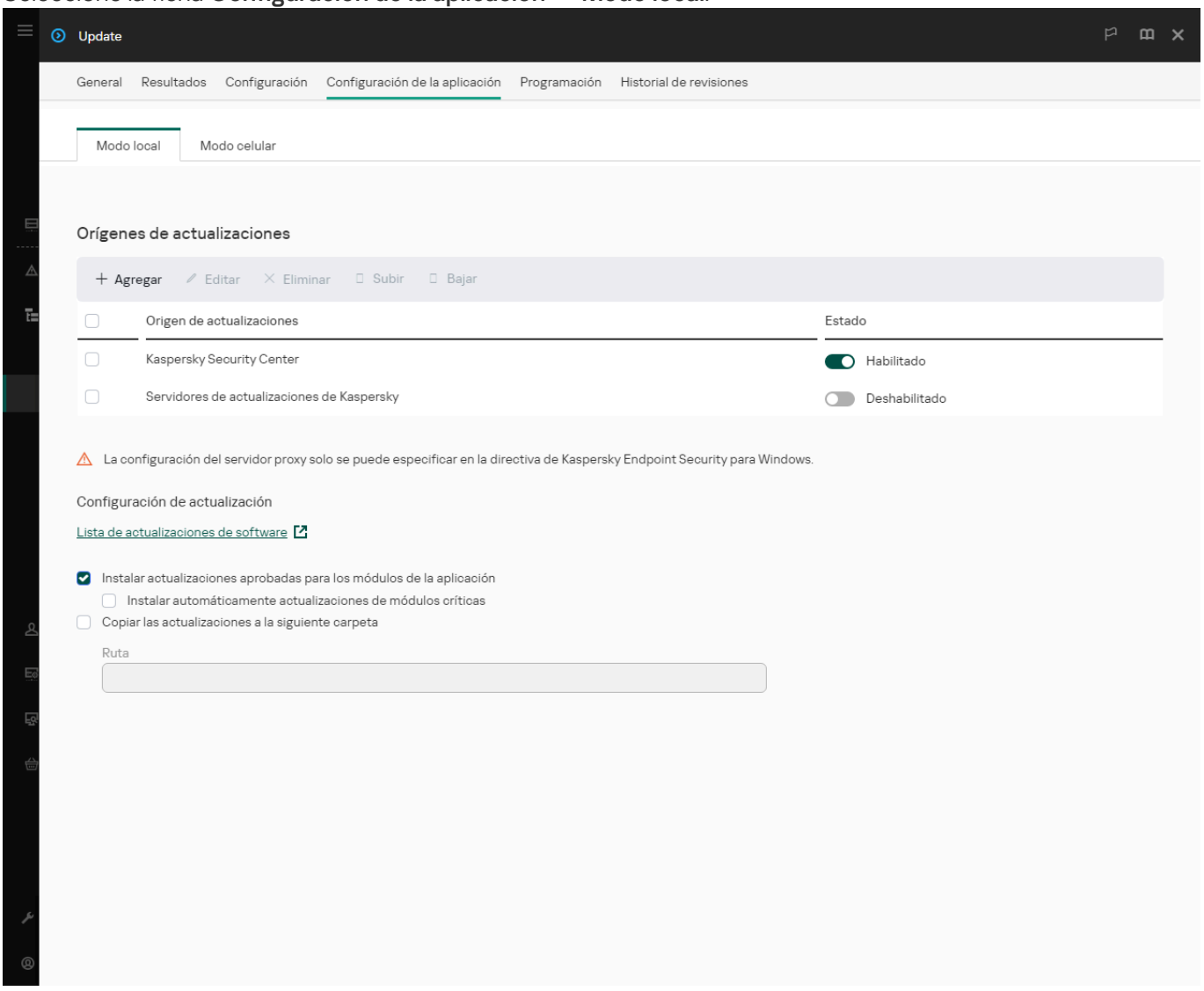
   Se abre la lista de tareas.

2. Seleccione la tarea **Actualización de bases de datos y módulos de la aplicación** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

   El asistente de inicio rápido del Servidor de administración crea automáticamente la tarea *Actualización de bases de datos y módulos de la aplicación*. Para crear la tarea *Actualización de bases de datos y módulos de la aplicación*, instale el Complemento de administración para Kaspersky Endpoint Security para Windows mientras está utilizando el Asistente.

3. Seleccione la ficha **Configuración de la aplicación** → **Modo local**.



Configuración de la tarea Actualización

4. En **Configuración de actualización**, seleccione las actualizaciones del módulo de la aplicación que desee instalar:

   - **Instalar actualizaciones aprobadas para los módulos de la aplicación**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.

   - **Instalar automáticamente actualizaciones de módulos críticas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.

   Si desea evitar que se descarguen las actualizaciones del módulo de la aplicación, desactive las casillas de verificación **Instalar actualizaciones aprobadas para los módulos de la aplicación** y **Instalar automáticamente actualizaciones de módulos críticas**, y prohíba que el usuario use tareas locales.

5. Si es necesario, configure las actualizaciones del módulo de la aplicación para el modo celular. El *modo móvil* es el modo de operación de Kaspersky Endpoint Security, cuando un equipo sale del perímetro de la red de organización (*equipo desconectado*).

6. Guarde los cambios.

Cómo configurar las actualizaciones del módulo de la aplicación en su interfaz

No puede configurar la tarea de grupo *Actualización de bases de datos y módulos de la aplicación* en la interfaz de la aplicación. Solo una tarea de actualización local, *Actualización de bases de datos y módulos de la aplicación*, está disponible para el usuario. Si no se muestra la tarea *Actualización de bases de datos y módulos de la aplicación*, significa que el administrador prohibió el uso de tareas locales en la directiva.

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. Esto abre la lista de tareas; seleccione la tarea *Actualización de bases de datos y módulos de la aplicación* y haga clic en ⚙.

   Se abre la ventana de propiedades de la tarea.

3. En el bloque **Descarga e instalación de actualizaciones para los módulos de la aplicación**, seleccione la casilla **Descargar actualizaciones de módulos de la aplicación**.

4. Seleccione las actualizaciones del módulo de la aplicación que desea instalar.

   - **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.

   - **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de 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 el 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 de acceso a Internet**.

3. Seleccione la casilla de verificación **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 que el servidor proxy no se utilice 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de red**.

5. En el bloque **Servidor proxy**, haga clic en el botón **Configuración**.

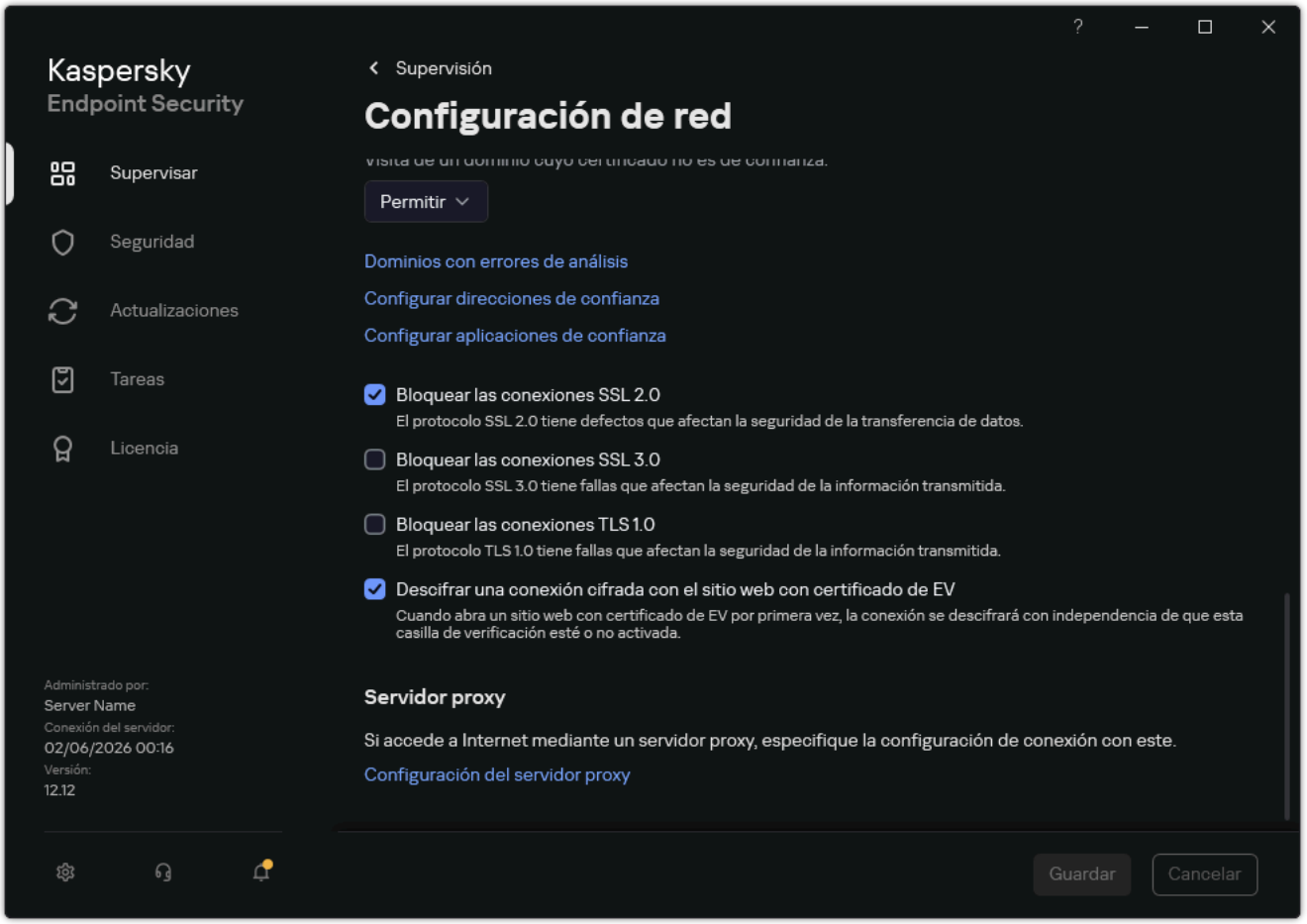
6. En la ventana que se abre, seleccione la casilla **No usar el servidor proxy para las direcciones locales**.

7. Guarde los cambios.

Para definir la configuración del servidor proxy en la interfaz de la aplicación:

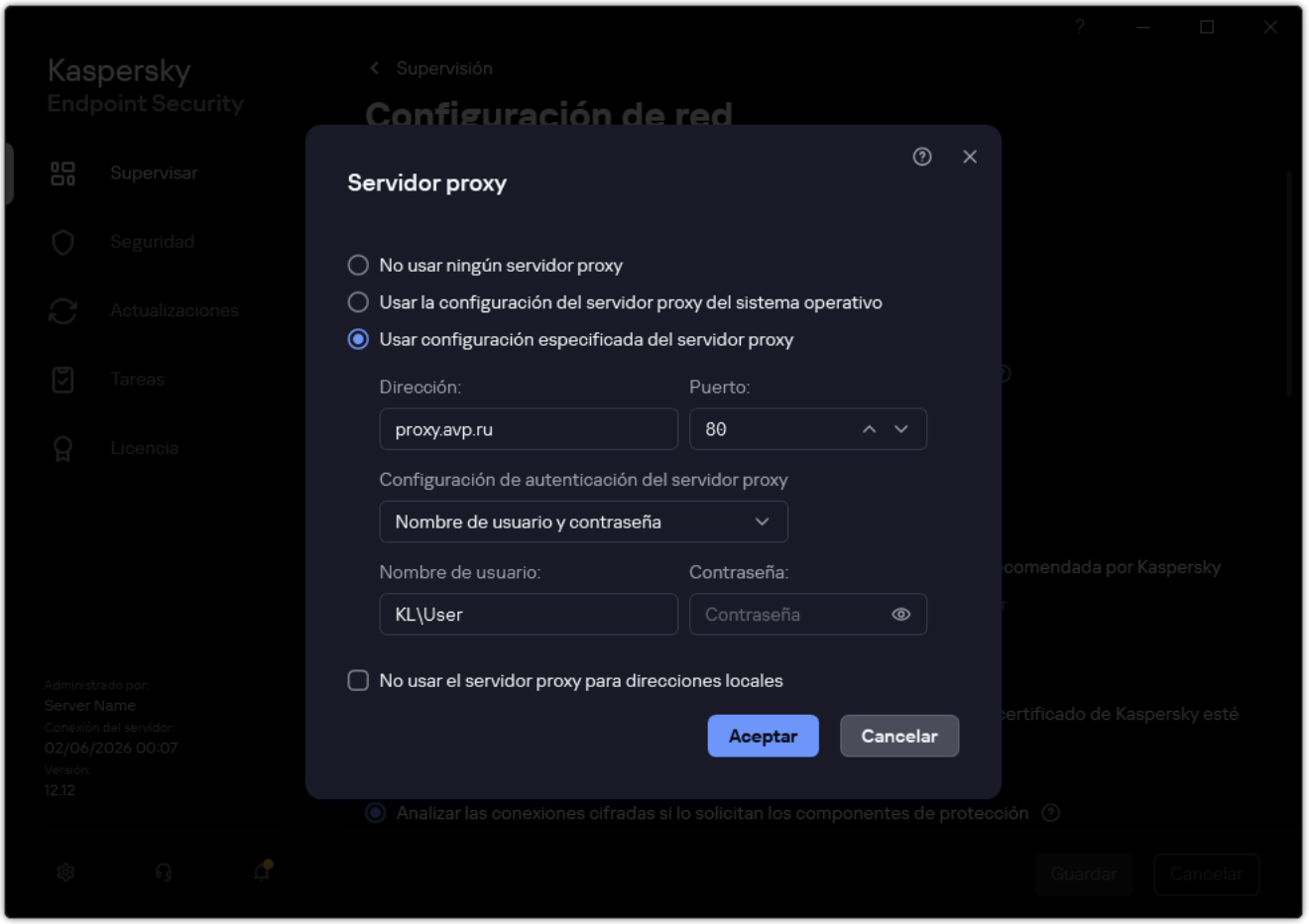
1. En la ventana principal de la aplicación haga clic en el botón ⚙.

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



Parámetros de la configuración de red para aplicaciones

3. En el bloque **Servidor proxy**, haga clic en el vínculo **Configuración del servidor proxy**.



Configuración de la conexión del servidor proxy

4. En la ventana que se abre, seleccione una de las siguientes opciones para determinar la dirección del servidor proxy:

   - **Usar la configuración del servidor proxy del sistema operativo**.

     Esta opción está seleccionada de forma predeterminada. Kaspersky Endpoint Security utiliza la configuración del servidor proxy que está definida en la configuración del sistema operativo.

   - **Usar configuración especificada del servidor proxy**.

     Si seleccionó esta opción, defina 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 manera predeterminada, la aplicación utiliza la autenticación NTLM de dominio del usuario actual.

6. Para que la aplicación no utilice el servidor proxy cuando las bases de datos y los módulos de la aplicación se actualicen desde una carpeta compartida, seleccione la casilla **No usar el servidor proxy para direcciones locales**.

7. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security utilizará el servidor proxy para descargar actualizaciones de los módulos de la aplicación y la base de datos. Kaspersky Endpoint Security también usará el servidor proxy para acceder a servidores de KSN y a 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

Después de que se actualicen por primera vez las bases de datos y los módulos de la aplicación, queda disponible la función para volver las bases de datos y los módulos de la aplicación a sus versiones anteriores.

Cada vez que un usuario comienza el proceso de actualización, Kaspersky Endpoint Security crea una copia de seguridad de las bases de datos y los módulos de la aplicación actuales. Esto le permite volver las bases de datos y los módulos de la aplicación a sus versiones anteriores cuando sea necesario. Revertir la última actualización resulta útil, por ejemplo, si una nueva versión de la base de datos provoca un falso positivo que hace que Kaspersky Endpoint Security bloquee una aplicación segura.

Kaspersky Endpoint Security en modo de Light Agent no es compatible con la tarea *Reversión de la 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

1. Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Reversión de la actualización**.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Programación de la tarea

Configure la programación de la tarea, por ejemplo, manualmente.

Paso 4. Nombre de la tarea

Ingrese un nombre para la tarea.

Paso 7. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Reversión de la actualización**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Reversión de la actualización*).

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del 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 la última actualización en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Actualizaciones**.

Tareas de actualización local

2. En el ícono **Reversión de bases de datos a su versión anterior**, haga clic en el botón **Revertir**.

Kaspersky Endpoint Security comenzará a revertir la última actualización de las bases de datos. La aplicación mostrará el progreso de la reversión, el tamaño de los archivos descargados y el origen de actualizaciones. Para detener la tarea en cualquier momento, haga 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 los ajustes de la tarea *Análisis de malware* y en la configuración de la aplicación.

Si Kaspersky Endpoint Security no puede detener la ejecución de un software malicioso, puede usar la tecnología de desinfección avanzada. Para las computadoras que están sujetas a la directiva, la desinfección avanzada está deshabilitada de manera predeterminada, ya que esta tecnología utiliza una cantidad considerable de recursos del equipo. Para las computadoras que no están sujetas a la directiva, la desinfección avanzada está habilitada de manera predeterminada.

La desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Para utilizar la tecnología en servidores, debe habilitar Desinfección avanzada inmediata en las propiedades de la tarea *Análisis de malware*. Este requisito previo no es necesario para utilizar la tecnología en estaciones de trabajo.

Cómo habilitar o deshabilitar la tecnología de Desinfección avanzada 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 correspondiente 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 anule la selección de la casilla **Habilitar la tecnología de desinfección avanzada** para habilitar o deshabilitar la tecnología de desinfección avanzada.
5. Guarde los cambios.

Cómo habilitar o deshabilitar la tecnología de Desinfección avanzada mediante Web Console y Cloud Console

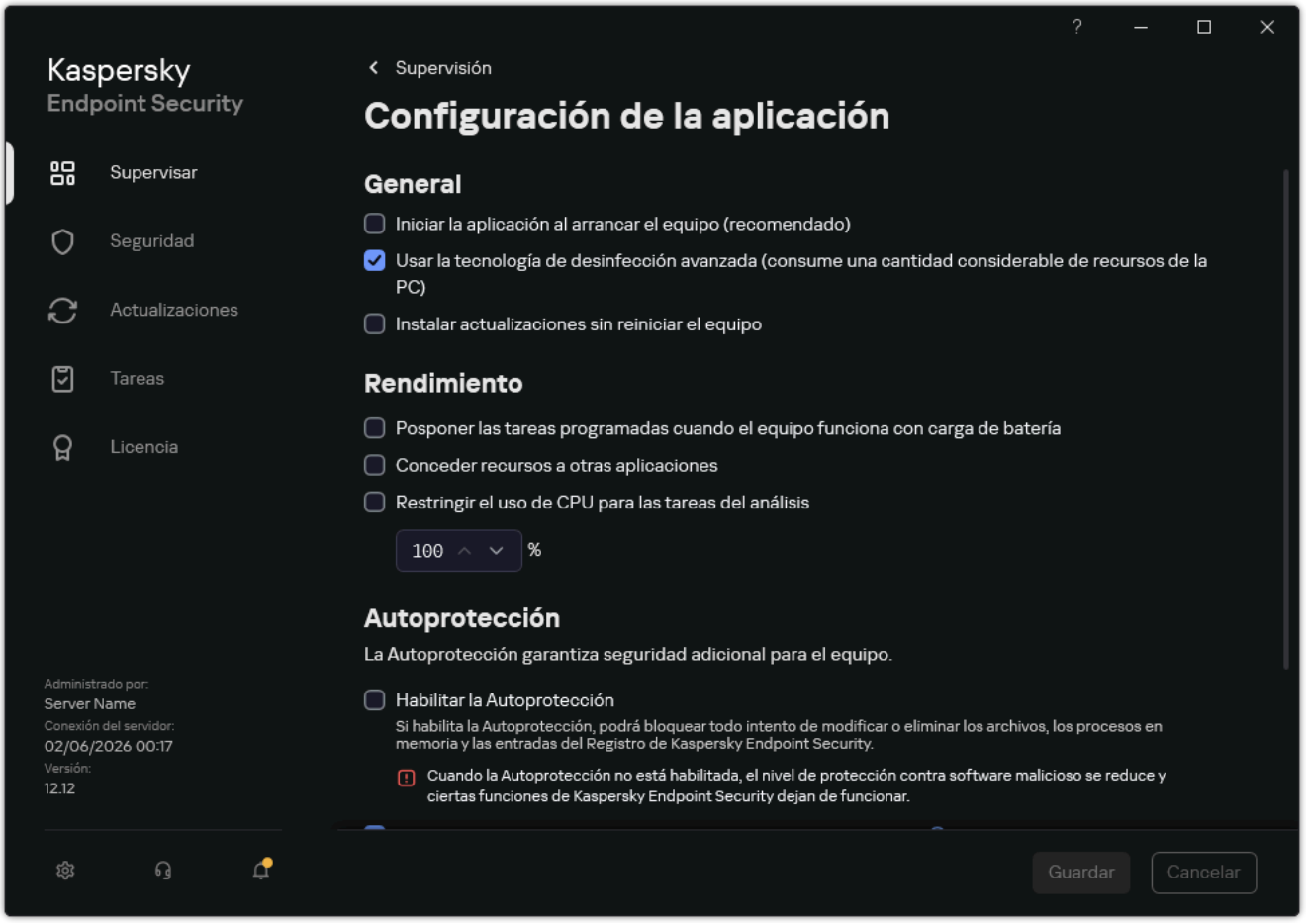
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Configuración general** → **Configuración de detección**.
5. En el bloque **Tecnología de desinfección avanzada**, active el interruptor **Tecnología de desinfección avanzada HABILITADA** para habilitar o deshabilitar la tecnología de Desinfección avanzada.
6. Guarde los cambios.

Cómo habilitar o deshabilitar la tecnología de Desinfección avanzada mediante la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 anule la selección de la casilla **Usar la tecnología de desinfección avanzada (consume una cantidad considerable de recursos de la PC)** para habilitar o deshabilitar la tecnología de desinfección avanzada.

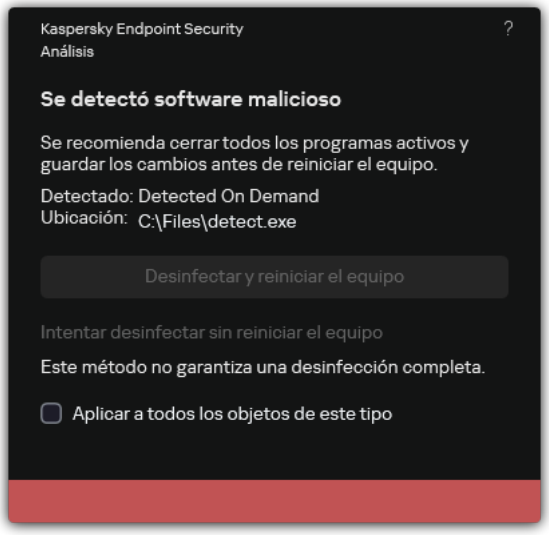
4. Guarde los cambios.

De esta manera, el usuario no podrá usar la mayoría de las características del sistema operativo mientras la desinfección avanzada está en curso. Cuando finalice la desinfección, se reiniciará el equipo.

Desinfección de amenazas activas en estaciones de trabajo

Para trabajar con amenazas activas en estaciones de trabajo, habilite la tecnología de Desinfección avanzada en la configuración de la aplicación. A continuación, configure la experiencia del usuario en las propiedades de la tarea *Análisis de malware*. En las propiedades de la tarea, encontrará la casilla **Ejecutar la desinfección avanzada inmediatamente**. Si la casilla está marcada, Kaspersky Endpoint Security realizará la desinfección sin notificar al usuario. Cuando finalice la desinfección, se reiniciará el equipo. Si la casilla no está marcada, Kaspersky Endpoint Security mostrará una notificación acerca de las amenazas activas (consulte la imagen a continuación). No puede cerrar esta notificación sin procesar el archivo.

La Desinfección avanzada durante una tarea de análisis antivirus en un equipo solo se realiza si la función Desinfección avanzada está habilitada en las propiedades de la directiva que se aplica al equipo.



Notificación sobre amenazas activas

Desinfección de amenazas activas en servidores

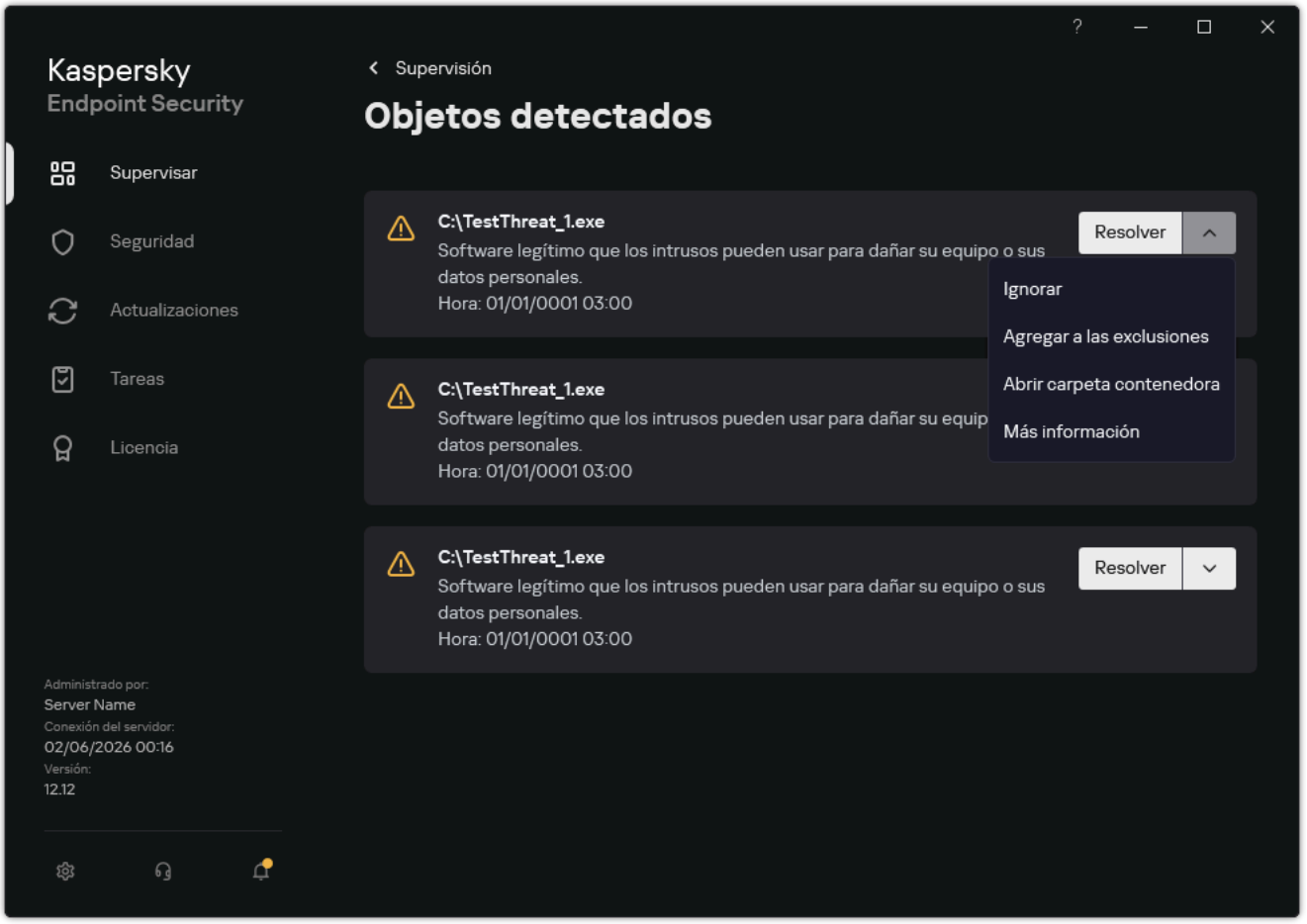
Para trabajar con amenazas activas en servidores, debe hacer lo siguiente:

- habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación;
- habilitar la Desinfección avanzada inmediata en las propiedades de la tarea *Análisis de malware*.

Si Kaspersky Endpoint Security está instalado en un equipo con Windows for Servers, Kaspersky Endpoint Security no mostrará la notificación. Por lo tanto, el usuario no podrá seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación y habilitar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis de malware*. A continuación, debe iniciar la tarea *Análisis de malware*.

Eliminar amenazas no procesadas

Kaspersky Endpoint Security registra información sobre los archivos que no procesó por algún motivo. Esta información se registra en forma de eventos en la lista de amenazas activas (vea la siguiente figura).



Una lista de amenazas activas

Un archivo infectado se considera *procesado* si Kaspersky Endpoint Security desinfectó el archivo o eliminó la amenaza como parte del análisis del equipo en busca de virus u otro malware.

Kaspersky Endpoint Security mueve el archivo a la lista de amenazas activas si, por algún motivo, Kaspersky Endpoint Security no puede realizar una acción en este archivo de conformidad con los ajustes especificados de la aplicación cuando analizar el equipo en busca de virus y otras amenazas.

Esta situación es posible en los siguientes casos:

- El archivo analizado no está disponible (por ejemplo, está ubicado en una unidad de red o en un disco extraíble sin permiso de escritura).
- En la configuración de la tarea de *Análisis de malware*, la acción sobre la detección de amenazas se establece en **Informar**. Luego, cuando la notificación del archivo infectado se mostró en la pantalla, el usuario seleccionó **Omitir**.

Si hay amenazas sin procesar, Kaspersky Endpoint Security cambia el ícono a . En la ventana principal de la aplicación, se muestra la notificación de la amenaza (vea la siguiente imagen). En la consola de Kaspersky Security Center, el estado del equipo cambia a *Crítico* – .

Cómo procesar una amenaza con 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 desee procesar.

3. Decida cómo desea manejar la amenaza:

   - **Desinfectar**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Eliminar**. Si esta opción está seleccionada, la aplicación detecta archivos infectados que se detectan desde el repositorio de amenazas activas. En este caso, la aplicación conserva el archivo detectado en la memoria de la computadora. Para eliminar la amenaza de la computadora, seleccione **Desinfectar**.

Cómo procesar una amenaza con 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 desee procesar.

3. Decida cómo desea manejar la amenaza:

   - **Desinfectar**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Eliminar**. Si esta opción está seleccionada, la aplicación detecta archivos infectados que se detectan desde el repositorio de amenazas activas. En este caso, la aplicación conserva el archivo detectado en la memoria de la computadora. Para eliminar la amenaza de la computadora, seleccione **Desinfectar**.

Cómo procesar una amenaza mediante la interfaz de la aplicación

1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **La protección está en riesgo**.

   Se abre la lista de amenazas activas.

2. Seleccione el objeto que desee procesar.

3. Decida cómo desea manejar la amenaza:

   - **Resolver**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Agregar a las exclusiones**. Si se selecciona esta acción, Kaspersky Endpoint Security sugiere agregar el archivo a la lista de exclusiones del análisis. Los ajustes de la exclusión se configuran automáticamente. Si agregar una exclusión no está disponible, significa que el administrador ha inhabilitado 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 existen amenazas activas restantes en la lista, el estado del equipo cambiará a *Aceptar*. Si se detecta el objeto nuevamente, Kaspersky Endpoint Security agregará una nueva entrada a la lista de amenazas activas.

- **Abrir carpeta contenedora**. Si se selecciona esta opción, Kaspersky Endpoint Security abre la carpeta que contiene el objeto en el Administrador de archivos. Luego, puede eliminar manualmente el objeto o moverlo a una carpeta fuera del alcance de la protección.

- **Más información**. Si esta opción está seleccionada, 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 habilitar la transferencia de información acerca de los archivos no procesados al Servidor de administración. Esta transferencia de datos está habilitada de forma predeterminada.

Cómo habilitar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y repositorios**.

4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.

5. Seleccione la casilla de verificación **Archivos no procesados**.

6. Guarde los cambios.

Cómo habilitar 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.

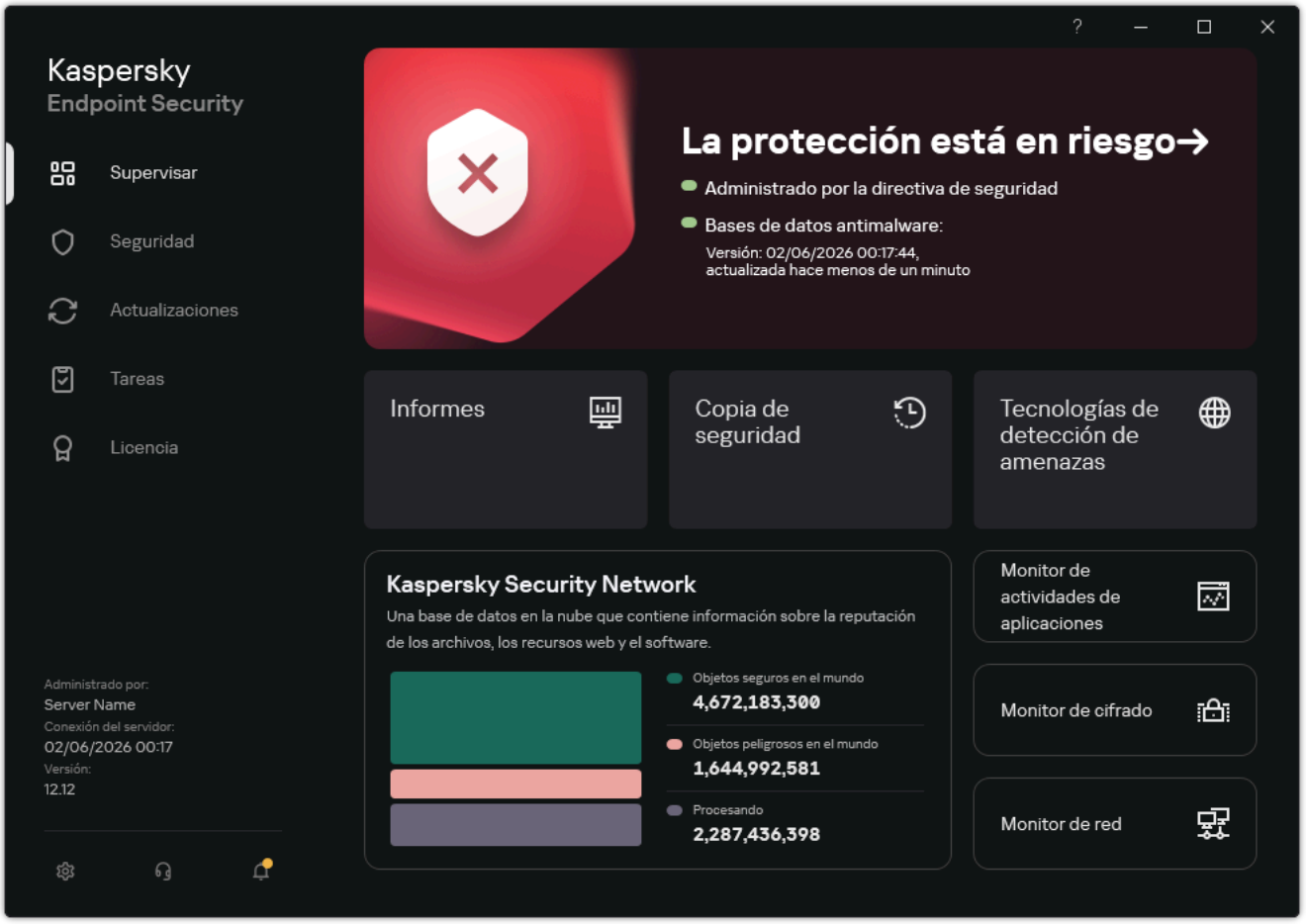
   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **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 **Acerca de los archivos no procesados**.

6. Guarde los cambios.



Ventana principal de la aplicación cuando se detecta una amenaza

Protección del equipo

Protección contra archivos peligrosos

El componente Protección contra archivos peligrosos le permite evitar la infección del sistema de archivos del equipo. De manera predeterminada, el componente Protección contra amenazas de archivo reside permanentemente en la memoria RAM del equipo y analiza en tiempo real todos los archivos abiertos, guardados y ejecutados. El componente analiza archivos en todas las unidades de la computadora, incluidas las unidades conectadas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

El componente analiza los archivos a los que acceden tanto el usuario como las aplicaciones. Cuando se detecta un archivo malintencionado, Kaspersky Endpoint Security bloquea la operación del archivo. El archivo entonces se elimina o se desinfecta, dependiendo de cómo se ha configurado el componente.

Si intenta acceder a un archivo cuyo contenido está almacenado en la nube de OneDrive, Kaspersky Endpoint Security descargará el contenido y lo analizará.

Habilitación y deshabilitación de la Protección contra archivos peligrosos

De manera predeterminada, el componente Protección contra archivos peligrosos está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para Protección contra archivos peligrosos, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que el nivel de seguridad **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky (consulte la tabla a continuación). 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 del nivel de seguridad recomendada.

El componente Protección contra amenazas de archivo usa datos recibidos de otros componentes de la aplicación. La habilitación de estos componentes es opcional. Los siguientes son algunos de los componentes que proporcionan datos adicionales:

- Kaspersky Security Network.
- Prevención de intrusiones en el host.
- Detección de comportamiento.

Cómo habilitar o deshabilitar el componente Protección contra archivos peligrosos 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

4. Utilice la casilla **Protección contra amenazas de archivo** para habilitar o deshabilitar el componente.

5. Si habilitó el componente, realice una de estas 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 contra amenazas de archivos realiza el control más estricto de todos los archivos abiertos, guardados e iniciados. El componente Protección contra amenazas de archivos analiza todos los tipos de archivo en todos los discos duros, unidades extraíbles y unidades de red del equipo. También analiza archivos de almacenamiento, paquetes de instalación y objetos OLE integrados.

     - **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección contra amenazas de archivos solo analiza los formatos de archivo especificados en todos los discos duros, unidades extraíbles y unidades de red del equipo, y en los objetos de OLE incorporados. El componente Protección contra amenazas de archivos no analiza paquetes de instalación ni archivos.

     - **Bajo**. La configuración de este nivel de seguridad de archivos garantiza la máxima velocidad de análisis. El componente Protección contra amenazas de archivos analiza solamente los archivos con las extensiones especificadas en todos los discos duros, unidades extraíbles y unidades de red del equipo. El componente Protección contra amenazas de archivos no analiza archivos compuestos.

   - Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración** y configure los ajustes del componente.

     Para restaurar los valores de los niveles de seguridad preestablecidos, haga clic en el botón **Predeterminado**.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos:

   - **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación bloquea este archivo.

   - **Bloquear**. Si esta opción está seleccionada, la aplicación bloquea automáticamente todos los archivos infectados sin intentar desinfectarlos.

   - **Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.

   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 si se puede desinfectar en el futuro.

7. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Protección contra archivos peligrosos 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Protección contra amenazas de archivo**.

5. Use el interruptor **Protección contra amenazas de archivo HABILITADA** para habilitar o deshabilitar el componente.

6. Si quiere agregar un objeto nuevo al alcance de la protección:

   a. En **Configuración avanzada**, seleccione la pestaña **Alcance de la protección**.

   b. Haga clic en **Agregar**.

   c. En la ventana que se abre, seleccione los objetos que desea agregar al alcance de la protección.

      Usar máscaras:

      - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

      - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras en cualquier parte de la ruta de acceso a una carpeta o un archivo. Por ejemplo, si desea que el alcance del análisis incluya la carpeta Descargas para todas las cuentas de usuario del equipo, escriba la máscara `C:\Users\*\Downloads\`.

      Puede excluir un objeto de la protección sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, habilite el conmutador del interruptor junto a este en la posición de apagado.

   d. Guarde los cambios.

7. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos:

   - **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación bloquea este archivo.

   - **Bloquear**. Si esta opción está seleccionada, la aplicación bloquea automáticamente todos los archivos infectados sin intentar desinfectarlos.

   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 si se puede desinfectar en el futuro.

8. Si es necesario, modifique la configuración avanzada de Protección contra archivos peligrosos.

9. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Protección contra archivos peligrosos en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. Use el interruptor **Protección contra amenazas de archivo** para habilitar o deshabilitar el componente.

4. Si habilitó el componente, realice una de estas 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 contra amenazas de archivos realiza el control más estricto de todos los archivos abiertos, guardados e iniciados. El componente Protección contra amenazas de archivos analiza todos los tipos de archivo en todos los discos duros, unidades extraíbles y unidades de red del equipo. También analiza archivos de almacenamiento, paquetes de instalación y objetos OLE integrados.

     - **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección contra amenazas de archivos solo analiza los formatos de archivo especificados en todos los discos duros, unidades extraíbles y unidades de red del equipo, y en los objetos de OLE incorporados. El componente Protección contra amenazas de archivos no analiza paquetes de instalación ni archivos.

     - **Bajo**. La configuración de este nivel de seguridad de archivos garantiza la máxima velocidad de análisis. El componente Protección contra amenazas de archivos analiza solamente los archivos con las extensiones especificadas en todos los discos duros, unidades extraíbles y unidades de red del equipo. El componente Protección contra amenazas de archivos no analiza archivos compuestos.

- Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina la configuración del componente.

  Para restaurar los valores de los niveles de seguridad preestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado**.

5. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos:

   - **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación bloquea este archivo.

   - **Bloquear**. Si esta opción está seleccionada, la aplicación bloquea automáticamente todos los archivos infectados sin intentar desinfectarlos.

   - **Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.

   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 si se puede desinfectar en el futuro.

6. Guarde los cambios.

Configuración de Protección contra archivos peligrosos recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
Tipos de archivos	**Archivos analizados según su formato**	Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, 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**	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.
Analizar solo archivos nuevos y modificados	**Activo**	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 compuestos.
Usar tecnología iSwift	**Activo**	Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
Usar tecnología iChecker	**Activo**	Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Analizar archivos de Microsoft Office	**Activo**	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.

Parámetro	Valor	Descripción
Analizar archivos de formato de correo electrónico	**Activo**	Analiza archivos de formato de correo electrónico. La aplicación analiza archivos MSG y EML. Los objetos OLE y los archivos MHT también se consideran archivos de formato de correo electrónico. Kaspersky Endpoint Security analiza los archivos en formato correo electrónico con un tamaño inferior a 1 MB independientemente de si la casilla está seleccionada o no.
Modo de análisis	**Modo inteligente**	En este modo, Protección contra archivos peligrosos analiza un objeto en función de las operaciones realizadas sobre ese objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo.
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección**	Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

Suspensión automática de la Protección contra amenazas de archivos

Puede configurar la suspensión automática de la Protección contra archivos peligrosos en una hora especificada o al trabajar con aplicaciones específicas.

La Protección contra archivos peligrosos solo debe pausarse 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 Servicio de soporte técnico de Kaspersky. Los expertos de Soporte lo ayudarán a configurar el componente Protección contra archivos peligrosos para que se ejecute simultáneamente con otras aplicaciones en su equipo.

Para configurar la suspensión automática de la Protección contra archivos peligrosos, realice lo siguiente:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Pausar Protección contra amenazas de archivo**, haga clic en el vínculo **Pausar Protección contra amenazas de archivo**.
5. En la ventana que se abre, defina la configuración para suspender la Protección contra archivos peligrosos:
   a. Configure una programación para pausar automáticamente Protección contra archivos peligrosos.
   b. Cree una lista de aplicaciones cuyo funcionamiento debería provocar que Protección contra archivos peligrosos detenga sus actividades.
6. Guarde los cambios.

Cambio de la acción tomada respecto de archivos infectados por el componente Protección contra amenazas de archivos

Por defecto, el componente Protección contra archivos peligrosos automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección arroja un error, el componente Protección contra archivos peligrosos elimina estos archivos.

Para cambiar la acción tomada respecto de archivos infectados por el componente Protección contra archivos peligrosos, realice lo siguiente:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. En el bloque **Acción al detectar una amenaza**, seleccione la opción relevante:

   - **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo.

   - **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación bloquea este archivo.

   - **Bloquear**. Si esta opción está seleccionada, la aplicación bloquea automáticamente todos los archivos infectados sin intentar desinfectarlos.

   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 si se puede desinfectar en el futuro.

4. Guarde los cambios.

Formación del alcance de la protección del componente Protección contra archivos peligrosos

El alcance de la protección se refiere a los objetos que el componente analiza cuando está habilitado. Los alcances de la protección de diferentes componentes tienen diferentes propiedades. La ubicación y el tipo de archivos que se analizarán son propiedades del alcance de la protección del componente Protección contra archivos peligrosos. De forma predeterminada, el componente Protección contra archivos peligrosos analiza solo los archivos potencialmente infectables que se ejecutan desde discos duros, unidades extraíbles y unidades de red.

Cuando seleccione el tipo de archivos por analizar, tenga presenta la siguiente información:

1. La probabilidad de que ciertos tipos de archivos (por ejemplo, los de formato TXT) contengan código malintencionado que pueda activarse es baja. Existen, por otro lado, formatos de archivo que sí contienen código ejecutable (.exe, .dll y otros). Junto con estos, existen ciertos tipos de archivos que pueden contener código ejecutable aunque no estén principalmente diseñados para ello (por ejemplo, los archivos de formato DOC). El riesgo de que el código malicioso ingrese en estos archivos y se active es alto.

2. Un intruso podría enviarle un archivo de extensión .txt que sea, en realidad, un ejecutable peligroso (un virus u otro tipo de aplicación malintencionada) al que se le ha cambiado el nombre. Si selecciona el análisis de archivos por extensión, la aplicación omite este archivo durante el análisis. Si se selecciona el análisis de archivos por formato, Kaspersky Endpoint Security analiza el encabezado del archivo independientemente de la extensión. Si se determina que el archivo es de un formato ejecutable (por ejemplo, EXE), se lo somete a análisis.

Para crear el alcance de la protección:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Tipos de archivos**, especifique el tipo de archivo que utilizará para analizar el componente Protección contra archivos peligrosos:

   - **Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones).

   - **Archivos analizados según su formato**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, 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 según su extensión**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión.

5. Haga clic en el vínculo **Editar el alcance de la protección**.

6. En la ventana que se abre, seleccione los objetos que desea agregar al alcance de la protección o excluir de este.

   No puede quitar ni modificar objetos que estén incluidos en el alcance de la protección predeterminado.

7. Si quiere agregar un objeto nuevo al alcance de la protección:

   a. Haga clic en **Agregar**.

      Se abre el árbol de carpetas.

   b. En el campo **Ruta**, escriba la ruta del archivo o la carpeta.

Usar máscaras:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras en cualquier parte de la ruta de acceso a una carpeta o un archivo. Por ejemplo, si desea que el alcance del análisis incluya la carpeta Descargas para todas las cuentas de usuario del equipo, escriba la máscara `C:\Users\*\Downloads\`.

El objeto **Este equipo** en la lista de recursos de la computadora 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 el alcance del análisis. Para hacerlo, desactive la casilla ubicada 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 compara 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 está siempre habilitado.

Para aumentar la efectividad de la protección, puede utilizar el análisis heurístico. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

Para configurar el uso del análisis heurístico en el funcionamiento del componente Protección contra archivos peligrosos, realice lo siguiente:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. Haga clic en **Configuración avanzada**.

4. Si desea que la aplicación utilice el análisis heurístico para la protección contra archivos peligrosos, seleccione la casilla **Análisis heurístico** en el bloque **Métodos de análisis**. Luego, use el control deslizante para elegir un nivel de análisis: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.

5. Guarde los cambios.

Utilización de tecnologías de análisis en la operación del componente Protección contra amenazas de archivos

Para configurar el uso de tecnologías de análisis en el funcionamiento del componente Protección contra archivos peligrosos:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Tecnologías de análisis**, seleccione las casillas junto a los nombres de las tecnologías que desea utilizar para la protección contra archivos peligrosos:

   - **Usar tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

5. Guarde los cambios.

Optimización del análisis de archivos

Puede optimizar el análisis de archivos realizado por el componente Protección contra archivos peligrosos reduciendo la duración del análisis y aumentando la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede lograr analizando solamente los archivos nuevos y aquellos que se han modificado desde el análisis anterior. Este modo se aplica tanto a archivos simples como compuestos.

También puede habilitar el uso de las tecnologías iChecker y iSwift, que optimizan la velocidad del análisis de archivos al excluir los archivos que no se han modificado desde el análisis más reciente.

Para optimizar el análisis de archivos:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Optimización**, seleccione la casilla **Analizar solo archivos nuevos y modificados**.
5. Guarde los cambios.

Análisis de archivos compuestos

Una técnica común para ocultar virus u otro malware es implantarlo en archivos compuestos, como archivos de almacenamiento o bases de datos. Para detectar virus u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

El método utilizado para procesar un archivo compuesto infectado (desinfección o eliminación) depende del tipo de archivo.

El componente Protección contra archivos peligrosos desinfecta los archivos compuestos con formato ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, ICE y JAR, y elimina archivos en todos los formatos restantes (excepto bases de datos de correo).

Para configurar el análisis de archivos compuestos:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.
3. Haga clic en **Configuración avanzada**.
4. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución, correo o archivos con formato de Office.
5. Si el análisis de solo archivos nuevos y modificados está desactivado, defina la configuración para analizar cada tipo de archivo compuesto: analice todos los archivos de este tipo o solo los archivos nuevos.

   Si está habilitado el análisis de archivos nuevos y modificados, Kaspersky Endpoint Security analiza solo archivos nuevos y modificados de todos los tipos de archivos compuestos.
6. Defina la configuración avanzada para analizar archivos compuestos.

   - **No desempaquetar archivos compuestos de gran tamaño**.

     Si esta casilla está seleccionada, Kaspersky Endpoint Security no analiza los archivos compuestos si su tamaño excede el valor.

Si esta casilla está desactivada, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.

> Kaspersky Endpoint Security analiza los archivos de gran tamaño que se extraen de archivos comprimidos, independientemente de si la casilla **No desempaquetar archivos compuestos de gran tamaño** está seleccionada.

- **Descomprimir archivos compuestos en segundo plano**.

  Si activa esta casilla, Kaspersky Endpoint Security permitirá acceder a los archivos compuestos que superen el tamaño especificado antes de que se los haya analizado. En este caso, Kaspersky Endpoint Security descomprimirá y analizará los archivos compuestos en segundo plano.

  Kaspersky Endpoint Security proporciona acceso a los archivos compuestos que son más pequeños que este valor solo después de descomprimir y analizar estos archivos.

  Si no activa esta casilla, Kaspersky Endpoint Security no permitirá acceder a ningún archivo compuesto, independientemente de su tamaño, hasta que se lo haya descomprimido y analizado.

7. Guarde los cambios.

Modificación del modo de análisis

El *Modo de análisis* hace referencia a la condición que desencadena el análisis del archivo del componente Protección contra archivos peligrosos. Por defecto, Kaspersky Endpoint Security analiza los archivos en el modo inteligente. En este modo de análisis de archivos, el componente Protección contra archivos peligrosos decide si analiza o no los archivos después de analizar las operaciones realizadas con el archivo por el usuario, por una aplicación en nombre del usuario (en la cuenta que se usó para iniciar sesión o en otra cuenta de usuario) o por el sistema operativo. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office Word la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo.

Para modificar el modo de análisis de archivos:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Modo de análisis**, seleccione el modo que desea utilizar:

   - **Modo inteligente**. En este modo, Protección contra archivos peligrosos analiza un objeto en función de las operaciones realizadas sobre ese objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo.

   - **Ante operaciones de acceso y modificación**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos siempre que haya un intento de abrirlos o modificarlos.

- **Ante operaciones de acceso**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos solo después de un intento de abrirlos.

- **Ante operaciones de ejecución**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos después de un intento de ejecutarlos.

5. Guarde los cambios.

Análisis de contenedores

Un *contenedor* es un entorno aislado en el que una aplicación puede ejecutarse sin interactuar directamente con el sistema operativo. El uso de contenedores conlleva los siguientes riesgos:

- Los piratas informáticos pueden aprovechar las vulnerabilidades de la contenedorización para poner en peligro las aplicaciones dentro del contenedor.

- Los piratas informáticos pueden explotar una configuración poco segura del entorno del contenedor para obtener acceso no autorizado a los datos del equipo o para comprometer 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 la red.

Kaspersky Endpoint Security analiza archivos no solo en los discos, sino también dentro de los contenedores. Es decir, Kaspersky Endpoint Security es una herramienta externa para detectar actividad maliciosa dentro de contenedores. Esto permite mantener el rendimiento de los contenedores y evita conflictos con otras aplicaciones dentro del contenedor. La instalación de Kaspersky Endpoint Security dentro del contenedor no es compatible.

Además de proporcionar seguridad para los contenedores, Kaspersky Endpoint Security permite administrar aplicaciones dentro de contenedores mediante el Control de aplicaciones. El Control de aplicaciones está configurado para contenedores de la misma manera que para las 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 contenedorización.

- El contenedor debe ejecutarse en el modo de aislamiento de procesos. El modo de aislamiento de Hyper-V no es compatible.

- 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 son compatibles. Las imágenes de Linux no son compatibles.

Acción al detectar amenaza

Si se detecta una amenaza dentro de un contenedor, la aplicación aplica la acción seleccionada para el componente Protección contra amenazas de archivo. 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 puede desinfectarse. De manera predeterminada, la funcionalidad de detención de contenedores está deshabilitada.

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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.
4. Haga clic en **Configuración**.
5. En la ventana que se abre, seleccione la pestaña **Adicional**.
6. En el bloque **Análisis de las operaciones sobre archivos ejecutadas en contenedores de Windows**, ajuste la configuración del análisis de contenedores:
   - **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 se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.
   - **No analizar las operaciones sobre archivos ejecutadas en contenedores de Windows**. Si esta casilla está seleccionada, la aplicación analiza el contenedor solo al inicio. Si no se selecciona la casilla, 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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Protección contra amenazas de archivo**.
5. En **Configuración avanzada**, seleccione la pestaña **Rendimiento**.

6. En el bloque **Optimización de análisis**, ajuste la configuración del análisis de contenedores:

   - **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 se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.

   - **No analizar las operaciones ejecutadas en contenedores de Windows**. Si esta casilla está seleccionada, la aplicación analiza el contenedor solo al inicio. Si no se selecciona la casilla, 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 principal de la aplicación haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.

3. En el bloque **Análisis de las operaciones sobre archivos ejecutadas en contenedores de Windows**, ajuste la configuración del análisis de contenedores:

   - **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 se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.

   - **No analizar las operaciones sobre archivos ejecutadas en contenedores de Windows**. Si esta casilla está seleccionada, la aplicación analiza el contenedor solo al inicio. Si no se selecciona la casilla, la aplicación analiza el contenedor continuamente en tiempo real.

4. Guarde los cambios.

Prevención de intrusiones en el host

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El componente Prevención contra intrusos impide que las aplicaciones realicen acciones que puedan ser peligrosas para el sistema operativo y garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus y el servicio de nube Kaspersky Security Network.

Para controlar el funcionamiento de las aplicaciones, el componente se basa en los *derechos* que estas tienen asignados. Los siguientes parámetros de acceso son algunos de esos derechos:

- Acceso a los recursos del sistema operativo (claves del Registro, opciones de ejecución automática, etc.)
- Acceso a datos personales (archivos, aplicaciones, etc.)

Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

Cuando una aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host hace lo siguiente:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.
2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Prevención de intrusiones en el host, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima* o *No confiables*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea las acciones de la aplicación tomando como referencia el grupo de confianza al que pertenece. Por ejemplo, las aplicaciones del grupo *Restricción máxima* no pueden acceder a los módulos del sistema operativo.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

Habilitación y deshabilitación de la Prevención de intrusiones en el host

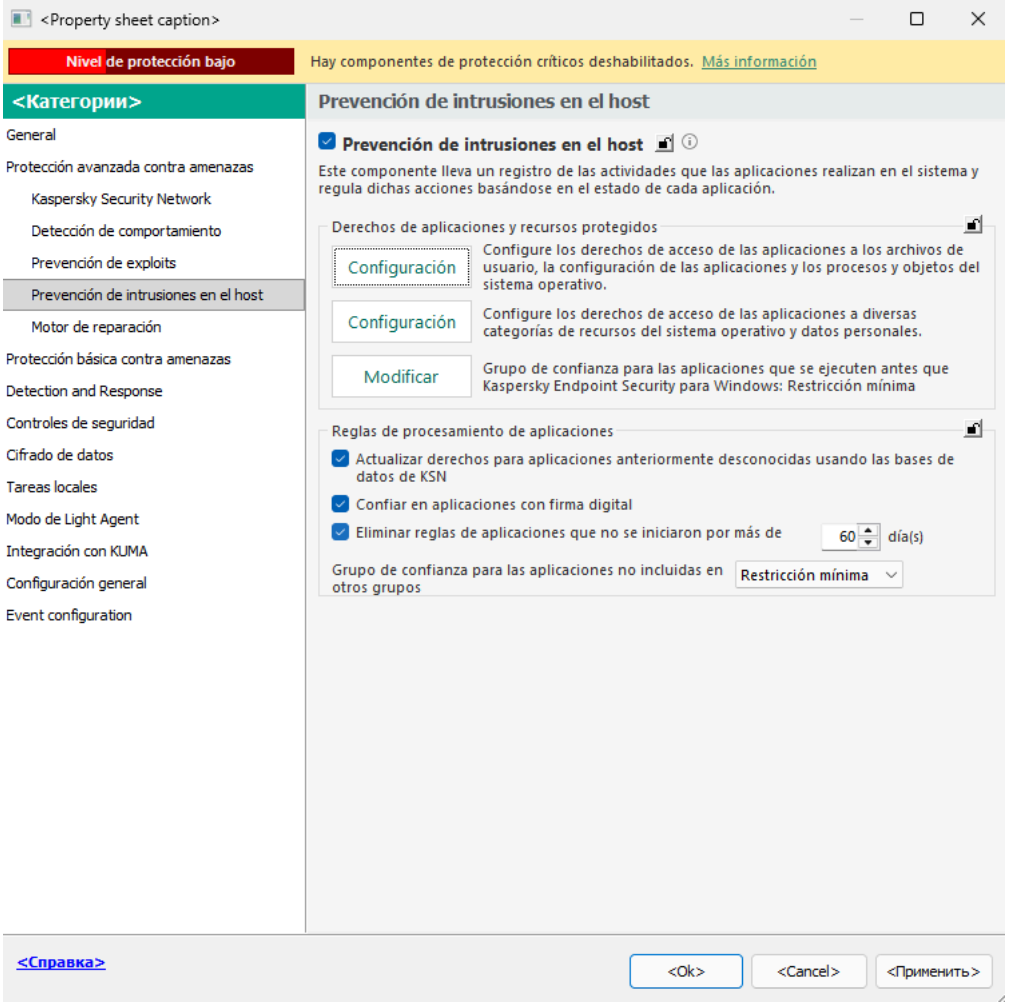
De manera predeterminada, el componente Prevención de intrusiones en el host está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky.

Cómo habilitar o deshabilitar el componente Prevención de intrusiones en el host 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. Utilice la casilla **Prevención de intrusiones en el host** para habilitar o deshabilitar el componente.

5. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar el componente Prevención de intrusiones en el host 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. Use el interruptor **Prevención de intrusiones en el host HABILITADA** para habilitar o deshabilitar el componente.

6. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Prevención de intrusiones en el host mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. Use el interruptor **Prevención de intrusiones en el host** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

Si habilita el componente Prevención de intrusiones en el host, Kaspersky Endpoint Security definirá el grupo de confianza de una aplicación teniendo en cuenta lo peligrosa que pueda resultar para el equipo. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo.

Administración de grupos de confianza de aplicaciones

Cuando se inicia cada aplicación por primera vez, el componente Prevención de intrusiones en el host comprueba la seguridad de la aplicación y la ubica 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). En función de los resultados de la búsqueda en la base de datos interna y la base de datos de Kaspersky Security Network, se ubica a la aplicación en un grupo de confianza. Cada vez que se inicia la aplicación, Kaspersky Endpoint Security envía una consulta nueva a la base de datos de KSN y ubica la aplicación en un grupo de confianza diferente si ha cambiado la reputación de la aplicación en las bases de datos de KSN.

Puede seleccionar el grupo de confianza donde Kaspersky Endpoint Security colocará todas las aplicaciones desconocidas automáticamente. Las aplicaciones que se ejecutaron antes de que se iniciara Kaspersky Endpoint Security se colocan automáticamente en el grupo de confianza determinado en la configuración de Prevención de intrusiones en el host.

Para aplicaciones que se iniciaron antes de Kaspersky Endpoint Security, solamente se supervisa la actividad de red. El control se realiza utilizando las reglas de red definidas en la configuración de Firewall.

Modificación del grupo de confianza de una aplicación

Cuando se inicia cada aplicación por primera vez, el componente Prevención de intrusiones en el host comprueba la seguridad de la aplicación y la ubica en uno de los grupos de confianza.

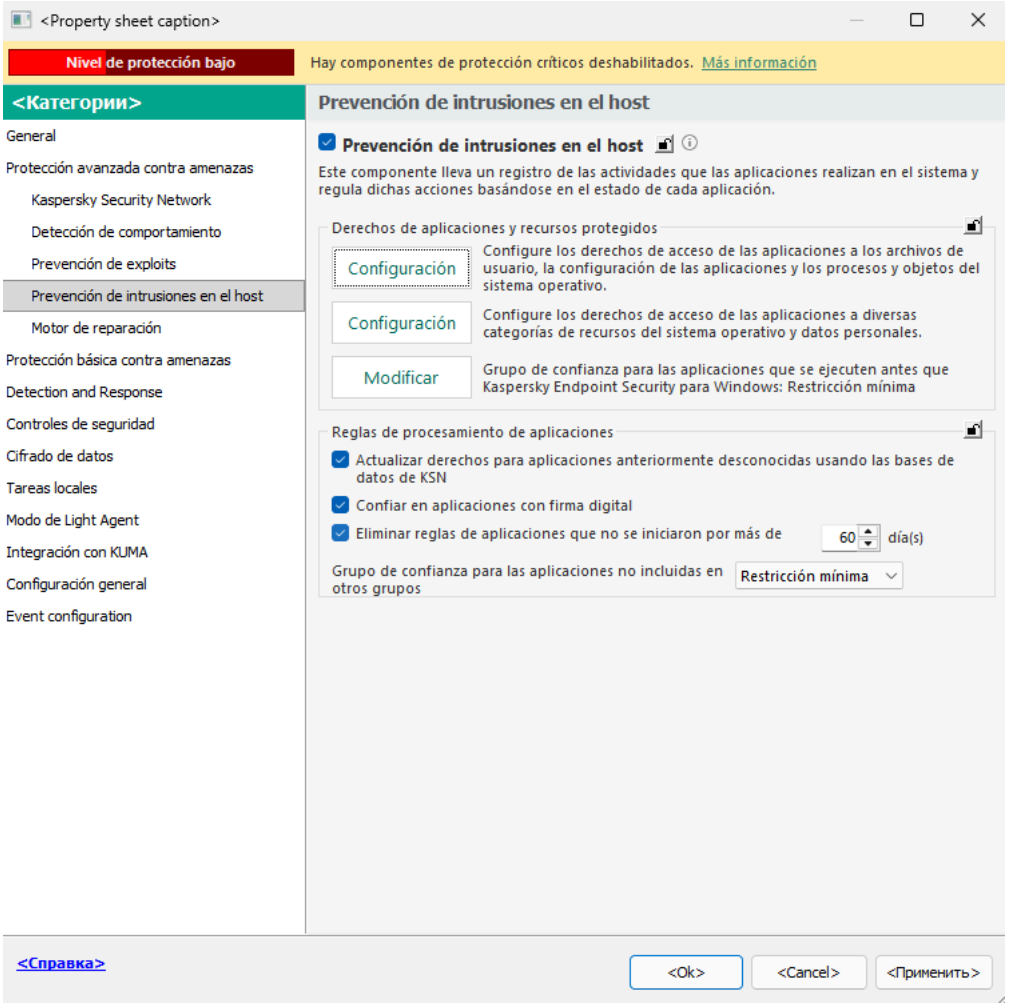
> Los especialistas de Kaspersky no recomiendan mover las aplicaciones del grupo de confianza asignado automáticamente a un grupo diferente. Considere, en cambio, modificar los derechos de una aplicación en particular cuando resulte necesario.

Cómo cambiar el grupo de confianza de una aplicación 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **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 una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

5. Seleccione la ficha **Derechos de aplicaciones**.

6. Haga clic en **Agregar**.

7. En la ventana que se abre, escriba un criterio de búsqueda para dar con la aplicación cuyo grupo de confianza desee cambiar.

   Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

8. Haga clic en **Actualizar**.

   Kaspersky Endpoint Security buscará la aplicación en una lista consolidada, en la que se recogen las aplicaciones instaladas en los equipos administrados. Las aplicaciones que coincidan con los criterios de búsqueda se mostrarán en una lista.

9. Seleccione la aplicación necesaria.

10. En la lista desplegable **Agregar la aplicación seleccionada al grupo de confianza**, seleccione un grupo de confianza para la aplicación.

11. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo cambiar el grupo de confianza de una 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

6. Seleccione la ficha **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.

7. Haga clic en **Agregar**.

   Se inicia un asistente para agregar la aplicación a un grupo de confianza.

8. Seleccione el grupo de confianza correspondiente para la aplicación.

9. Seleccione el tipo **Aplicación**. Vaya al siguiente paso.

   Para cambiar el grupo de confianza de más de una aplicación, seleccione el tipo **Grupo** y escriba un nombre para el grupo de aplicaciones.

10. En la lista de aplicaciones que se abre, seleccione las aplicaciones para las que se cambiará el grupo de confianza.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

11. Salga del Asistente.

    La aplicación se agregará al grupo de confianza.

12. Guarde los cambios.

Cómo cambiar el grupo de confianza de una aplicación mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. Haga clic en **Administrar aplicaciones**.

   Esto abre la lista de aplicaciones instaladas.

4. Seleccione la aplicación necesaria.

5. En el menú contextual de la aplicación, haga clic en **Restricciones** → **<grupo de confianza>**.

6. Guarde los cambios.

La aplicación se agregará al nuevo grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo. Se asignará el estado *(definido por el usuario)* a la aplicación. El componente Prevención de intrusiones en el host mantendrá la aplicación en el grupo definido por el usuario incluso si la reputación de la misma se modifica en Kaspersky Security Network.

Configuración de los derechos disponibles en los grupos de confianza

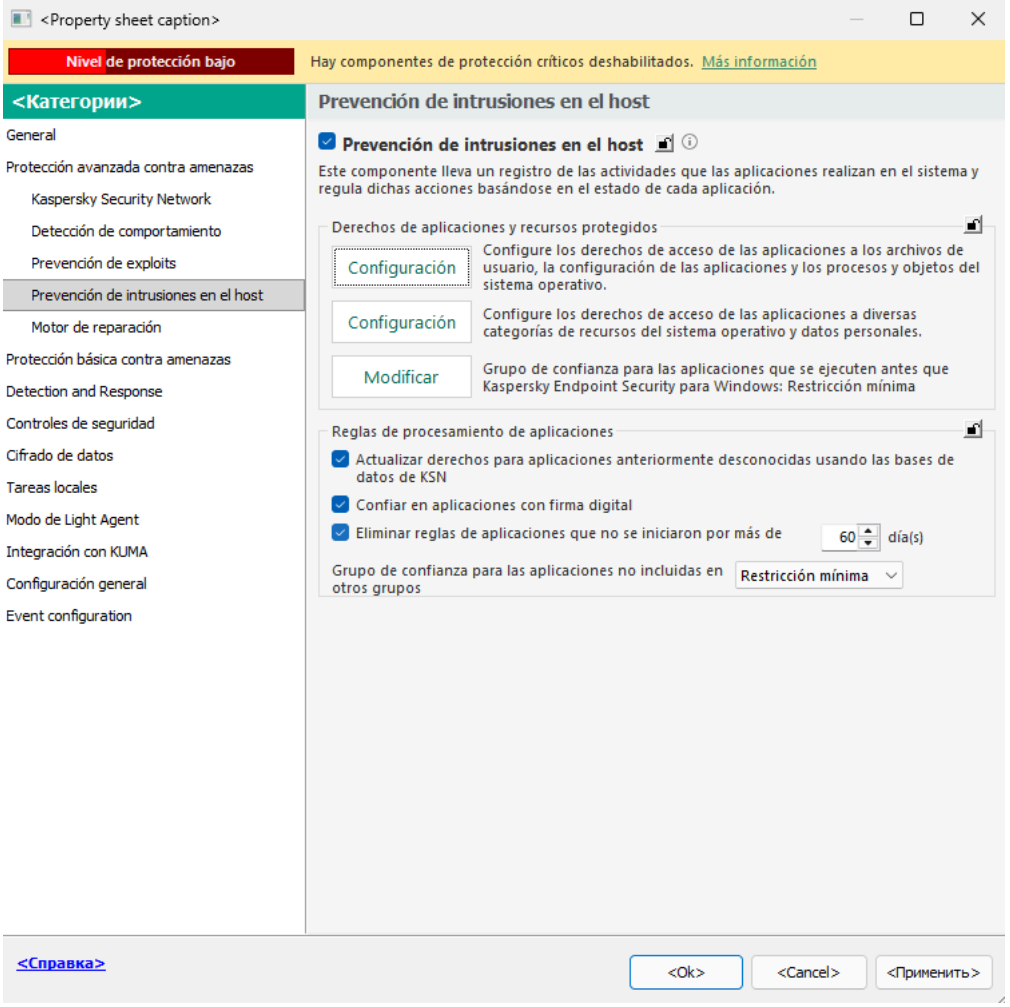
De manera predeterminada, los grupos de confianza tienen definidos los derechos óptimos para cada categoría de aplicaciones. Los grupos de aplicaciones que forman parte de un grupo de confianza heredan de este la configuración de sus derechos.

Cómo cambiar los derechos de un grupo de confianza 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → 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 una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

5. Vaya a la pestaña **Derechos de aplicaciones**.

6. Seleccione el grupo de confianza necesario.

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:

   - Seleccione **Archivos y registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.

   - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

9. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Permitir** (✓) o **Bloquear** (⊘).

10. Seleccione la opción **Registrar eventos** (✓ / ⊘) si le interesa supervisar cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

11. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo cambiar los derechos de un grupo de confianza 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

6. Vaya a la pestaña **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.

7. En la parte izquierda de la ventana, seleccione el grupo de confianza pertinente.

8. En la parte derecha de la ventana, en la lista desplegable, realice una de las siguientes acciones:

   - Seleccione **Archivos y registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.

   - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

   Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

9. Busque el recurso en el que esté interesado y seleccione una opción en la columna con la acción pertinente: **Heredar**, **Permitir** (✓), **Bloquear** (✕).

10. Seleccione la opción **Registrar eventos** (/) si le interesa supervisar cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

11. Guarde los cambios.

Cómo cambiar los derechos de un grupo de confianza mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **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 necesario.

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:

   - Seleccione **Archivos y registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.

   - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

   Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

7. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Permitir** ( ) o **Denegar** ( ).

8. Seleccione la opción **Registrar eventos** ( ) si le interesa supervisar cómo se utilizan los recursos del equipo.

   Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

9. Guarde los cambios.

Se cambiarán los derechos del grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo. El grupo pasará a tener el estado (*Configuración personalizada*).

Selección de un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security

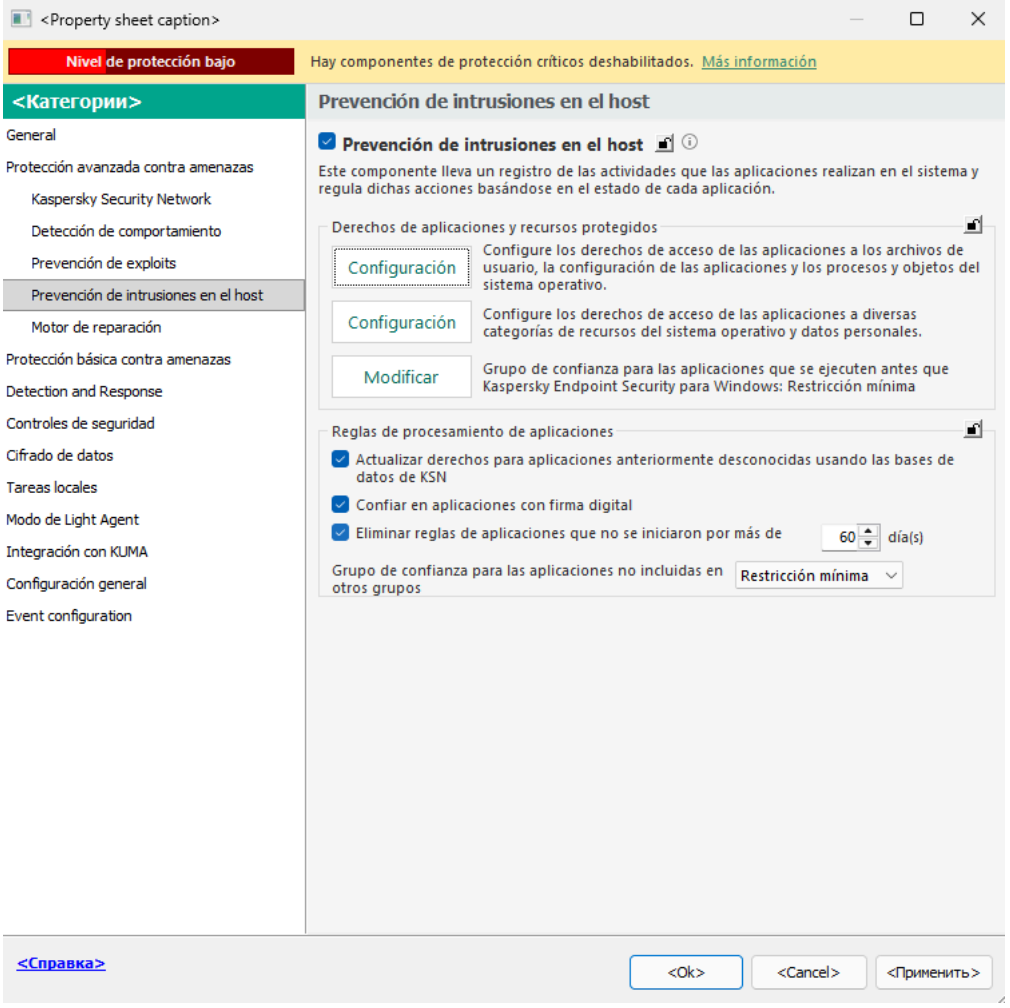
Para aplicaciones que se iniciaron antes de Kaspersky Endpoint Security, solamente se supervisa la actividad de red. El control se realiza utilizando las reglas de red definidas en la configuración de Firewall. Para especificar qué reglas de red se deben aplicar a la supervisión de la actividad de red para dichas aplicaciones, debe seleccionar un grupo de confianza.

Cómo seleccionar un grupo de confianza para las aplicaciones que se inicien antes que Kaspersky Endpoint Security 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **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 la configuración **Grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security**, seleccione el grupo de confianza correspondiente.

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

Cómo seleccionar un grupo de confianza para las aplicaciones que se inicien antes que Kaspersky Endpoint Security 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. Para la configuración **Grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security**, seleccione el grupo de confianza correspondiente.

6. Guarde los cambios.

Cómo seleccionar un grupo de confianza para las aplicaciones que se inicien antes que Kaspersky Endpoint Security mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. En el bloque **Grupo de confianza para las aplicaciones que se ejecuten antes que Kaspersky Endpoint Security**, seleccione el grupo de confianza correspondiente.

4. Guarde los cambios.

Como resultado, cualquier aplicación que se inicie antes que Kaspersky Endpoint Security se ubicará en el grupo de confianza que acaba de definir. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo.

Selección del grupo de confianza para aplicaciones desconocidas

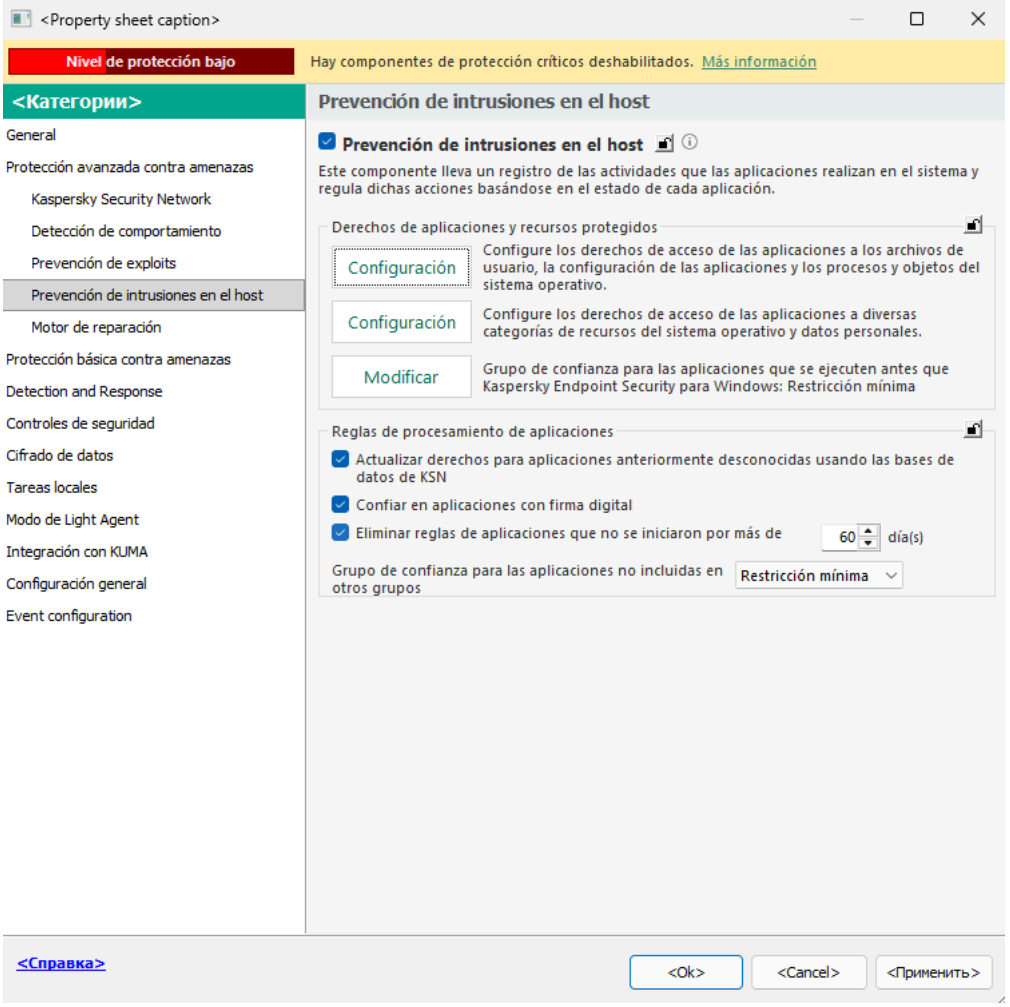
Cuando una aplicación se ejecuta por primera vez, el componente Prevención de intrusiones en el host la asigna a un grupo de confianza. De manera predeterminada, cuando una aplicación no está registrada en Kaspersky Security Network, se la agrega al grupo *Restricción mínima*. Lo mismo ocurre cuando el equipo no tiene acceso a Internet. Si KSN incorpora, en algún momento, datos sobre una aplicación que originariamente se consideró desconocida, Kaspersky Endpoint Security modificará los derechos de la misma. De ocurrir esto, podrá modificar los derechos manualmente.

Cómo seleccionar el grupo de confianza para aplicaciones desconocidas 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la lista desplegable **Grupo de confianza para aplicaciones no incluidas en otros grupos** para seleccionar el grupo de confianza que desee.

   Si ha optado por participar en Kaspersky Security Network, cada vez ejecuta una aplicación, Kaspersky Endpoint Security envía una consulta a KSN para determinar la reputación de la misma. En función de la respuesta recibida, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración del componente Prevención contra intrusos.

5. Utilice la casilla **Actualizar derechos para aplicaciones anteriormente desconocidas usando las bases de datos de KSN** para determinar si los derechos de las aplicaciones desconocidas deberán actualizarse automáticamente.

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

Cómo seleccionar el grupo de confianza para aplicaciones desconocidas 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la lista desplegable **Grupo de confianza para aplicaciones no incluidas en otros grupos** para seleccionar el grupo de confianza que desee.

   Si ha optado por participar en Kaspersky Security Network, cada vez ejecuta una aplicación, Kaspersky Endpoint Security envía una consulta a KSN para determinar la reputación de la misma. En función de la respuesta recibida, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración del componente Prevención contra intrusos.

6. Utilice la casilla **Actualizar derechos para aplicaciones anteriormente desconocidas usando las bases de datos de KSN** para determinar si los derechos de las aplicaciones desconocidas deberán actualizarse automáticamente.

7. Guarde los cambios.

Cómo seleccionar el grupo de confianza para aplicaciones desconocidas mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. En el bloque **Reglas de procesamiento de aplicaciones**, seleccione el grupo de confianza correspondiente.

   Si ha optado por participar en Kaspersky Security Network, cada vez ejecuta una aplicación, Kaspersky Endpoint Security envía una consulta a KSN para determinar la reputación de la misma. En función de la respuesta recibida, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración del componente Prevención contra intrusos.

4. Utilice la casilla **Actualizar reglas de aplicaciones anteriormente desconocidas desde KSN** para determinar si los derechos de las aplicaciones desconocidas deberán actualizarse automáticamente.

5. Guarde los cambios.

Selección del grupo de confianza para aplicaciones con firma digital

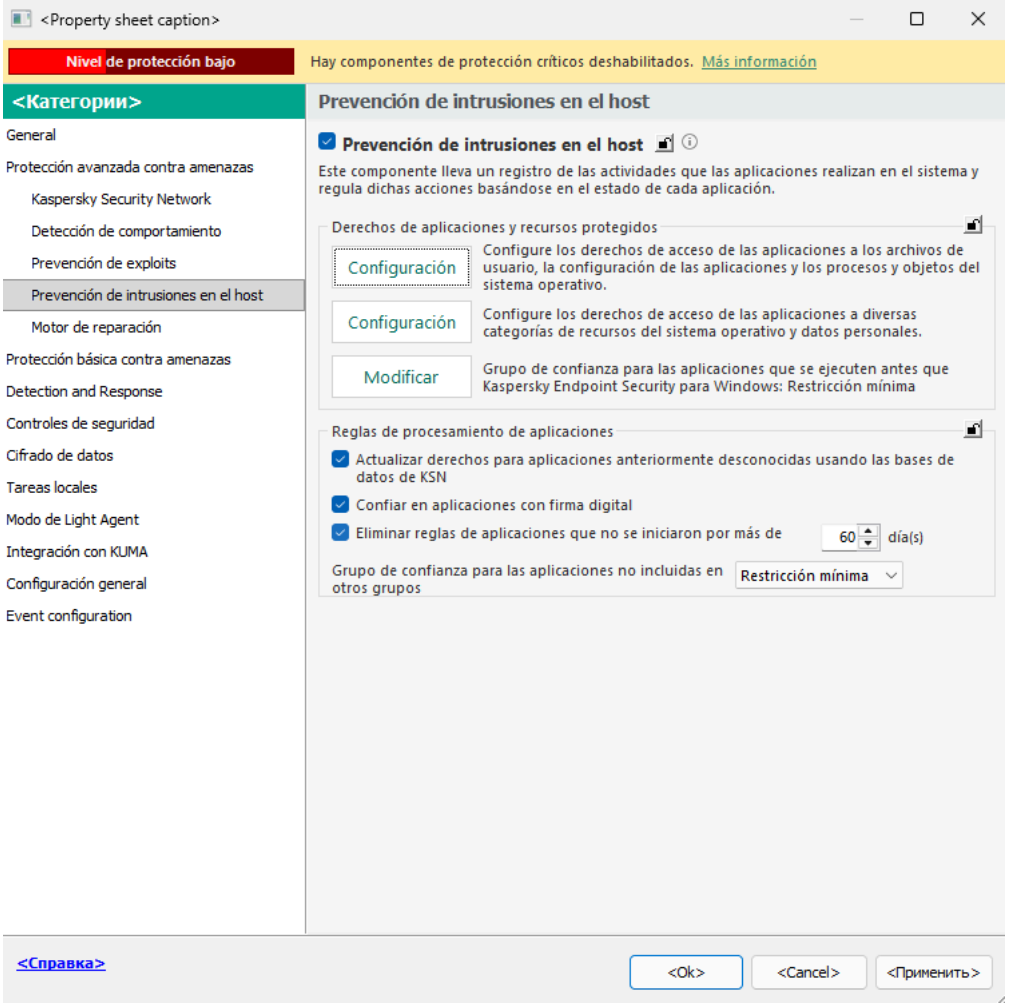
Kaspersky Endpoint Security siempre coloca las aplicaciones firmadas por certificados de Microsoft Office o Kaspersky en el grupo *De confianza*.

Cómo seleccionar un grupo de confianza para las aplicaciones con firma digital 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Reglas de procesamiento de aplicaciones**, use la casilla de verificación **Confiar en aplicaciones con firma digital** para indicar si las aplicaciones que tengan la firma digital de un proveedor de confianza deberán asignarse automáticamente al grupo De confianza.

   Se considera proveedor de confianza a todo aquel que Kaspersky ha incluido en el grupo de confianza. Si lo desea, puede agregar manualmente el certificado de un proveedor al almacén de confianza de certificados del sistema.

   Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que las aplicaciones con firma digital sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.

5. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo seleccionar un grupo de confianza para las aplicaciones con firma digital 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Reglas de procesamiento de aplicaciones**, use la casilla de verificación **Confiar en aplicaciones con firma digital** para indicar si las aplicaciones que tengan la firma digital de un proveedor de confianza deberán asignarse automáticamente al grupo De confianza.

   Se considera proveedor de confianza a todo aquel que Kaspersky ha incluido en el grupo de confianza. Si lo desea, puede agregar manualmente el certificado de un proveedor al almacén de confianza de certificados del sistema.

   Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que las aplicaciones con firma digital sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.

6. Guarde los cambios.

Cómo seleccionar un grupo de confianza para las aplicaciones con firma digital mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. En el bloque **Reglas de procesamiento de aplicaciones**, use la casilla de verificación **Confiar en aplicaciones con firma digital** para indicar si las aplicaciones que tengan la firma digital de un proveedor de confianza deberán asignarse automáticamente al grupo De confianza.

   Se considera proveedor de confianza a todo aquel que Kaspersky ha incluido en el grupo de confianza. Si lo desea, puede agregar manualmente el certificado de un proveedor al almacén de confianza de certificados del sistema.

   Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que las aplicaciones con firma digital sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.

4. Guarde los cambios.

Administración de los derechos de las aplicaciones

Por defecto, la actividad de una aplicación se controla a través de los derechos de aplicaciones definidos para el grupo de confianza al que la aplicación pertenece. El grupo de confianza de una aplicación se determina cuando se la ejecuta por primera vez. Si lo necesita, puede modificar los derechos de todo un grupo de confianza, de una aplicación individual o de un grupo de aplicaciones pertenecientes a un grupo de confianza determinado.

Los derechos que se definen manualmente tienen mayor prioridad que los que se han determinado para un grupo de confianza. En otras palabras, cuando una aplicación tiene derechos que se han definido para ella manualmente y derechos que ha heredado de su grupo de confianza, el componente Prevención de intrusiones en el host toma como válidos los derechos definidos manualmente y controla la actividad de la aplicación basándose en ellos.

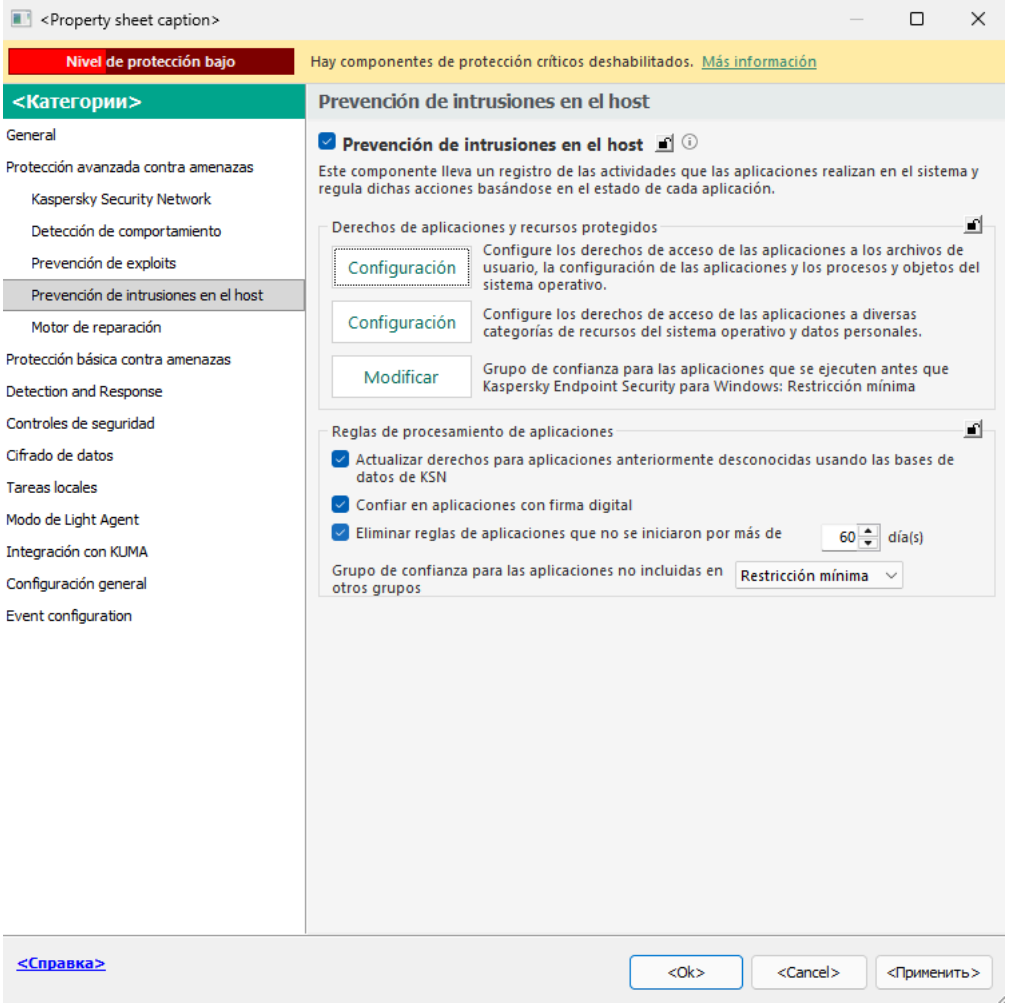
Las reglas que se crean para una aplicación son heredadas por las aplicaciones secundarias. Esto quiere decir, por ejemplo, que si bloquea por completo las actividades de red para cmd.exe, el acceso a la red también estará bloqueado para notepad.exe si dicho programa se inicia a través de cmd.exe. Cuando una aplicación no es una aplicación secundaria de la aplicación desde la que se ejecuta, las reglas no se heredan.

Cómo cambiar los derechos de una 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → 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 una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

5. Vaya a la pestaña **Derechos de aplicaciones**.

6. Haga clic en **Agregar**.

7. En la ventana que se abre, escriba un criterio de búsqueda para dar con la aplicación cuyos derechos desea cambiar.

   Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

8. Haga clic en **Actualizar**.

   Kaspersky Endpoint Security buscará la aplicación en una lista consolidada, en la que se recogen las aplicaciones instaladas en los equipos administrados. Las aplicaciones que coincidan con los criterios de búsqueda se mostrarán en una lista.

9. Seleccione la aplicación necesaria.

10. En la lista desplegable **Agregar la aplicación seleccionada al grupo de confianza**, seleccione **Grupos por defecto** y haga clic en **Aceptar**.

    La aplicación se agregará al grupo por defecto.

11. Seleccione la aplicación de su interés, abra al menú contextual de la misma y haga clic en el elemento **Derechos de aplicaciones**.

    Se abren las propiedades de la aplicación.

12. Realice una de las siguientes acciones:

    - Seleccione **Archivos y registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.

    - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

    Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

13. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Permitir** ( ) o **Bloquear** ( ).

14. Seleccione la opción **Registrar eventos** (/) si le interesa supervisar cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

15. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo cambiar los derechos de una 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

6. Vaya a la pestaña **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.

7. Haga clic en **Agregar**.

   Se inicia un asistente para agregar la aplicación a un grupo de confianza.

8. Seleccione el grupo de confianza correspondiente para la aplicación.

9. Seleccione el tipo **Aplicación**. Vaya al siguiente paso.

   Para cambiar el grupo de confianza de más de una aplicación, seleccione el tipo **Grupo** y escriba un nombre para el grupo de aplicaciones.

10. En la lista de aplicaciones que se abre, seleccione las aplicaciones cuyos derechos desee cambiar.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

11. Salga del Asistente.

    La aplicación se agregará al grupo de confianza.

12. En la parte izquierda de la ventana, seleccione la aplicación de su interés.

13. En la parte derecha de la ventana, en la lista desplegable, realice una de las siguientes acciones:

    - Seleccione **Archivos y registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.

    - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

    Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

14. Busque el recurso en el que esté interesado y seleccione una opción en la columna con la acción pertinente: **Heredar**, **Permitir** ( ), **Bloquear** ( ).

15. Seleccione la opción **Registrar eventos** (/) si le interesa supervisar cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

16. Guarde los cambios.

Cómo cambiar los derechos de una aplicación mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. Haga clic en **Administrar aplicaciones**.

   Esto abre la lista de aplicaciones instaladas.

4. Seleccione la aplicación necesaria.

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:

   - Seleccione **Archivos y registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.

   - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

7. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Permitir** ( ) o **Denegar** ( ).

8. Seleccione la opción **Registrar eventos** ( ) si le interesa supervisar cómo se utilizan los recursos del equipo.

   Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

9. Seleccione la pestaña **Exclusiones** y configure los parámetros avanzados de la aplicación (vea la tabla de más abajo).

10. Guarde los cambios.

Parámetros avanzados de la aplicación

Parámetro	Descripción
No verificar archivos abiertos por esta aplicación	Kaspersky Endpoint Security no analizará ningún archivo que la aplicación abra. 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 la red y los archivos de la aplicación en el sistema operativo. Puede configurar la supervisión de la actividad de las aplicaciones para diferentes componentes de Kaspersky Endpoint Security: • **No supervisar los componentes de protección y control**. La actividad de la aplicación se supervisa 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 y Endpoint Detection and Response**. La actividad de las aplicaciones se supervisa a través del agente MDR incorporado y el EDR (KATA) agent incorporado. • **No interceptar entradas interactivas de la consola de Endpoint Detection and Response**. Kaspersky Endpoint Security no envía datos de telemetría sobre la administración de la aplicación en la consola. Los datos de telemetría son utilizados por Kaspersky Anti Targeted Attack Platform (EDR).
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 lo inicia una aplicación para la que se configuran los derechos de aplicaciones (Prevención de intrusiones en el host) y las reglas de red de aplicaciones (Firewall).
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Endpoint Security no supervisará las actividades de red ni las operaciones de archivo que realicen las aplicaciones iniciadas por la aplicación. Puede aplicar la exclusión de manera recurrente. De esta manera, la aplicación no supervisa la actividad de toda la cadena de aplicaciones secundarias.
Permitir interacción con la interfaz de Kaspersky Endpoint Security	La Autoprotección de Kaspersky Endpoint Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona esta casilla, se permite que la aplicación de acceso remoto administre la configuración de Kaspersky Endpoint Security a través de la interfaz de Kaspersky Endpoint Security.
No analizar el tráfico cifrado/No analizar todo el tráfico	Kaspersky Endpoint Security no analizará el tráfico de red que tenga origen en la aplicación. Puede excluir de los análisis todo el tráfico o solo el tráfico cifrado. También puede excluir direcciones IP y números de puerto individuales 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 datos personales

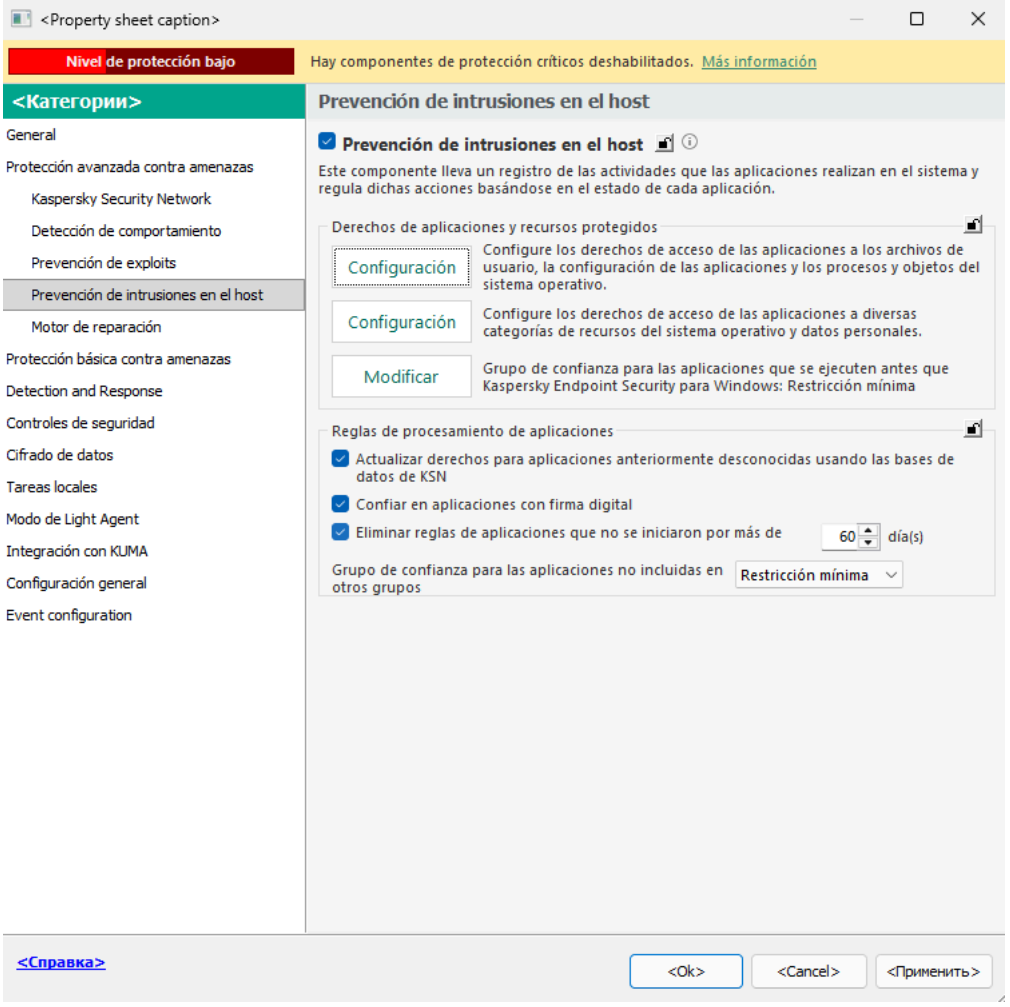
El componente Prevención de intrusiones en el host administra los derechos de aplicaciones de realizar acciones en varias categorías de recursos del sistema operativo y datos personales. Los especialistas de Kaspersky han establecido categorías predefinidas de recursos protegidos. Por ejemplo, la categoría *Sistema operativo* tiene una subcategoría llamada *Configuración de inicio*, en la que se reúnen todas las claves del Registro asociadas a la autoejecución de aplicaciones. No puede modificar ni eliminar las categorías predefinidas de recursos protegidos o los recursos protegidos que están dentro de estas categorías.

Cómo agregar un recurso protegido 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **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 una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

5. Vaya a la pestaña **Recursos protegidos**.

   En la parte izquierda de la ventana, verá una lista de recursos protegidos; los derechos para acceder a esos recursos estarán en el lado derecho. Los derechos varían según el grupo de confianza.

6. Seleccione la categoría de recursos protegidos a los que desea agregar un nuevo recurso protegido.

   Si desea agregar una subcategoría, haga clic en **Agregar** → **Categoría**.

7. Haga clic en el botón **Agregar**. En la lista desplegable, seleccione el tipo de recurso que desee agregar: **Archivo o carpeta** o **Clave del Registro**.

8. En la ventana que se abre, seleccione un archivo, una carpeta o una clave del registro.

   Puede ver cuáles son los derechos con los que cuentan las aplicaciones para acceder a los recursos agregados. Si selecciona un recurso en la parte izquierda de la ventana, Kaspersky Endpoint Security le mostrará los derechos de acceso correspondientes a cada grupo de confianza. Si no necesita controlar el uso que las aplicaciones hagan de un recurso nuevo, utilice la casilla ubicada junto al recurso en cuestión.

9. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo agregar un recurso protegido 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

6. Vaya a la pestaña **Recursos protegidos**.

   En la parte izquierda de la ventana, verá una lista de recursos protegidos; los derechos para acceder a esos recursos estarán en el lado derecho. Los derechos varían según el grupo de confianza.

7. Haga clic en **Agregar**.

   Se abre el asistente para agregar recursos.

8. En el bloque **Nombre del grupo**, seleccione la categoría de recursos protegidos a la que se agregará el nuevo recurso protegido.

   Si desea agregar una subcategoría, seleccione la opción **Categoría de recursos protegidos**.

9. Seleccione el tipo de recurso que desee agregar: **Archivo o carpeta** o **Clave del Registro**.

10. Seleccione un archivo, una carpeta o una clave del Registro.

11. Salga del Asistente.

    Puede ver cuáles son los derechos con los que cuentan las aplicaciones para acceder a los recursos agregados. Si selecciona un recurso en la parte izquierda de la ventana, Kaspersky Endpoint Security le mostrará los derechos de acceso correspondientes a cada grupo de confianza. Si no necesita controlar el uso que las aplicaciones hagan de los recursos, utilice la casilla ubicada en la columna **Estado**.

12. Guarde los cambios.

Cómo agregar un recurso protegido mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **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 agregar un nuevo recurso protegido.

   Si desea agregar una subcategoría, haga clic en **Agregar** → **Categoría**.

5. Haga clic en el botón **Agregar**. En la lista desplegable, seleccione el tipo de recurso que desee agregar: **Archivo o carpeta** o **Clave del Registro**.

6. En la ventana que se abre, seleccione un archivo, una carpeta o una clave del registro.

   Puede ver cuáles son los derechos con los que cuentan las aplicaciones para acceder a los recursos agregados. Si selecciona un recurso en la parte izquierda de la ventana, Kaspersky Endpoint Security le mostrará una lista de aplicaciones con sus correspondientes derechos de acceso. Si no necesita controlar el uso que las aplicaciones hagan de los recursos, utilice el botón **Habilitar control**, ubicado en la columna **Estado**.

7. Guarde los cambios.

Kaspersky Endpoint Security controlará el acceso a los recursos del sistema operativo y a los datos personales especificados. El acceso de las aplicaciones a cada recurso variará en función del grupo de confianza al que pertenezca la aplicación. El grupo de confianza de una aplicación puede modificarse.

Eliminación de la información sobre las aplicaciones en desuso

En Kaspersky Endpoint Security, las actividades de las aplicaciones se controlan a través de derechos. Los derechos de una aplicación están determinados por su grupo de confianza. El grupo de confianza en el que Kaspersky Endpoint Security coloca una aplicación se determina cuando esta se ejecuta por primera vez. El grupo de confianza puede cambiarse manualmente. También es posible configurar manualmente los derechos de una aplicación específica. Kaspersky Endpoint Security almacena los derechos y el grupo de confianza de cada aplicación.

Para conservar recursos, Kaspersky Endpoint Security elimina automáticamente la información de las aplicaciones que ya no se utilizan. La información se elimina según las siguientes reglas:

- Cuando el grupo de confianza y los derechos de una aplicación se determinaron automáticamente, Kaspersky Endpoint Security elimina la información de esa aplicación luego de 30 días. El plazo de almacenamiento de la información no se puede modificar, y tampoco es posible desactivar la eliminación automática.

- Cuando el grupo de confianza o los derechos de acceso de una aplicación se determinaron manualmente, Kaspersky Endpoint Security elimina la información de esa aplicación después de 60 días (este es el plazo de almacenamiento predeterminado). En este caso, el plazo de almacenamiento sí puede modificarse, y también es posible desactivar la eliminación automática (encontrará instrucciones para tal fin más abajo).

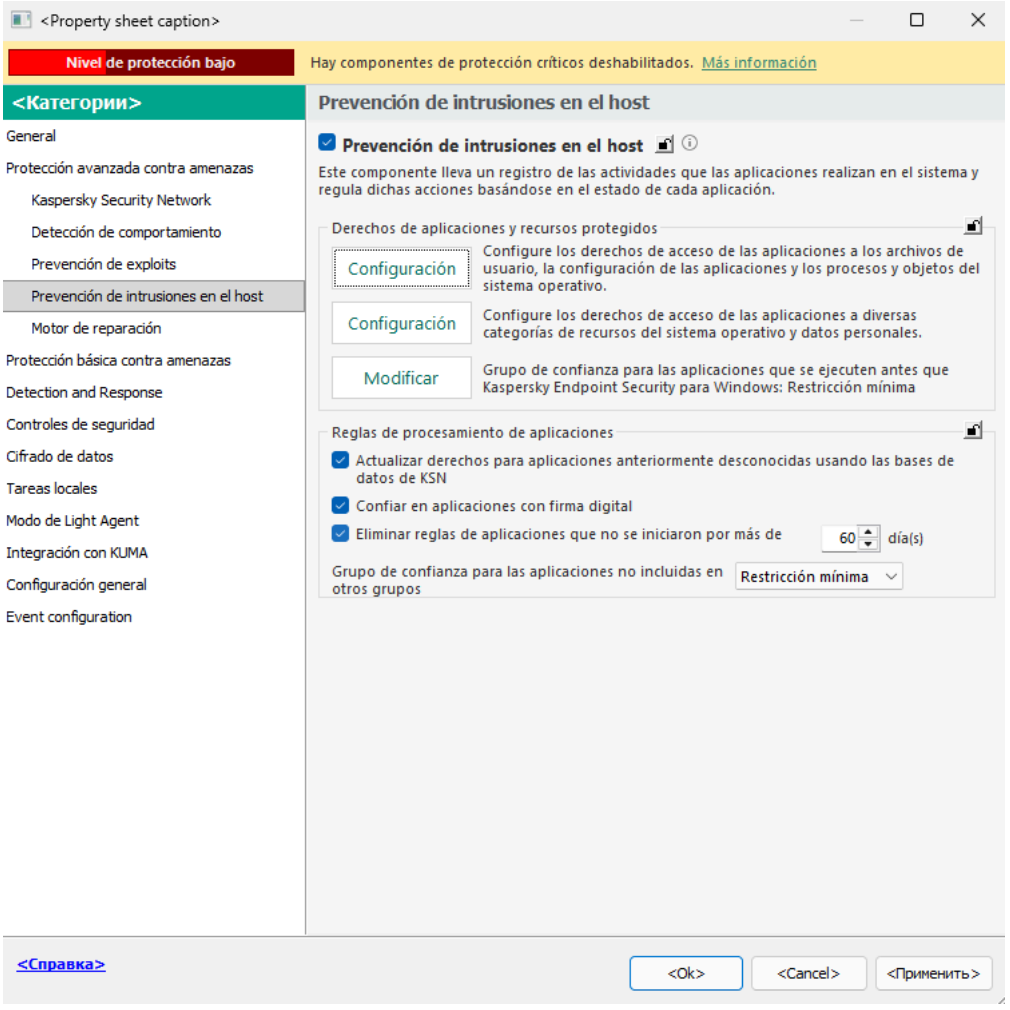
Cuando inicie una aplicación cuya información se haya eliminado, Kaspersky Endpoint Security la analizará como si fuera la primera vez que se la ejecuta.

Cómo configurar la eliminación automática de información vinculada a aplicaciones en desuso 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.



Configuración de Prevención de intrusiones

4. En el bloque **Reglas de procesamiento de aplicaciones**, realice una de las siguientes acciones:

   - Si desea configurar la eliminación automática, seleccione la casilla **Eliminar reglas de aplicaciones que no se iniciaron por más de N día(s)** e ingrese el número de días.

     Transcurrido el número de días que especifique, Kaspersky Endpoint Security eliminará la información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente. La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado automáticamente se eliminará luego de treinta días.

   - Si desea desactivar la eliminación automática, cancele la selección de la casilla **Eliminar reglas de aplicaciones que no se iniciaron por más de N día(s)**.

     La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente se conservará por tiempo indefinido (es decir, el plazo de almacenamiento será ilimitado). Kaspersky Endpoint Security únicamente eliminará (luego de treinta días) la información de las aplicaciones cuyo grupo de confianza o cuyos derechos se hayan determinado automáticamente.

5. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar la eliminación automática de información vinculada a aplicaciones en desuso 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de intrusiones en el host**.

5. En el bloque **Reglas de procesamiento de aplicaciones**, realice una de las siguientes acciones:

   - Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas de aplicaciones que no se iniciaron por más de (días, entre 1 y 90)** e ingrese el número de días.

     Transcurrido el número de días que especifique, Kaspersky Endpoint Security eliminará la información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente. La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado automáticamente se eliminará luego de treinta días.

   - Si desea desactivar la eliminación automática, anule la selección de la casilla de verificación **Eliminar reglas de aplicaciones que no se iniciaron por más de (días, entre 1 y 90)**.

     La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente se conservará por tiempo indefinido (es decir, el plazo de almacenamiento será ilimitado). Kaspersky Endpoint Security únicamente eliminará (luego de treinta días) la información de las aplicaciones cuyo grupo de confianza o cuyos derechos se hayan determinado automáticamente.

6. Guarde los cambios.

Cómo configurar la eliminación automática de información vinculada a aplicaciones en desuso mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.

3. En el bloque **Reglas de procesamiento de aplicaciones**, realice una de las siguientes acciones:

- Si desea configurar la eliminación automática, seleccione la casilla **Eliminar reglas de aplicaciones que no se iniciaron por más de N días (entre 1 y 90)** e ingrese el número de días.

  Transcurrido el número de días que especifique, Kaspersky Endpoint Security eliminará la información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente. La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado automáticamente se eliminará luego de treinta días.

- Si desea desactivar la eliminación automática, cancele la selección de la casilla **Eliminar reglas de aplicaciones que no se iniciaron por más de N días (entre 1 y 90)**.

  La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente se conservará por tiempo indefinido (es decir, el plazo de almacenamiento será ilimitado). Kaspersky Endpoint Security únicamente eliminará (luego de treinta días) la información de las aplicaciones cuyo grupo de confianza o cuyos derechos se hayan determinado automáticamente.

4. Guarde los cambios.

Monitoreo de Prevención de intrusiones en el host

La aplicación puede generar informes sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

Si desea monitorear las operaciones de Prevención de intrusiones en el host, active la creación de informes. Por ejemplo, puede habilitar el reenvío de los informes generados para aplicaciones específicas en la configuración del componente Prevención de intrusiones en el host.

A la hora de configurar el monitoreo, tenga en cuenta que reenviar eventos a Kaspersky Security Center significará más tráfico en la red. Si lo desea, puede optar por guardar los informes únicamente en el registro local de Kaspersky Endpoint Security.

Protección del acceso a dispositivos de audio y video

La funcionalidad de protección de la señal de audio y la funcionalidad de protección del acceso a la cámara web no son compatibles con los equipos basados en Arm.

Existen programas especiales que pueden darle a un atacante la capacidad de acceder a los dispositivos de grabación de audio y video de un equipo (por ejemplo, a los micrófonos y las cámaras web).
Kaspersky Endpoint Security puede detectar si una aplicación está recibiendo una señal de audio o de video y proteger esa información si la aplicación no está autorizada a captarla.

De forma predeterminada, Kaspersky Endpoint Security permite que solo las aplicaciones del grupo *De confianza* reciban transmisiones de audio y video. Las aplicaciones de los grupos *Restricción mínima*, *Restricción máxima* y *No confiables* no pueden recibir transmisiones de audio ni de video de los dispositivos. Si necesita que una aplicación específica reciba una señal de audio o de video, puede brindarle acceso manualmente.

Particularidades de la protección de audio

La protección de audio tiene las siguientes particularidades:

- Para que la característica funcione, el componente Prevención de intrusiones en el host debe estar habilitado.
- Si la aplicación comenzó a recibir la transmisión de audio antes de que se iniciara el componente Prevención de intrusiones en el host, Kaspersky Endpoint Security permitirá que la aplicación reciba la transmisión de audio y no mostrará ninguna notificación.
- Si movió la aplicación al grupo *No confiables* o al grupo *Restricción máxima* luego de que la aplicación comenzara a recibir la transmisión de audio, Kaspersky Endpoint Security permitirá que la aplicación reciba la transmisión de audio y no mostrará ninguna notificación.
- Si modifica los ajustes que rigen el acceso de una aplicación a los dispositivos de grabación de audio (por ejemplo, si prohíbe que la aplicación acceda a la señal de audio), deberá reiniciar dicha aplicación para que esta deje de tener acceso a la señal de audio.
- El control de acceso a la señal de audio de los dispositivos de grabación de sonidos no depende del acceso de una aplicación a la cámara web.
- Kaspersky Endpoint Security protege el acceso solo a micrófonos incorporados y micrófonos externos. Los demás dispositivos de grabación de audio no son compatibles.
- Kaspersky Endpoint Security no puede garantizar la protección de una transmisión de audio desde dispositivos como cámaras DSLR, videocámaras portátiles y cámaras de acción.
- Cuando ejecute aplicaciones de grabación o reproducción de audio y video por primera vez después de instalar Kaspersky Endpoint Security, es posible que se interrumpa la grabación o reproducción de audio y video. Esto es necesario a fin de habilitar la funcionalidad que controla el acceso de las aplicaciones a dispositivos para grabar audio. El servicio del sistema que controla el hardware de audio se reiniciará cuando se ejecute Kaspersky Endpoint Security por primera vez.

Particularidades de la protección de acceso a la cámara web

La funcionalidad de protección de acceso a cámaras web tiene las siguientes consideraciones especiales y limitaciones:

- La aplicación controla video e imágenes fijas derivadas del procesamiento de datos de una cámara web.
- La aplicación controla la transmisión de audio si forma parte de la transmisión de video recibida de la cámara web.
- La aplicación controla solamente las cámaras web conectadas por medio de USB o IEEE1394 que se indican como Dispositivos de imagen en el Administrador de 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 BadUSB

Algunos virus modifican el firmware de los dispositivos USB para hacer que el sistema operativo considere que el dispositivo USB es un teclado. De esta manera, el virus puede ejecutar comandos en su cuenta de usuario para descargar malware, por ejemplo.

El componente Prevención de ataques BadUSB impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo.

Cuando un dispositivo USB se conecta a un equipo y el sistema operativo lo identifica como un teclado, la aplicación le solicita al usuario que ingrese un código numérico generado por la aplicación desde ese teclado o con un Teclado en pantalla, si está disponible (vea la siguiente imagen). Este procedimiento se conoce como autorización del teclado.

Si el código se ingresa correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al que se conectó) en la lista de teclados autorizados. No es necesario repetir la autorización del teclado cuando el teclado vuelve a conectarse o después del reinicio del sistema operativo.

> Si el teclado autorizado se conecta a otro puerto USB del equipo, la aplicación mostrará otra vez una solicitud de autorización para este teclado.

Si se ha ingresado incorrectamente el código numérico, la aplicación genera un nuevo código. Puede configurar el número de intentos ingresando el código numérico. Si el código numérico se ingresa incorrectamente varias veces o se cierra la ventana de autorización del teclado (vea la siguiente imagen), la aplicación bloquea la entrada desde este teclado. Cuando transcurre el tiempo de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación le solicita al usuario que lleve a cabo nuevamente la autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea un teclado que no haya sido autorizado.

El componente Prevención de ataques BadUSB no se instala por defecto. Si desea utilizarlo, agréguelo en las propiedades del paquete de instalación antes de instalar la aplicación. Si la aplicación ya está instalada, modifique la selección de componentes disponibles.

Autorización del teclado

Habilitación y deshabilitación de Prevención de ataques BadUSB

Los dispositivos USB identificados por el sistema operativo como teclados y conectados al equipo antes de la instalación del componente de Prevención de ataques BadUSB se consideran autorizados después de la instalación del componente.

Cómo habilitar o deshabilitar el componente Prevención de ataques 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.
4. Utilice la casilla **Prevención de ataques BadUSB** para habilitar o deshabilitar el componente.

5. En el bloque **Autorización del dispositivo USB al conectarlo**, ajuste la configuración de seguridad para ingresar el código de autorización:

   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para ingresar el código de autorización, la aplicación bloquea el dispositivo USB después del quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, volverá a tener 5 intentos para ingresar el código de autorización.

   - **Tiempo de espera al alcanzar el número máximo de intentos (minutos)**. Duración del bloqueo del dispositivo USB después de la cantidad especificada de intentos fallidos de ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

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

Cómo habilitar o deshabilitar el componente Prevención de ataques 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de ataques BadUSB**.

5. Use el interruptor **Prevención de ataques BadUSB HABILITADA** para habilitar o deshabilitar el componente.

6. En el bloque **Autorización de dispositivos USB**, ajuste la configuración de seguridad para ingresar el código de autorización:

   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para ingresar el código de autorización, la aplicación bloquea el dispositivo USB después del quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, volverá a tener 5 intentos para ingresar el código de autorización.

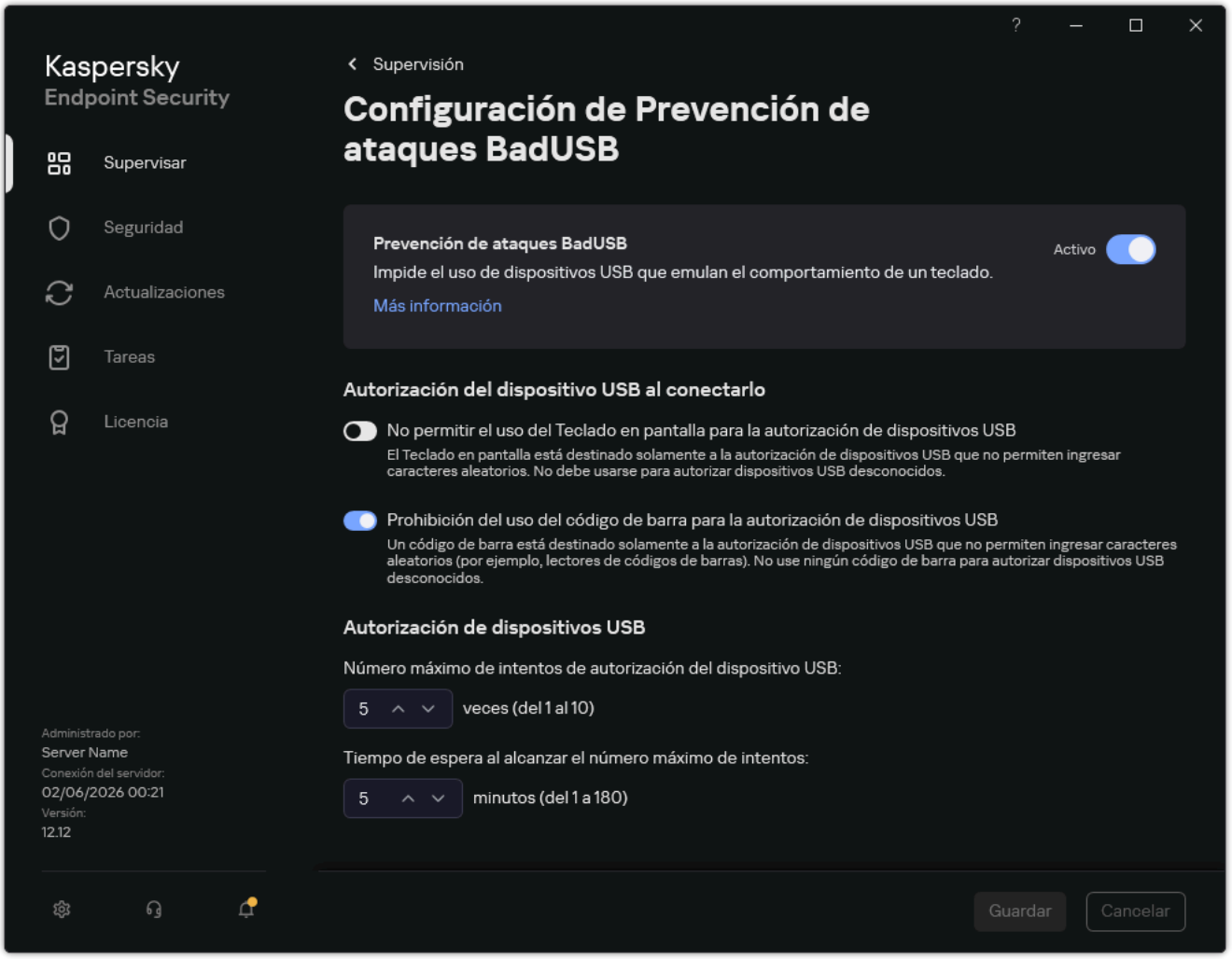
   - **Tiempo de espera cuando se alcanza la cantidad máxima de intentos (min)**. Duración del bloqueo del dispositivo USB después de la cantidad especificada de intentos fallidos de ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

7. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Prevención de ataques BadUSB en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.



Configuración del componente Prevención de ataques BadUSB

3. Use el interruptor **Prevención de ataques BadUSB** para habilitar o deshabilitar el componente.

4. En el bloque **Autorización del dispositivo USB al conectarlo**, ajuste la configuración de seguridad para ingresar el código de autorización:

   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para ingresar el código de autorización, la aplicación bloquea el dispositivo USB después del quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, volverá a tener 5 intentos para ingresar el código de autorización.

   - **Tiempo de espera al alcanzar el número máximo de intentos**. Duración del bloqueo del dispositivo USB después de la cantidad especificada de intentos fallidos de ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

5. Guarde los cambios.

De esta manera, si Prevención de ataques BadUSB está habilitado, 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 lo autorice.

Usar el Teclado en pantalla para la autorización de dispositivos USB

El teclado en pantalla debería usarse únicamente para autorizar dispositivos USB que no sean compatibles con la entrada de caracteres aleatorios (p. ej., lectores de códigos de barras). No se recomienda el uso del 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.
4. Use la casilla **No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB** para 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

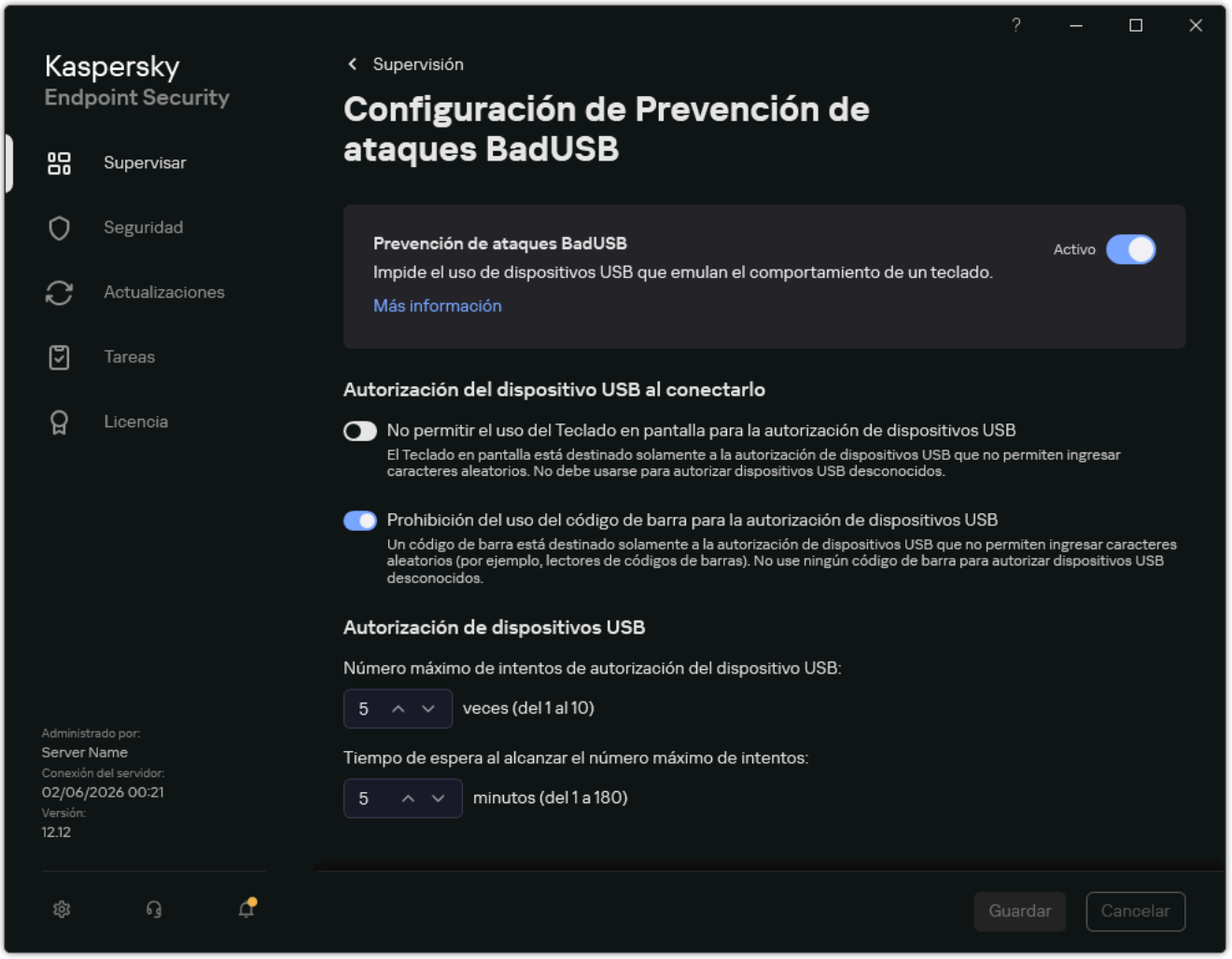
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Prevención de ataques BadUSB**.
5. Use el interruptor **Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB** para permitir 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 principal de la aplicación haga clic en el botón ⚙.

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.



Configuración del componente Prevención de ataques BadUSB

3. Use el interruptor **No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB** para permitir o bloquear el uso del teclado en pantalla para la autorización.

4. Guarde los cambios.

Autorización de dispositivos USB

Autorización del lector de códigos de barras

Al conectar al equipo un lector de códigos de barras, el componente Prevención de ataques BadUSB identifica este dispositivo como un dispositivo de entrada y le solicita que realice la autorización. Para autorizar el lector de códigos de barras, debe analizar el código de barras que se muestra en la pantalla. La aplicación genera un código de barras con el formato Code39 compatible con la mayoría de los lectores de códigos de barras y QR.

Kaspersky Endpoint Security también es compatible con otro método de autorización de lectores de códigos de barras. Si usa dispositivos con pantalla táctil, puede usar un teclado en pantalla para escribir un código. Para ello, necesita habilitar el teclado en pantalla. Este método es conveniente, por ejemplo, cuando se usan lectores de códigos de barras fijos e incorporados a cajas registradoras. Los demás métodos de autorización de lectores de códigos de barras están prohibidos.

De forma predeterminada, la aplicación no utiliza un código de barras para autorizar dispositivos USB.

Cómo habilitar la autorización de dispositivos USB mediante un 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

4. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.

5. Use la casilla **No permitir el uso de un código de barra para la autorización de dispositivos USB** para permitir o bloquear el uso de códigos de barras para la autorización.

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

Cómo habilitar la autorización de dispositivos USB mediante un código de barras 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Prevención de ataques BadUSB**.

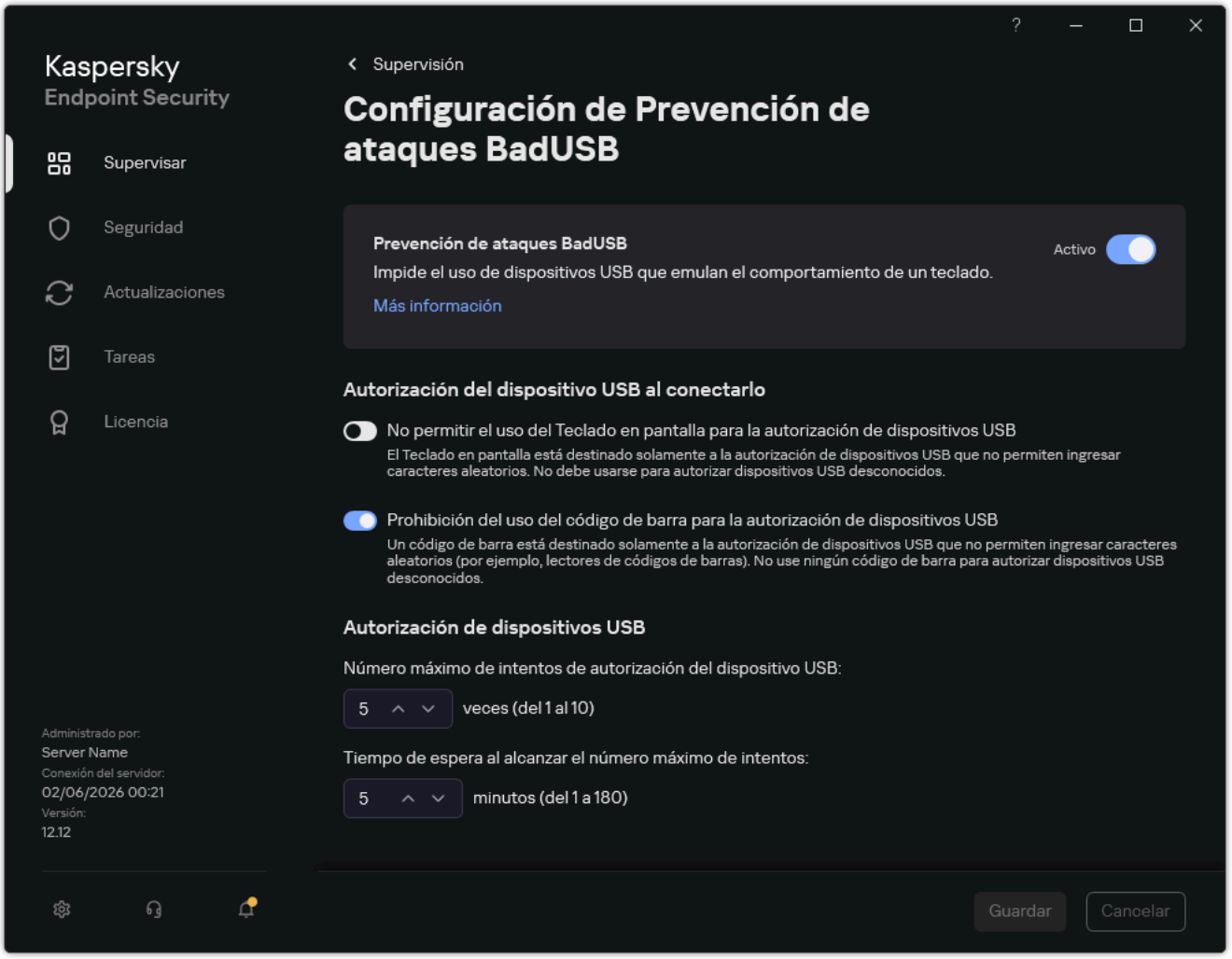
5. Use el interruptor **Prohibición del uso del código de barra para la autorización de dispositivos USB** para permitir o bloquear el uso de códigos de barras para la autorización.

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

Cómo habilitar la autorización de dispositivos USB mediante un código de barras en la interfaz de la aplicación

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

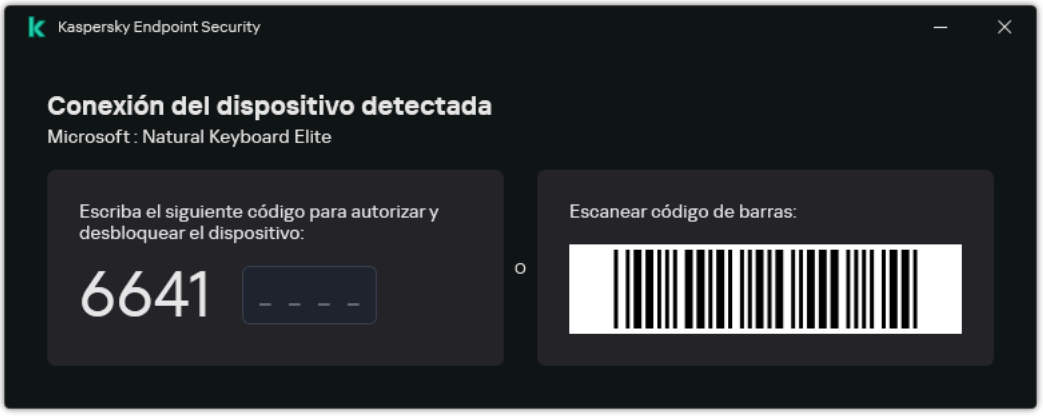
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.



Configuración del componente Prevención de ataques BadUSB

3. Use el interruptor **Prohibición del uso del código de barra para la autorización de dispositivos USB** para permitir o bloquear el uso de códigos de barras para la autorización.

4. Guarde los cambios.

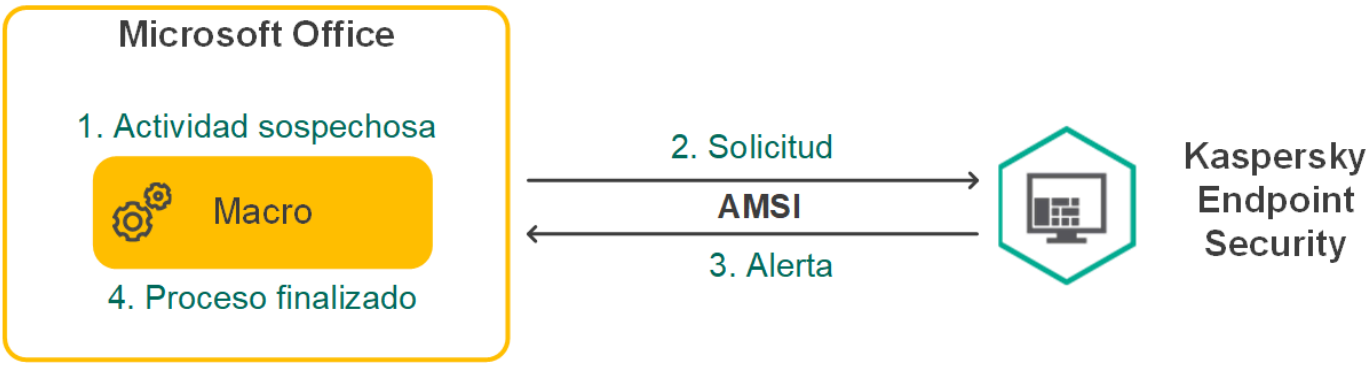


Autorización del lector de códigos de barras

Protección vía AMSI

El componente Protección vía AMSI está diseñado para admitir la Antimalware Scan Interface de Microsoft. La *interfaz de análisis antimalware AMSI* permite que las aplicaciones de terceros envíen a Kaspersky Endpoint Security aquellos objetos que precisan analizar (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 obtener más detalles sobre AMSI, consulte la documentación de Microsoft.

La Protección vía AMSI únicamente puede detectar amenazas y notificárselo a la aplicación. La aplicación de terceros después de recibir una notificación de una amenaza no le permite realizar acciones maliciosas (por ejemplo, la finaliza la acción).



Ejemplo del funcionamiento de AMSI

El componente Protección vía AMSI puede rechazar una solicitud de una aplicación de terceros, por ejemplo, si esta aplicación excede 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 vía AMSI no rechaza las solicitudes de aquellas aplicaciones de terceros para las cuales la integración continua con el componente de protección vía AMSI está habilitado.

La Protección vía 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
- Windows Server 2016 Essentials/Standard/Datacenter (se incluye el modo Server Core)
- Windows Server 2019 Essentials/Standard/Datacenter (se incluye el modo Server Core)
- Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition (se incluye modo Server Core)
- Windows Server 2025 Standard / Datacenter.

Habilitación y deshabilitación de la Protección vía AMSI

De forma predeterminada, la Protección vía AMSI está habilitada y funciona en el modo que recomienda Kaspersky (consulte la tabla a continuación).

Cómo habilitar o deshabilitar la Protección vía 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Escáner AMSI**.
4. Utilice la casilla **Escáner AMSI** para habilitar o deshabilitar el componente.
5. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

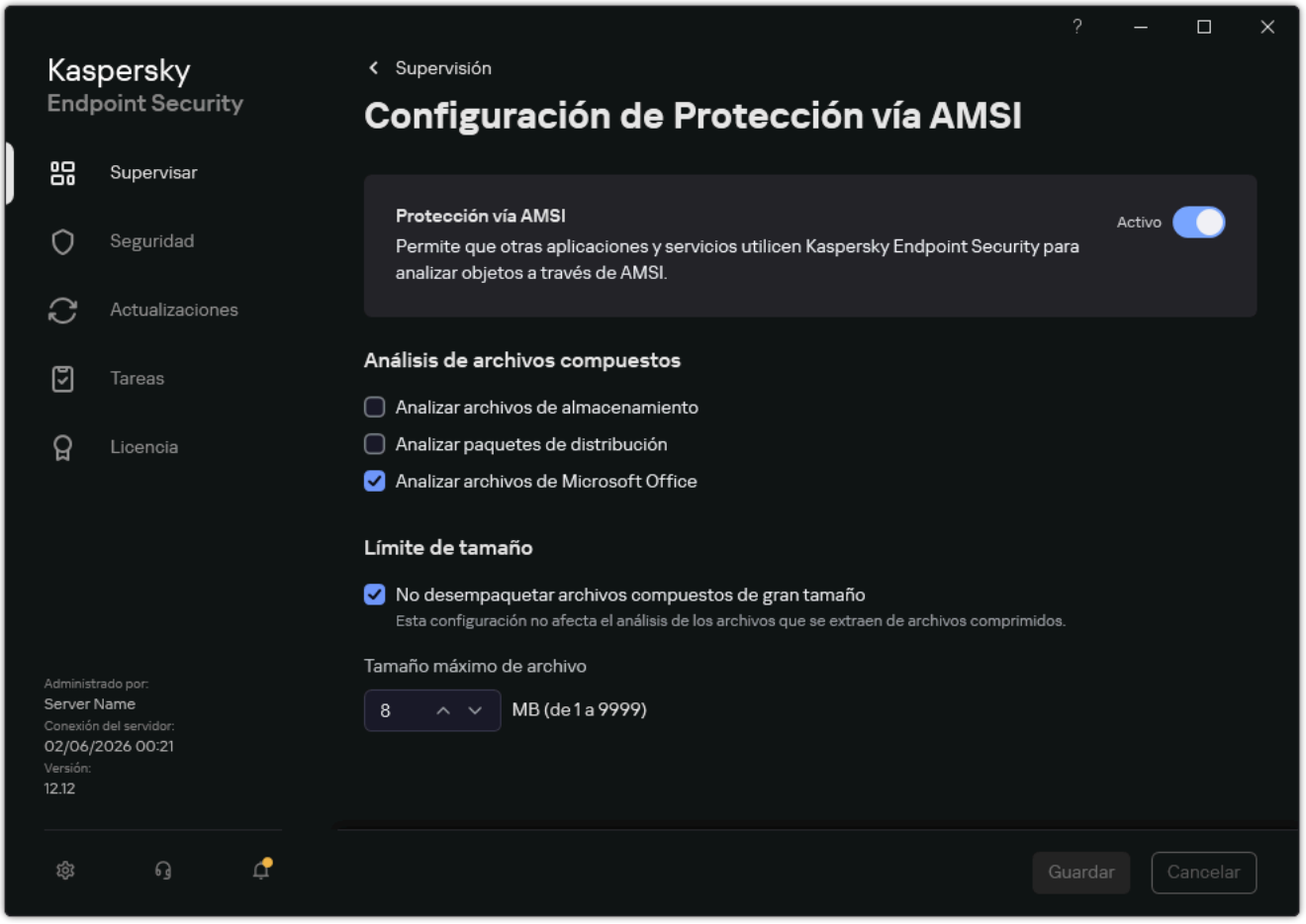
Cómo habilitar o deshabilitar la Protección vía AMSI en Web Console y Cloud Console

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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Protección vía AMSI**.
5. Use el interruptor **Protección vía AMSI HABILITADA** para habilitar o deshabilitar el componente.
6. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo habilitar o deshabilitar la Protección vía AMSI en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección vía AMSI**.



Configuración de Protección vía AMSI

3. Use el interruptor **Protección vía AMSI** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

Configuración de la Protección vía AMSI que recomiendan los expertos de Kaspersky

Parámetro	Valor	Descripción
Analizar archivos de almacenamiento	**Inactivo**	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar paquetes de distribución	**Inactivo**	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos de Microsoft Office	**Activo**	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.
No desempaquetar archivos compuestos de gran tamaño	**Tamaño máximo de archivo** **8 MB**	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada o no.

Optimización del análisis de archivos mediante la Protección vía AMSI

Puede optimizar el análisis de archivos: reducir la duración del análisis y aumentar la velocidad operativa de Kaspersky Endpoint Security. Puede seleccionar los archivos compuestos que deben analizarse: archivos comprimidos, paquetes de distribución o archivos en formatos de oficina. También puede limitar el tamaño de los archivos compuestos que se analizarán. El componente Protección vía 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 u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

Cómo optimizar el análisis de archivos con Protección vía 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Escáner AMSI**.

4. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.

5. En el bloque **Límite de tamaño**, realice una de las siguientes acciones:

   - Para que el componente Protección vía AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos grandes** e ingrese el valor que considere apropiado. El componente Protección vía AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

   - Para permitir que el componente Protección vía AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **No desempaquetar archivos compuestos grandes**.

   El componente Protección vía AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

6. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo optimizar un análisis de archivos con Protección vía 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Protección vía AMSI**.

5. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.

6. En el bloque **Optimización de análisis**, realice una de las siguientes acciones:

   - Para que el componente Protección vía AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **Límites de tamaño habilitados** e ingrese el valor que considere apropiado. El componente Protección vía AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

   - Para permitir que el componente Protección vía AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **Límites de tamaño habilitados**.

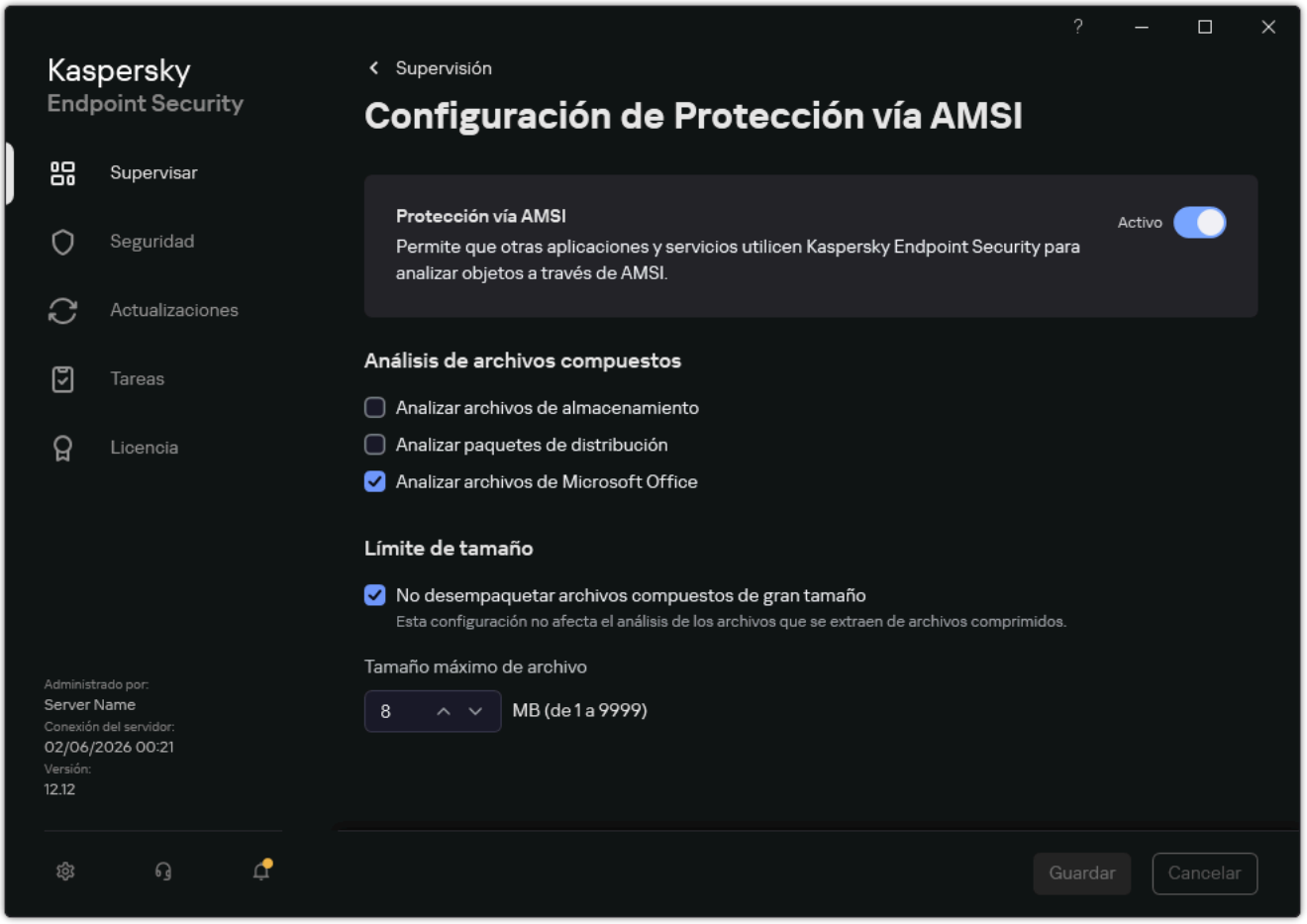
   El componente Protección vía AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **Límites de tamaño habilitados** está seleccionada.

7. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados 🔒.

Cómo optimizar el análisis de archivos con Protección vía AMSI en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección vía AMSI**.



Configuración de Protección vía AMSI

3. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.

4. En el bloque **Límite de tamaño**, realice una de las siguientes acciones:

   - Para que el componente Protección vía AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos de gran tamaño** e ingrese el valor que considere apropiado. El componente Protección vía AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

   - Para permitir que el componente Protección vía AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **No desempaquetar archivos compuestos de gran tamaño**.

   El componente Protección vía AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No desempaquetar archivos compuestos de gran tamaño** está seleccionada.

5. Guarde los cambios.

Protección contra amenazas web

El componente Protección contra amenazas web está diseñado para bloquear sitios web maliciosos y fraudulentos e impedir la descarga de archivos dañinos de Internet. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Kaspersky Endpoint Security analiza tráfico HTTP, HTTPS y FTP. La aplicación analiza tanto direcciones URL como direcciones IP.

Para usar la Protección contra amenazas web, debe completar la configuración inicial de la aplicación:

- Para que la aplicación pueda supervisar el tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitada de manera predeterminada).

- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación controla todos).

- Seleccione las aplicaciones cuyo tráfico desee que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya figuran en la lista de aplicaciones que recomienda Kaspersky. Si el navegador que utiliza no está en la lista, agréguelo.

- Recomendamos inyectar un script de interacción de página web en el tráfico web (la inyección de script está deshabilitada de forma predeterminada). Esta secuencia de comandos permite el registro de eventos de Protección contra amenazas web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Cuando un usuario intente abrir un sitio web malicioso o fraudulento, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia.

Habilitación y deshabilitación de la Protección contra amenazas web

De manera predeterminada, el componente Protección contra amenazas web está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para la Protección contra amenazas web, la aplicación puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que el nivel de seguridad de tráfico web **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky (vea la tabla a continuación). Puede seleccionar uno de los niveles preinstalados de seguridad para el tráfico web que se recibe o se transmite mediante los protocolos HTTP y FTP, o configurar un nivel de seguridad personalizado para el tráfico web. Si modifica la configuración del nivel de seguridad del tráfico web, siempre puede volver a la configuración recomendada del nivel de seguridad 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 habilitar o deshabilitar el componente Protección contra 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.
4. Utilice la casilla **Protección contra amenazas web** para habilitar o deshabilitar el componente.
5. Si habilitó el componente, realice una de estas 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 con el cual el componente Protección contra amenazas web realiza el análisis máximo del tráfico web que recibe el equipo a través de los protocolos HTTP y FTP. El componente Protección contra amenazas web analiza en detalle todos los objetos de tráfico web mediante el uso de todas las bases de datos de la aplicación y realiza el análisis heurístico más avanzado posible.
     - **Recomendado**. Este es el nivel de seguridad que proporciona el equilibrio óptimo entre el rendimiento de la aplicación y la seguridad del tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de 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 asegura la máxima velocidad de análisis de tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de análisis superficial.

- Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración** y configure los ajustes del componente.

  Para restaurar los valores de los niveles de seguridad preestablecidos, haga clic en el botón **Predeterminado**.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos de tráfico web malicioso:

   - **Bloquear**. Cuando 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**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web permite que el objeto se descargue al equipo, pero agrega información sobre el mismo a la lista de amenazas activas.

7. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Protección contra amenazas 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas web**.

5. Use el interruptor **Protección contra amenazas web HABILITADA** para habilitar o deshabilitar el componente.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos de tráfico web malicioso:

   - **Bloquear**. Cuando 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 sistema operativo)**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web permite que el objeto se descargue al equipo, pero agrega información sobre el mismo a la lista de amenazas activas.

7. Si es necesario, haga una lista de direcciones web de confianza.

8. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Protección contra amenazas web

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.

3. Use el interruptor **Protección contra amenazas web** para habilitar o deshabilitar el componente.

4. Si habilitó el componente, realice una de estas 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 con el cual el componente Protección contra amenazas web realiza el análisis máximo del tráfico web que recibe el equipo a través de los protocolos HTTP y FTP. El componente Protección contra amenazas web analiza en detalle todos los objetos de tráfico web mediante el uso de todas las bases de datos de la aplicación y realiza el análisis heurístico más avanzado posible.

     - **Recomendado**. Este es el nivel de seguridad que proporciona el equilibrio óptimo entre el rendimiento de la aplicación y la seguridad del tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de 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 asegura la máxima velocidad de análisis de tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de análisis superficial.

   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina la configuración del componente.

     Para restaurar los valores de los niveles de seguridad preestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado**.

5. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos de tráfico web malicioso:

   - **Bloquear**. Cuando 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**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web permite que el objeto se descargue al equipo, pero agrega información sobre el mismo a la lista de amenazas activas.

6. Guarde los cambios.

Configuración de Protección contra amenazas web recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
Comprobar si la dirección web está en la base de datos de direcciones web maliciosas	**Activo**	Analizar los vínculos para determinar si están incluidos en la base de datos de direcciones web malintencionadas le permite rastrear sitios web que estén en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web malintencionadas, la que se incluye en el paquete de instalación de la aplicación y se actualiza durante las actualizaciones de las bases de datos de Kaspersky Endpoint Security.
Comprobar si la dirección web está en la base de datos de direcciones web fraudulentas	**Activo**	La base de datos de direcciones web fraudulentas incluye las direcciones web de los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases de datos de Kaspersky Endpoint Security.
Usar análisis heurístico (Protección contra amenazas web)	**Análisis medio**	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

Parámetro	Valor	Descripción
Usar análisis heurístico (Antiphishing)	**Activo**	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.
Acción al detectar una amenaza	**Bloquear**	Cuando 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 contra 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 con la base de datos de direcciones maliciosas

Analizar los vínculos para determinar si están incluidos en la base de datos de direcciones web malintencionadas le permite rastrear sitios web que estén en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web malintencionadas, la que se incluye en el paquete de instalación de la aplicación y se actualiza durante las actualizaciones de las bases de datos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security analiza todos los vínculos para determinar si están incluidos en bases de datos de direcciones web malintencionadas. La configuración de análisis de conexión segura de la aplicación no afecta la funcionalidad de análisis de vínculos. En otras palabras, si el análisis de conexiones cifradas está deshabilitado, Kaspersky Endpoint Security verifica los vínculos con bases de datos de direcciones web maliciosas, incluso si el tráfico de red se transmite a través de una conexión cifrada.

Cómo habilitar o deshabilitar la verificación para comprobar si las direcciones web están la base de datos de direcciones web maliciosas con la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra 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 anule la selección de la casilla **Comprobar si la dirección web está en la base de datos de direcciones web maliciosas** para habilitar o deshabilitar la verificación de direcciones con la base de datos de direcciones web maliciosas.

6. Guarde los cambios.

Cómo habilitar o deshabilitar la verificación para comprobar si las direcciones web están la base de datos de direcciones web maliciosas en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Métodos de análisis**, seleccione o anule la selección de la casilla **Comprobar si la dirección web está en la base de datos de direcciones web maliciosas** para habilitar o deshabilitar la verificación 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 del sistema operativo. El análisis heurístico puede detectar amenazas sobre las cuales no existen registros 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 sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

Cómo habilitar o deshabilitar el uso de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra 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 **Utilizar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar el tráfico web en busca de virus y otro malware.

6. A continuación, use el control deslizante para elegir un nivel de análisis: **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 sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

7. Guarde los cambios.

Cómo habilitar o deshabilitar el uso de análisis heurístico en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra 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 otro malware.

   Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

5. Guarde los cambios.

Anti-Phishing

Protección contra amenazas web comprueba los vínculos para ver si pertenecen a direcciones web de suplantación de identidad (phishing). Esto ayuda a evitar *ataques de suplantación de identidad (phishing)*. Un ataque de phishing puede imitar, por ejemplo, un mensaje de correo electrónico supuestamente enviado por su banco, con un vínculo al sitio web oficial del banco. Cuando hace clic en el vínculo, se abre una copia exacta del sitio web del banco e, incluso, puede ver la dirección web real en el navegador, a pesar de que se trata de una imitación. A partir de ese momento, se hace un seguimiento de todas sus acciones dentro del sitio y pueden ser usadas para robar su dinero.

Teniendo en cuenta que los vínculos a los sitios web fraudulentos no solo pueden recibirse en mensajes de correo electrónico, sino también por otros medios, como programas de mensajería, el componente Protección contra amenazas web supervisa los intentos de acceder a un sitio web fraudulento en el nivel de análisis del tráfico web y bloquea el acceso a dichos sitios. Las listas de direcciones web de phishing se incluyen en el kit de distribución de Kaspersky Endpoint Security.

Puede configurar Antiphishing solo en la Consola de administración (MMC) o en la interfaz local de la aplicación. No puede configurar Antiphishing en Web Console o Cloud Console. De forma predeterminada, Antiphishing con análisis heurístico está habilitado.

Cómo habilitar o deshabilitar la tecnología de Antiphishing 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra 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 **Configuración de Anti-Phishing**, seleccione o borre la casilla de verificación **Comprobar si la dirección web está en la base de datos de direcciones web fraudulentas** para habilitar o deshabilitar Antiphishing.

   La base de datos de direcciones web fraudulentas incluye las direcciones web de los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases de datos de Kaspersky Endpoint Security.

6. Seleccione la casilla **Utilizar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar páginas web en busca de vínculos fraudulentos.

   Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones del sistema operativo. El análisis heurístico puede detectar amenazas sobre las cuales no existen registros en las bases de datos de Kaspersky Endpoint Security.

   Para analizar vínculos, además de la base de datos antivirus y el análisis heurístico, puede usar bases de datos de reputación de Kaspersky Security Network.

7. Guarde los cambios.

Cómo habilitar o deshabilitar Antiphishing en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.

3. Haga clic en **Configuración avanzada**.

4. Si desea que el componente Protección contra amenazas web compruebe los vínculos con las bases de datos de direcciones web de phishing, seleccione la casilla **Comprobar si la dirección web está en la base de datos de direcciones web fraudulentas** en el bloque **Antiphishing**. La base de datos de direcciones web fraudulentas incluye las direcciones web de los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases 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 vínculos fraudulentos.

   Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones del sistema operativo. El análisis heurístico puede detectar amenazas sobre las cuales no existen registros en las bases de datos de Kaspersky Endpoint Security.

Para analizar vínculos, además de la base de datos antivirus y el análisis heurístico, puede usar bases de datos de reputación de Kaspersky Security Network.

6. Guarde los cambios.

Creación de la lista de direcciones web de confianza

Además de los sitios web fraudulentos y maliciosos, Protección contra amenazas web puede bloquear otros sitios web. Por ejemplo, Protección contra amenazas web bloquea el tráfico HTTP que no cumple con los estándares RFC. Puede crear una lista de direcciones URL cuyo contenido considera confiable. El componente Protección contra amenazas web no analiza la información de direcciones web de confianza en busca de virus u otras amenazas. Esta opción es útil, por ejemplo, cuando el componente Protección contra 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 específica o la dirección de un sitio web.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de direcciones web de confianza en una directiva. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Cómo agregar una dirección web de confianza con la Consola de administración (MMC)

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

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

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.

4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, seleccione la pestaña **Direcciones web de confianza**.

6. Seleccione la casilla de verificación **No analizar el tráfico web de las direcciones web de confianza**.

   Si se selecciona esta opción, el componente Protección contra amenazas web no analiza el contenido de las páginas o los sitios web cuyas direcciones están incluidas en la lista de direcciones web de confianza. Puede agregar a esta lista tanto direcciones específicas como máscaras de páginas o sitios web.

7. Cree una lista de direcciones URL o páginas web cuyo contenido considera confiable.

   Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara.

   También puede importar una lista de direcciones web de confianza desde un archivo XML.

8. Guarde los cambios.

Cómo agregar una dirección web de confianza con 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 ficha **Configuración de la aplicación**.
4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas web**.
5. Haga clic en **Direcciones web de confianza**.
6. Cree una lista de direcciones URL o páginas web cuyo contenido considera confiable.

   Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara.

   También puede importar una lista de direcciones web de confianza desde un archivo JSON.
7. Guarde los cambios.

Cómo agregar una dirección web de confianza en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.
3. Haga clic en **Configuración avanzada**.
4. Seleccione la casilla de verificación **No analizar tráfico web de direcciones URL de confianza**.

   Si se selecciona esta opción, el componente Protección contra amenazas web no analiza el contenido de las páginas o los sitios web cuyas direcciones están incluidas en la lista de direcciones web de confianza. Puede agregar a esta lista tanto direcciones específicas como máscaras de páginas o sitios web.
5. Cree una lista de direcciones URL o páginas web cuyo contenido considera confiable.

   Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara.

   También puede importar una lista de direcciones web de confianza desde un archivo XML.
6. Guarde los cambios.

Como resultado, Protección contra 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 agregar 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 contra amenazas web, Protección contra amenazas de correo y Control web están haciendo su trabajo.

Exportar e importar la lista de direcciones web de confianza

Puede exportar la lista de direcciones web de confianza a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una 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 otro servidor.

Cómo exportar e importar una lista de direcciones web de confianza a la Consola de administración (MMC)

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

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

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.

4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, seleccione la pestaña **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 vínculo **Exportar**.

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de direcciones web de confianza exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de direcciones web de confianza completa al archivo XML.

7. Para importar la lista de direcciones web de confianza:

   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de direcciones web de confianza.

   b. Abra el archivo.

      Cuando ya exista una lista de direcciones web de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

8. Guarde los cambios.

Cómo exportar e importar una lista de direcciones web de confianza a 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 ficha **Configuración de la aplicación**.
4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas web**.
5. Para exportar la lista de exclusiones al 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 la lista de exclusiones al bloque **Lista de reglas**, haga lo siguiente:

   a. Haga clic en el botón → **Importar**.

   En la ventana que se abre, seleccione el archivo JSON que se usará para importar la lista de direcciones web de confianza.

   b. Abra el archivo.

   Cuando ya exista una lista de direcciones web de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.
7. Guarde los cambios.

Protección contra amenazas de correo

El componente Protección contra amenazas de correo analiza los archivos adjuntos a los mensajes de correo entrantes y salientes para detectar virus y otras amenazas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

La Protección contra amenazas de 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 agregar el certificado de Kaspersky al almacén de certificados y seleccionar su almacén de certificados propios.

La Protección contra amenazas de correo no es compatible con otros protocolos y clientes de correo.

Es posible que la Protección contra amenazas de correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, la Protección contra amenazas de correo incluye una extensión para Microsoft Office Outlook. La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365. En equipos basados en Arm, la extensión de Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64.

Si utiliza un navegador para acceder a su cliente de correo electrónico, el componente Protección contra amenazas de correo no analizará sus mensajes.

Cuando se detecta un archivo malicioso en un archivo adjunto, Kaspersky Endpoint Security agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[El mensaje ha sido procesado] <asunto del mensaje>*.

Habilitación y deshabilitación de la Protección contra amenazas de correo

De manera predeterminada, el componente Protección contra amenazas de correo está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para la Protección contra amenazas de correo, la aplicación puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que el nivel de seguridad de correo **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky (vea la tabla a continuación). Puede seleccionar uno de los niveles preinstalados de seguridad del correo o configurar un nivel de seguridad personalizado del correo. Si ha cambiado la configuración del nivel de seguridad del correo, siempre puede volver a la configuración recomendada del nivel de seguridad del correo.

Si se está trabajando con el cliente de correo Mozilla Thunderbird, el componente Protección contra amenazas de correo no analiza mensajes que se transmiten mediante el protocolo IMAP en busca de virus y otras amenazas si se utilizan filtros para mover mensajes desde la carpeta Bandeja de entrada.

Cómo habilitar o deshabilitar el componente Protección contra amenazas de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

4. Utilice la casilla **Protección contra amenazas de correo** para habilitar o deshabilitar el componente.

5. Si habilitó el componente, realice una de estas acciones en el bloque **Nivel de seguridad**:

- Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:

  - **Alto**. Cuando este nivel de seguridad del correo electrónico se selecciona, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico más detalladamente. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico profundo. El nivel de seguridad de correo Alto se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo gratuito desde una red doméstica sin protección centralizada del correo.

  - **Recomendado**. Este es el nivel de seguridad del correo electrónico que proporciona el equilibrio óptimo entre el rendimiento de la aplicación y la seguridad del correo electrónico. El componente Protección contra amenazas de 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 del 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 contra amenazas de correo solo analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza los archivos adjuntos a los mensajes de correo electrónico. En este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico con una velocidad máxima y utiliza lo mínimo de los recursos del sistema operativo. Se recomienda utilizar el nivel de seguridad de correo Bajo en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una red LAN empresarial con protección de correo electrónico centralizada.

- Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración** y configure los ajustes del componente.

  Para restaurar los valores de los niveles de seguridad preestablecidos, haga clic en el botón **Predeterminado**.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos:

- **Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*.

- **Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. Si el objeto no puede desinfectarse, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

- **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar el componente Protección contra amenazas de correo 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de correo**.

5. Use el interruptor **Protección contra amenazas de correo HABILITADA** para habilitar o deshabilitar el componente.

6. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos:

   - **Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. Si el objeto no puede desinfectarse, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

   - **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

7. Si es necesario, modifique la configuración avanzada de Protección contra amenazas de correo.

8. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Protección contra amenazas de correo en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

3. Use el interruptor **Protección contra amenazas de correo** para habilitar o deshabilitar el componente.

4. Si habilitó el componente, realice una de estas acciones en el bloque **Nivel de seguridad**:

   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:

     - **Alto**. Cuando este nivel de seguridad del correo electrónico se selecciona, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico más detalladamente. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico profundo. El nivel de seguridad de correo Alto se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo gratuito desde una red doméstica sin protección centralizada del correo.

     - **Recomendado**. Este es el nivel de seguridad del correo electrónico que proporciona el equilibrio óptimo entre el rendimiento de la aplicación y la seguridad del correo electrónico. El componente Protección contra amenazas de 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 del 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 contra amenazas de correo solo analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza los archivos adjuntos a los mensajes de correo electrónico. En este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico con una velocidad máxima y utiliza lo mínimo de los recursos del sistema operativo. Se recomienda utilizar el nivel de seguridad de correo Bajo en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una red LAN empresarial con protección de correo electrónico centralizada.

   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina la configuración del componente.

     Para restaurar los valores de los niveles de seguridad preestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado**.

5. En el bloque **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos:

   - **Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. Si el objeto no puede desinfectarse, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

   - **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

6. Guarde los cambios.

Configuración de Protección contra amenazas de correo recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
Alcance de la protección	**Mensajes entrantes y salientes**	El *Alcance de la 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 el envío de archivos infectados. También puede activar el análisis de mensajes salientes si desea evitar el envío de archivos en formatos particulares, como archivos de audio y video, por ejemplo.
Conectar extensión de Microsoft Outlook	**Activo**	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 planea analizar el correo con la extensión para Microsoft Outlook, recomendamos que 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.
Analizar archivos de almacenamiento adjuntos	**Activo**	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar archivos adjuntos con formatos de Microsoft Office	**Activo**	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.
Filtro de datos adjuntos	**Cambiar el nombre de los archivos adjuntos de los tipos seleccionados**	Si selecciona esta opción, Protección contra amenazas de correo reemplazará el último carácter de extensión encontrado en los archivos adjuntos de los tipos especificados con el carácter de guion bajo (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.
Análisis heurístico	**Análisis medio**	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección**	Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*.

Modificación de la acción que se llevará a cabo en mensajes de correo electrónico infectados

Por defecto, el componente Protección contra amenazas de correo intenta desinfectar automáticamente todos los mensajes de correo infectados que se detectan. Si la desinfección produce un error, el componente Protección contra amenazas de correo elimina los mensajes de correo electrónico infectados.

Para modificar la acción que se llevará a cabo en mensajes de correo infectados:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

3. En el bloque **Acción al detectar una amenaza**, seleccione la acción que realizará Kaspersky Endpoint Security cuando se detecte un mensaje infectado:

   - **Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*.

   - **Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. Si el objeto no puede desinfectarse, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

   - **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

4. Guarde los cambios.

Formación del alcance de protección del componente Protección contra amenazas de correo

El *Alcance de la protección* hace referencia a los objetos que son analizados por el componente cuando está activo. Los alcances de la protección de diferentes componentes tienen diferentes propiedades. Las propiedades del alcance de la protección del componente Protección contra amenazas de correo incluyen la configuración para integrar el componente Protección contra amenazas de correo en clientes de correo y el tipo de mensajes de correo electrónico y los protocolos de correo electrónico cuyo tráfico es analizado por el componente Protección contra amenazas de correo. De forma predeterminada, Kaspersky Endpoint Security analiza tanto mensajes de correo electrónico como tráfico (entrantes y salientes) de los protocolos POP3, SMTP, NNTP e IMAP, y está integrado en el cliente de correo Microsoft Office Outlook.

Para formar el alcance de protección del componente Protección contra amenazas de correo, realice lo siguiente:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Alcance de la protección**, seleccione los mensajes que desea 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 el envío de archivos infectados. También puede activar el análisis de mensajes salientes si desea evitar el envío de archivos en formatos particulares, como archivos de audio y video, por ejemplo.

Si opta por analizar solo mensajes entrantes, le recomendamos que realice un análisis único de todos los mensajes salientes porque existe la posibilidad de que su equipo tenga gusanos de correo electrónico que se estén diseminando por correo electrónico. Esto ayuda a evitar problemas ocasionados por el envío masivo no controlado de mensajes infectados desde su equipo.

5. En el bloque **Conectividad**, realice lo siguiente:

   - Si desea que el componente Protección contra amenazas de correo analice los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que se reciban en el equipo del usuario, seleccione la casilla **Analizar el tráfico POP3, SMTP, NNTP e IMAP**.

     Si no desea que el componente Protección contra amenazas de correo analice los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen al equipo del usuario, desmarque la casilla **Analizar el tráfico POP3, SMTP, NNTP e IMAP**. En este caso, los mensajes son analizados por la extensión Protección contra amenazas de correo incorporada al cliente de correo de Microsoft Office Outlook después de que llegan al equipo del usuario si se selecciona la casilla **Conectar extensión de Microsoft Outlook**.

     Si usa un cliente de correo que no sea Microsoft Office Outlook, el componente Protección contra amenazas de correo no analiza los mensajes que se transmiten a través de los protocolos POP3, SMTP, NNTP e IMAP cuando la casilla **Analizar el tráfico POP3, SMTP, NNTP e IMAP** está desactivada.

   - Si desea permitir el acceso a la configuración del componente Protección contra amenazas de correo desde Microsoft Office Outlook y habilitar 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 **Conectar extensión de Microsoft Outlook**.

     Si desea bloquear el acceso a la configuración del componente Protección contra amenazas de correo desde Microsoft Office Outlook y deshabilitar 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, desmarque la casilla **Conectar extensión de Microsoft Outlook**.

     La extensión de la Protección contra amenazas de correo se incorpora al cliente de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

6. Guarde los cambios.

Análisis de archivos compuestos adjuntos a mensajes de correo electrónico

Puede habilitar o deshabilitar el análisis de adjuntos a mensajes, limitar el tamaño máximo de adjuntos a mensajes para analizar y limitar la duración máxima del análisis de adjuntos a mensajes.

Para configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Análisis de archivos compuestos**, ajuste la configuración del análisis:

   - **Analizar archivos adjuntos con formatos de Microsoft Office**. Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.

   - **Analizar archivos de almacenamiento adjuntos**. Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).

     Si, durante el análisis, la aplicación detecta una contraseña de un archivo de almacenamiento 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 guarda. Durante el análisis, el archivo de almacenamiento se descomprime. Si la aplicación genera un error durante el proceso de descompresión, puede eliminar manualmente los archivos descomprimidos que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tienen el prefijo PR.

   - **No analizar archivos de almacenamiento de más de N MB (de 1 a 9999)**. Si esta casilla está seleccionada, el componente Protección contra amenazas de correo excluye del análisis los archivos adjuntos en los mensajes de correo electrónico si el tamaño excede el valor especificado. Si se desactiva la casilla, el componente Protección contra amenazas de correo analiza los archivos adjuntos de correo de cualquier tamaño.

   - **Limitar el tiempo para analizar archivos a N s (de 1 a 9999)**. Si la casilla está seleccionada, el tiempo asignado al análisis de archivos adjuntos en los mensajes de correo se limita al período especificado.

5. Guarde los cambios.

Filtrado de datos adjuntos de mensajes de correo electrónico

El filtro de documentos adjuntos no se aplica a mensajes de correo electrónico salientes.

Las aplicaciones malintencionadas pueden propagarse por correo electrónico, en forma de archivos adjuntos. Puede configurar el filtrado según el tipo de adjuntos a mensajes de modo que los archivos de los tipos especificados se renombren o se eliminen automáticamente. Al cambiarles el nombre a los archivos adjuntos de cierta clase, Kaspersky Endpoint Security puede impedir la ejecución automática de aplicaciones malintencionadas.

Para configurar el filtrado de archivos adjuntos:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

3. Haga clic en **Configuración avanzada**.

4. En el bloque **Filtro de datos adjuntos**, realice una de las siguientes acciones:

   - **Deshabilitar el filtrado**. Si selecciona esta opción, el componente Protección contra amenazas de correo no filtrará los archivos adjuntos de los mensajes de correo electrónico.

   - **Cambiar el nombre de los archivos adjuntos de los tipos seleccionados**. Si selecciona esta opción, Protección contra amenazas de correo reemplazará el último carácter de extensión encontrado en los archivos adjuntos de los tipos especificados con el carácter de guion bajo (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.

   - **Eliminar archivos adjuntos de los tipos seleccionados**. Si selecciona esta opción, el componente Protección contra amenazas de correo eliminará de los mensajes de correo electrónico los tipos de archivos adjuntos que especifique.

5. Si seleccionó la opción **Cambiar el nombre de los archivos adjuntos de los tipos seleccionados** o la opción **Eliminar archivos adjuntos de los tipos seleccionados** en el paso anterior, seleccione las casillas que se encuentran frente a los tipos de archivos relevantes.

6. Guarde los cambios.

Exportar e importar extensiones para filtrado de datos adjuntos

Puede exportar la lista de extensiones de filtrado 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 otro servidor.

Cómo exportar e importar una lista de extensiones de filtrado de archivos adjuntos a 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de correo**.

5. Para exportar la lista de extensiones al bloque **Filtrado de datos adjuntos**:

   a. Seleccione las extensiones que desea exportar.

   b. Haga clic en el vínculo **Exportar**.

c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de extensiones. Seleccione también la carpeta en la que se guardará este archivo.

d. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de extensiones completa al archivo XML.

6. Para importar una lista de extensiones en el bloque **Filtrado de datos adjuntos**, haga lo siguiente:

a. Haga clic en el vínculo **Importar**.

b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de extensiones.

c. Abra el archivo.

Cuando ya exista una lista de extensiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.

4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, seleccione la pestaña **Filtrado de datos 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 vínculo **Exportar**.

c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de extensiones. Seleccione también la carpeta en la que se guardará este archivo.

d. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de extensiones completa al archivo XML.

7. Para importar la lista de extensiones:

a. Haga clic en el vínculo **Importar**.

b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de extensiones.

c. Abra el archivo.

Cuando ya exista una lista de extensiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

8. Guarde los cambios.

Análisis de correo electrónico en Microsoft Office Outlook

Durante la instalación de Kaspersky Endpoint Security, la extensión de la Protección contra amenazas de correo se incorpora a Microsoft Office Outlook (en adelante, Outlook). La extensión permite analizar mensajes en el nivel de cliente de correo en lugar de en el 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 realiza en el cliente de correo.

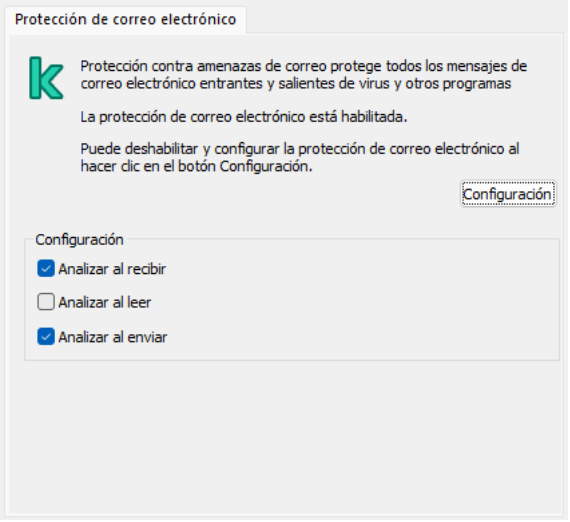
Puede abrir la configuración del componente Protección contra amenazas de correo desde Outlook y especificar en qué momento se deben analizar los mensajes de correo electrónico en busca de virus y otras amenazas.

La extensión Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365.

En equipos basados en Arm, la extensión de Protección contra amenazas de 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 son analizados primero por el componente Protección contra amenazas de correo (si se selecciona la casilla Analizar el tráfico POP3, SMTP, NNTP e IMAP en la interfaz de Kaspersky Endpoint Security) y, luego, por la extensión de Protección contra amenazas de correo para Outlook. Si el componente Protección contra amenazas de correo detecta un objeto malicioso en un mensaje, lo notifica sobre este evento.

Se puede establecer la configuración del componente Protección contra amenazas de correo directamente en Outlook si la extensión de Microsoft Outlook está conectada en la interfaz de Kaspersky Endpoint Security (consulte la figura a continuación).



Configuración del componente Protección contra amenazas de correo en Outlook

Los mensajes salientes son analizados primero por la extensión de la Protección contra amenazas de correo para Outlook y luego por el componente Protección contra amenazas de correo.

Si el correo se analiza usando la extensión de la Protección contra amenazas de correo para Outlook, se recomienda usar el Modo de intercambio en caché. Para información más detallada sobre el modo caché de Exchange y recomendaciones sobre su uso, consulte la Base de conocimientos de Microsoft.

Para configurar el modo de funcionamiento de la extensión de Protección contra amenazas de correo para Outlook:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.
4. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, en el bloque **Conectividad**, haga clic en el botón **Configuración**.
6. En la ventana **Protección de correo electrónico**, haga lo siguiente:
   - Seleccione la casilla **Analizar al recibir** si quiere que la extensión de Protección contra amenazas de correo para Outlook analice mensajes entrantes cuando llegan al buzón de correo.
   - Seleccione la casilla **Analizar al leer** si quiere que la extensión de Protección contra amenazas de correo para Outlook analice mensajes entrantes cuando los abra el usuario.
   - Seleccione la casilla **Analizar al enviar** si quiere que la extensión de Protección contra amenazas de correo para Outlook analice mensajes salientes cuando sean enviados.
7. Guarde los cambios.

Análisis de correos electrónicos en Thunderbird, MyOffice y R7-Office

El componente Protección contra amenazas de correo analiza los archivos adjuntos a los mensajes de correo entrantes y salientes para detectar virus y otras amenazas. En los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, la aplicación obtiene acceso a los mensajes solo a *nivel de protocolo* (POP3, SMTP, IMAP y NNTP).

Para analizar el tráfico en los clientes de correo Mozilla Thunderbird, MyOffice Mail y R7-Office Organizer, debe agregar el certificado de Kaspersky al almacén de certificados y seleccionar su almacén de certificados propios.

Si utiliza un navegador para acceder a su cliente de correo electrónico, el componente Protección contra amenazas de correo no analizará sus mensajes.

Protección contra amenazas de correo en tiempo real

Protección contra amenazas de correo puede analizar tanto los mensajes entrantes como los salientes. Por defecto, el componente Protección contra amenazas de correo intenta desinfectar automáticamente todos los mensajes de correo infectados que se detectan. Si la desinfección produce un error, el componente Protección contra amenazas de correo elimina los mensajes de correo electrónico infectados. Cuando se detecta un archivo malicioso en un archivo adjunto, Kaspersky Endpoint Security agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[El mensaje ha sido procesado] <asunto del mensaje>*.

Si se está trabajando con el cliente de correo Mozilla Thunderbird, el componente Protección contra amenazas de correo no analiza mensajes que se transmiten mediante el protocolo IMAP en busca de virus y otras amenazas si se utilizan filtros para mover mensajes desde la carpeta Bandeja de entrada.

Análisis de malware en bases de datos de correos

La tarea *Análisis de malware* permite analizar archivos en correos. Si se detecta un objeto malicioso en los archivos de estos clientes de correo, Kaspersky Endpoint Security solo agrega información sobre los objetos detectados a la lista de amenazas activas. La aplicación no desinfecta ni elimina los archivos infectados en las bases de datos de correo, sin importar cuál sea la configuración de la tarea.

Eliminar amenazas activas

Protección contra amenazas de 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 solo puede detectar la amenaza en las bases de datos de correos. Protección contra amenazas de correo no incluye componentes que permitan específicamente desarmar un mensaje en partes (encabezado, cuerpo, archivos adjuntos), con respecto a Microsoft Office Outlook. De este modo, la aplicación no puede eliminar ni desinfectar los objetos detectados. Kaspersky Endpoint Security solo agrega información sobre los objetos detectados a la lista de amenazas activas.

Para eliminar las amenazas activas:

1. Busque y elimine de forma manual el mensaje que contiene el objeto detectado desde la interfaz del cliente de correo.

   La aplicación muestra información sobre el objeto detectado en la lista de amenazas activas.

   Ejemplo de la tarjeta de un 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. Compacte la base de datos.

   Al eliminar un mensaje en la interfaz de usuario, el cliente de correo solo agrega una marca de eliminación. El cliente de correo solo elimina el mensaje después de compactar la base de datos. Para obtener más información sobre la compactación de bases de datos, consulte la ayuda de su cliente de correo (por ejemplo, Mozilla Thunderbird).

3. Vuelva a ejecutar la tarea *Análisis de malware* y asegúrese de que la amenaza ya no esté presente.

Protección contra amenazas de red

El componente *Protección contra amenazas de red* (también llamado 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 ataque de red contra el equipo del usuario, bloquea la conexión al equipo agresor. Las distintas clases de ataques de red sobre las que se tiene registro, así como las maneras de combatirlos, se describen en las bases de datos de la aplicación. La lista de ataques de red que detecta el componente Protección contra amenazas de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación.

Habilitación y deshabilitación de la Protección contra amenazas de red

De forma predeterminada, la Protección contra amenazas de red está habilitada y en ejecución en modo óptimo. Kaspersky Endpoint Security supervisa el tráfico de red entrante en busca de actividad característica de los ataques de red y bloquea los ataques.

Cómo habilitar o deshabilitar la protección contra amenazas 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.

4. Utilice la casilla **Protección contra amenazas de red** para habilitar o deshabilitar el componente.

5. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la protección contra amenazas 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de red**.

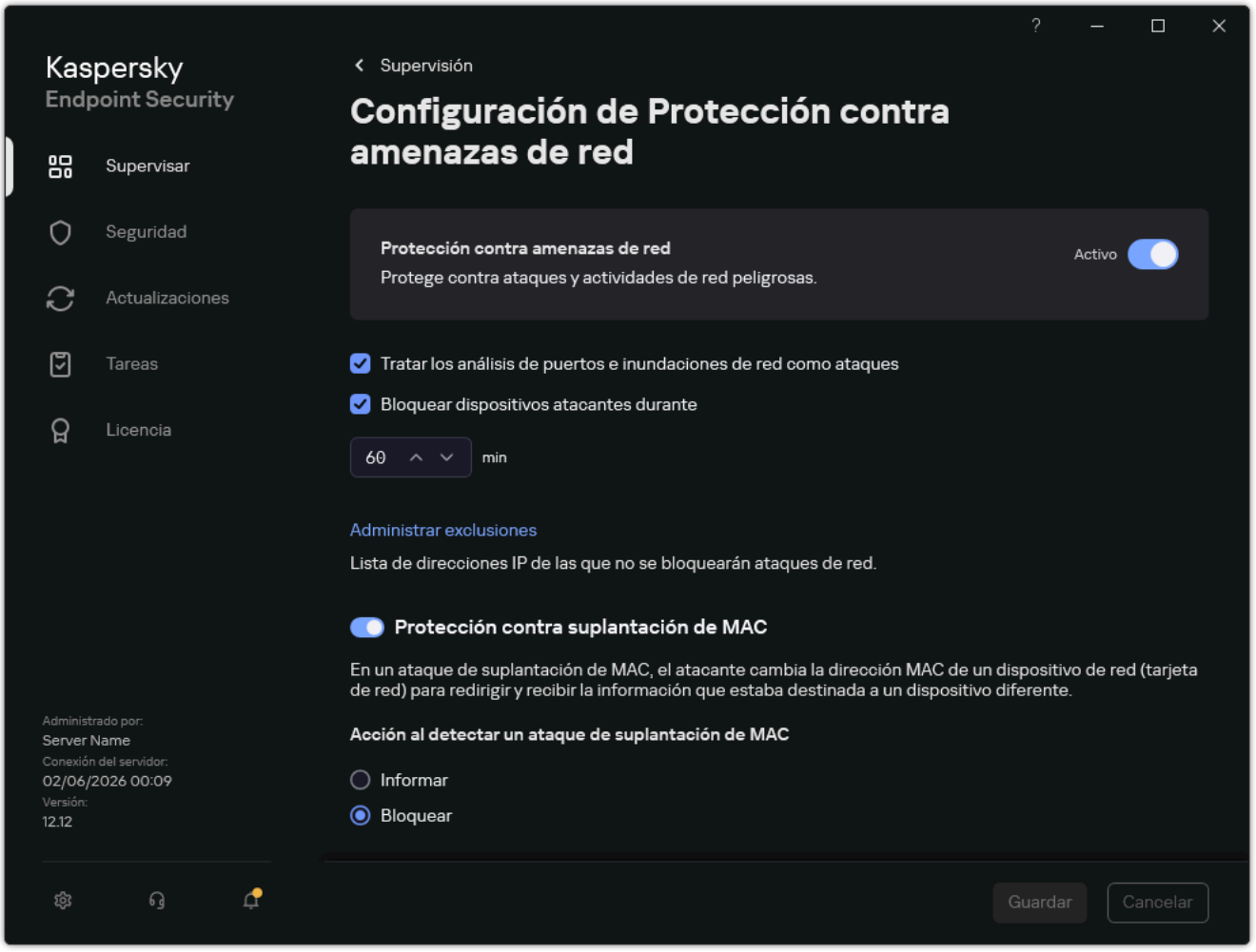
5. Use el interruptor **Protección contra amenazas de red HABILITADA** para habilitar o deshabilitar el componente.

6. Guarde los cambios.

Cómo habilitar o deshabilitar la protección contra amenazas de red en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.



Configuración de Protección contra amenazas de red

3. Use el interruptor **Protección contra amenazas de red** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

Bloquear un equipo atacante

Si el componente Protección contra amenazas de red está habilitado, Kaspersky Endpoint Security bloquea automáticamente las amenazas de red. Además, la aplicación puede bloquear el equipo atacante y restringir el envío de paquetes de red por un periodo de tiempo 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.

4. En **Configuración de Protección contra amenazas de red**, seleccione la casilla **Bloquear dispositivos atacantes durante N min**.

   Si se habilita esta opción, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección. 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 de verificación **Bloquear dispositivos atacantes durante N min**.

6. Guarde los cambios.

Cómo bloquear un equipo atacante 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de red**.

5. En el bloque **Acción al detectar una amenaza**, seleccione la casilla **Bloquear ataque y dispositivo atacante durante (min)**.

   Si se habilita esta opción, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección. 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.

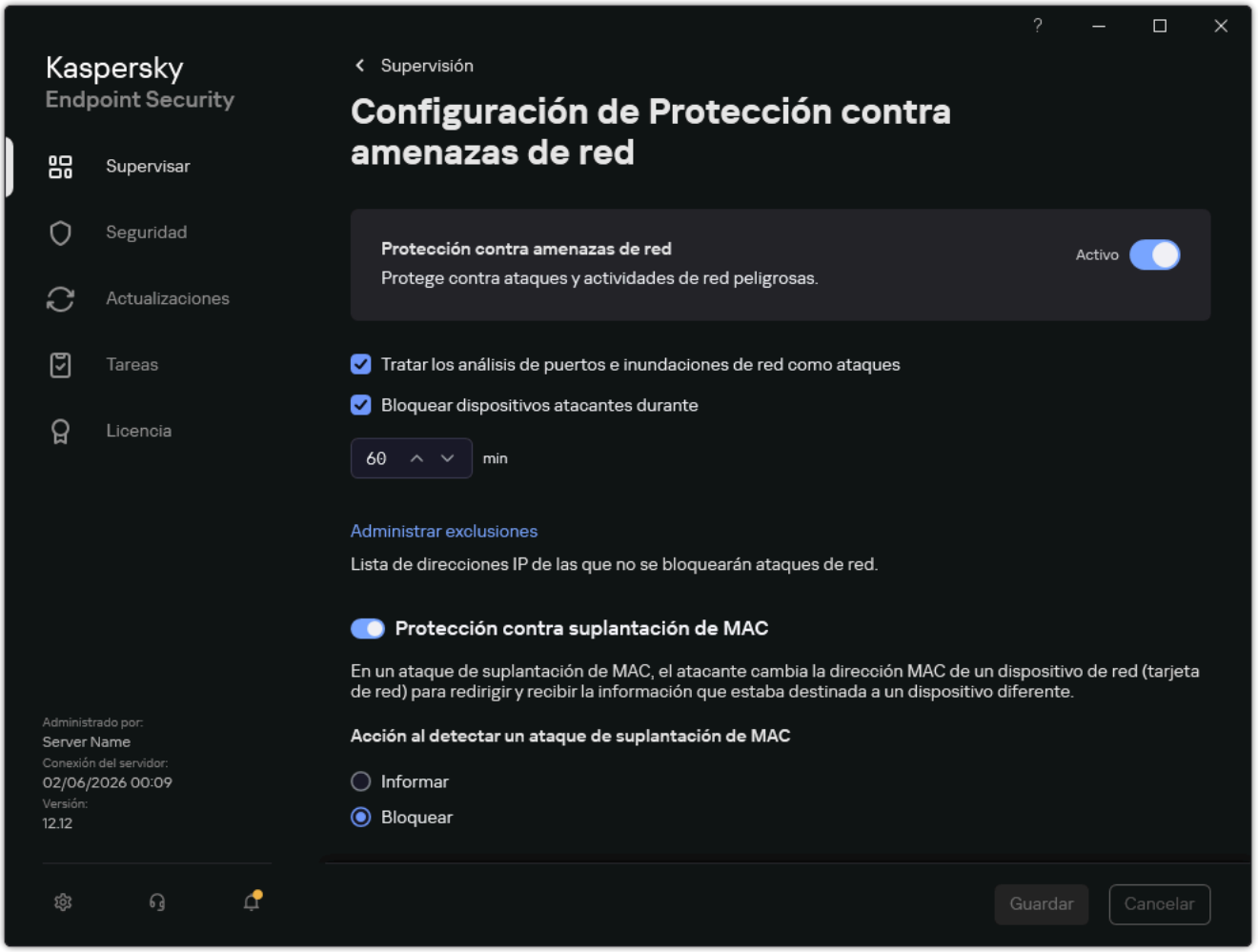
6. Cambie el tiempo de duración del bloqueo hacia el equipo atacante.

7. Guarde los cambios.

Cómo bloquear un equipo atacante en la interfaz de usuario de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.



Configuración de Protección contra amenazas de red

3. Active el interruptor **Bloquear dispositivos atacantes durante N min**.

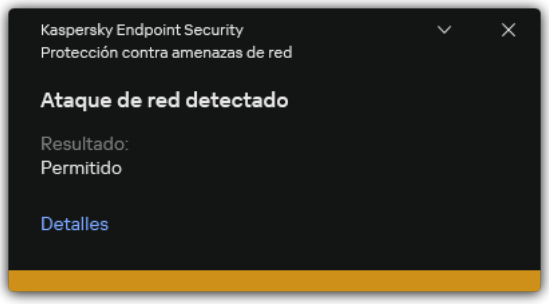
   Si se habilita esta opción, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección. 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 ubicado debajo del conmutador del interruptor de **Bloquear dispositivos atacantes durante N min**.

5. Guarde los cambios.

De esta manera, cuando Kaspersky Endpoint Security detecta un ataque de red contra un equipo del usuario, bloquea todas las conexiones 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 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 de red

Kaspersky Endpoint Security desbloquea el equipo cuando se agota el tiempo especificado. La consola de Kaspersky Security Center no proporciona herramientas para supervisar equipos bloqueados que no sean eventos de *Ataque de red detectado* en el informe. Solo puede ver una lista de equipos bloqueados en la interfaz de la aplicación. Esta funcionalidad es proporcionada por la herramienta *Monitor de red*. También puede usar la herramienta Monitor de red para desbloquear un equipo.

Para desbloquear un equipo:

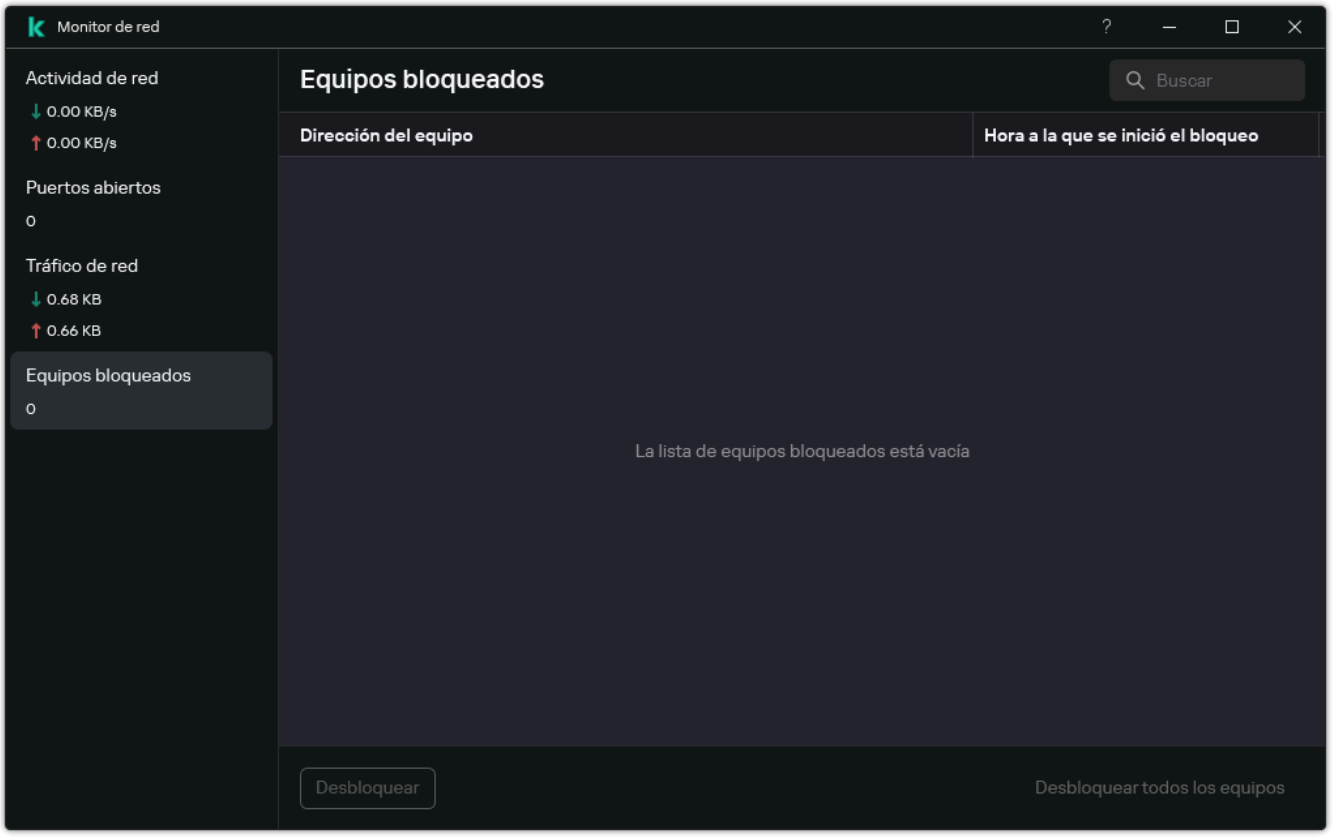
1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Monitor de red**.

2. Vaya a la pestaña **Equipos bloqueados**.

   Esto abre una lista de equipos bloqueados (consulte la figura a continuación).

   La lista de equipos bloqueados se vacía cada vez que Kaspersky Endpoint Security se reinicia o cuando se modifica la configuración de Protección contra amenazas de red.

3. Seleccione el equipo que desea desbloquear y haga clic en **Desbloquear**.



Lista de equipos bloqueados

Configuración de direcciones de exclusiones del bloqueo

Kaspersky Endpoint Security puede reconocer un ataque a la 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 agregar las direcciones IP de estos dispositivos a la lista de exclusiones. También puede seleccionar el protocolo y el puerto que se utilizan para la comunicación y permitir actividades de red específicas.

La capacidad de seleccionar protocolos y puertos para exclusiones se agregó en Kaspersky Endpoint Security 12.2. Asegúrese de que la aplicación y el complemento de administración estén actualizados a la versión 12.2 o posterior. Si está utilizando una versión anterior de la aplicación o el complemento de administración, Kaspersky Endpoint Security puede permitir actividades de red solo por dirección IP.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de exclusiones de bloqueo. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Cómo configurar las direcciones de las exclusiones del bloqueo 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.
4. En el bloque **Configuración de Protección contra amenazas de red**, haga clic en el botón **Exclusiones**.
5. En la ventana que se abre, haga clic en el botón **Agregar**.
6. Ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.
   Si es necesario, seleccione el protocolo y los puertos a través de los cuales se transmiten los datos.
7. Guarde los cambios.

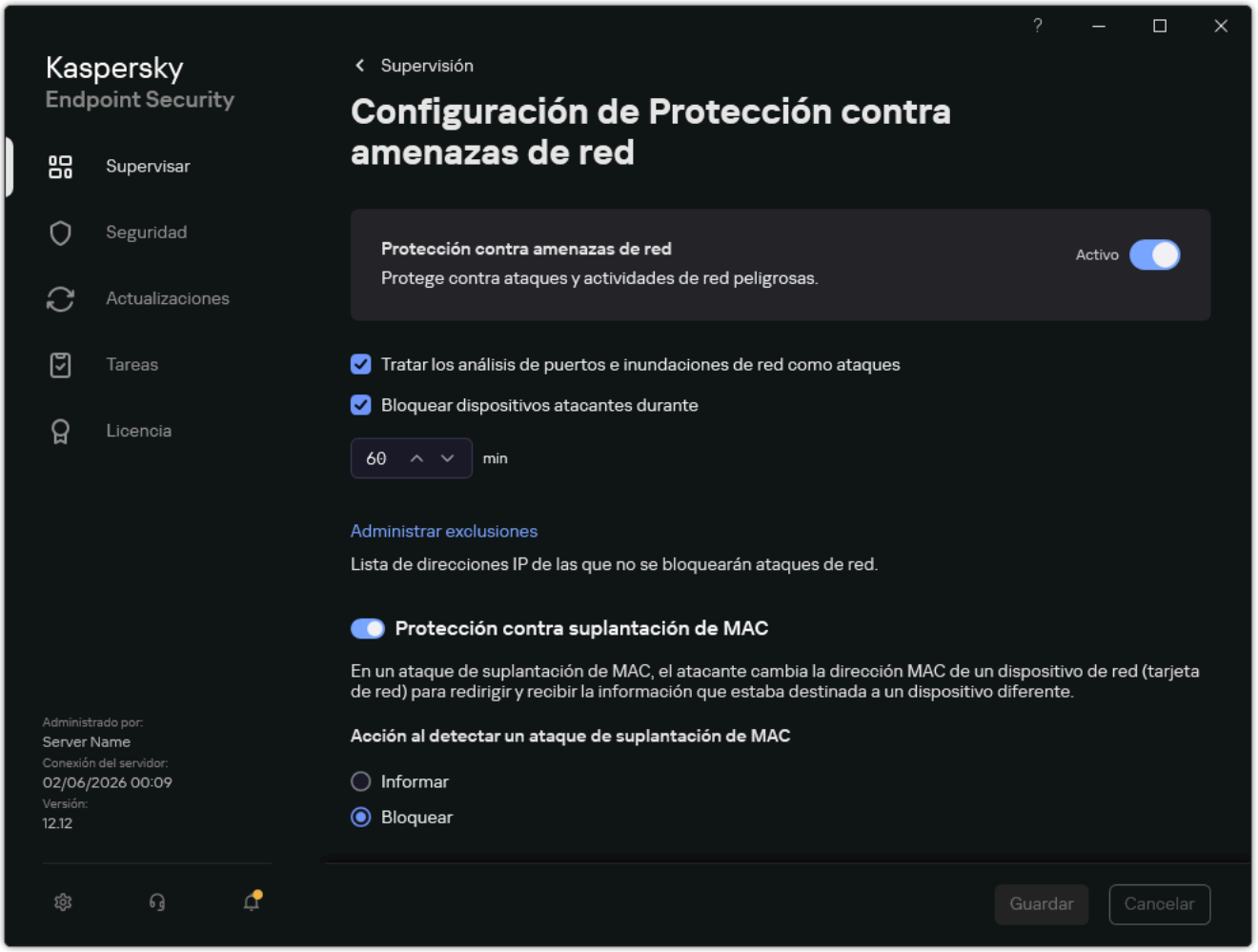
Cómo configurar las direcciones de las exclusiones del bloqueo en Web Console y Cloud Console

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 ficha **Configuración de la aplicación**.
4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de red**.
5. En la parte superior de la ventana, haga clic en el vínculo **Direcciones IP de confianza**.
6. En la ventana que se abre, haga clic en el botón **Agregar**.
7. Ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.
   Si es necesario, especifique la subred.
8. Guarde los cambios.

Cómo configurar las direcciones de las exclusiones del bloqueo en la interfaz de usuario de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.



Configuración de Protección contra amenazas de red

3. Haga clic en el vínculo **Administrar exclusiones**.

4. En la ventana que se abre, haga clic en el botón **Agregar**.

5. Ingrese la dirección IP del equipo desde el cual no se deben bloquear 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.

Exportar e importar la lista de exclusiones de bloqueo

Puede exportar la lista de exclusiones a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.

4. En el bloque **Configuración de Protección contra amenazas de 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, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.

   c. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de 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 que se usará para importar la lista de exclusiones.

   b. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

8. Guarde los cambios.

Configurar Protección contra amenazas de red por tipo

Puede activar o desactivar las defensas de Kaspersky Endpoint Security contra los siguientes tipos de ataques de red:

- Ataques de *saturación de red*, con los cuales se busca afectar los recursos de red (por ejemplo, los servidores web) de una organización. En esta clase de ataque, se realiza una gran cantidad de solicitudes con el fin de sobrecargar el ancho de banda disponible para los recursos de red. La saturación impide el acceso a los recursos de la organización.

- Ataques de *análisis de puertos*, en los cuales se realiza un sondeo de los puertos UDP, los puertos TCP y los servicios de red del equipo. El escaneo de puertos permite determinar qué tan vulnerable es un equipo; suele estar seguido por algún tipo de ataque más peligroso. Esto también revela el sistema operativo del equipo, lo que permite elegir el ataque de red más apropiado.

- Ataques de *suplantación de MAC*, que consisten en cambiar la dirección MAC de un dispositivo (tarjeta) de red. Al realizar este cambio, un atacante puede redirigir los datos destinados a un dispositivo a otro dispositivo diferente y, de ese modo, obtener acceso a la información. Kaspersky Endpoint Security le permite saber si se detecta uno de estos ataques y bloquearlo.

Si alguna de sus aplicaciones autorizadas realiza operaciones que son típicas de estas clases de ataques, puede deshabilitar las funciones de detección pertinentes. Con ello evitará las falsas alarmas.

De manera predeterminada, Kaspersky Endpoint Security no está configurado para detectar ataques de saturación de red, de escaneo de puertos o de suplantación de MAC.

No recomendamos habilitar 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 contra amenazas de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.

4. Utilice la casilla **Tratar los análisis de puertos e inundaciones de red como ataques** para habilitar o deshabilitar la detección de estos ataques.

   Si esta funcionalidad está habilitada, Kaspersky Endpoint Security supervisa el tráfico de red para detectar escaneo de puertos y saturación de red. Si se detecta este tipo de comportamientos, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación ofrece información sobre el equipo que está realizando las solicitudes. Esta información es necesaria para brindar una respuesta oportuna. Sin embargo, Kaspersky Endpoint Security no bloquea el equipo que está realizando las solicitudes, ya que este tráfico puede ser algo normal en la red corporativa.

5. En el bloque **Modo de protección contra suplantación de MAC**, seleccione una de las siguientes opciones:

   - **No rastrear suplantaciones de MAC**.
   - **Informar**.
   - **Bloquear**.

6. Guarde los cambios.

Cómo configurar Protección contra amenazas de red por tipo 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de red**.

5. Utilice la casilla **Tratar los análisis de puertos e inundaciones de red como ataques** para habilitar o deshabilitar la detección de estos ataques.

   Si esta funcionalidad está habilitada, Kaspersky Endpoint Security supervisa el tráfico de red para detectar escaneo de puertos y saturación de red. Si se detecta este tipo de comportamientos, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación ofrece información sobre el equipo que está realizando las solicitudes. Esta información es necesaria para brindar una respuesta oportuna. Sin embargo, Kaspersky Endpoint Security no bloquea el equipo que está realizando las solicitudes, ya que este tráfico puede ser algo normal en la red corporativa.

6. En el bloque **Protección contra suplantación de MAC**, seleccione una de las siguientes opciones:

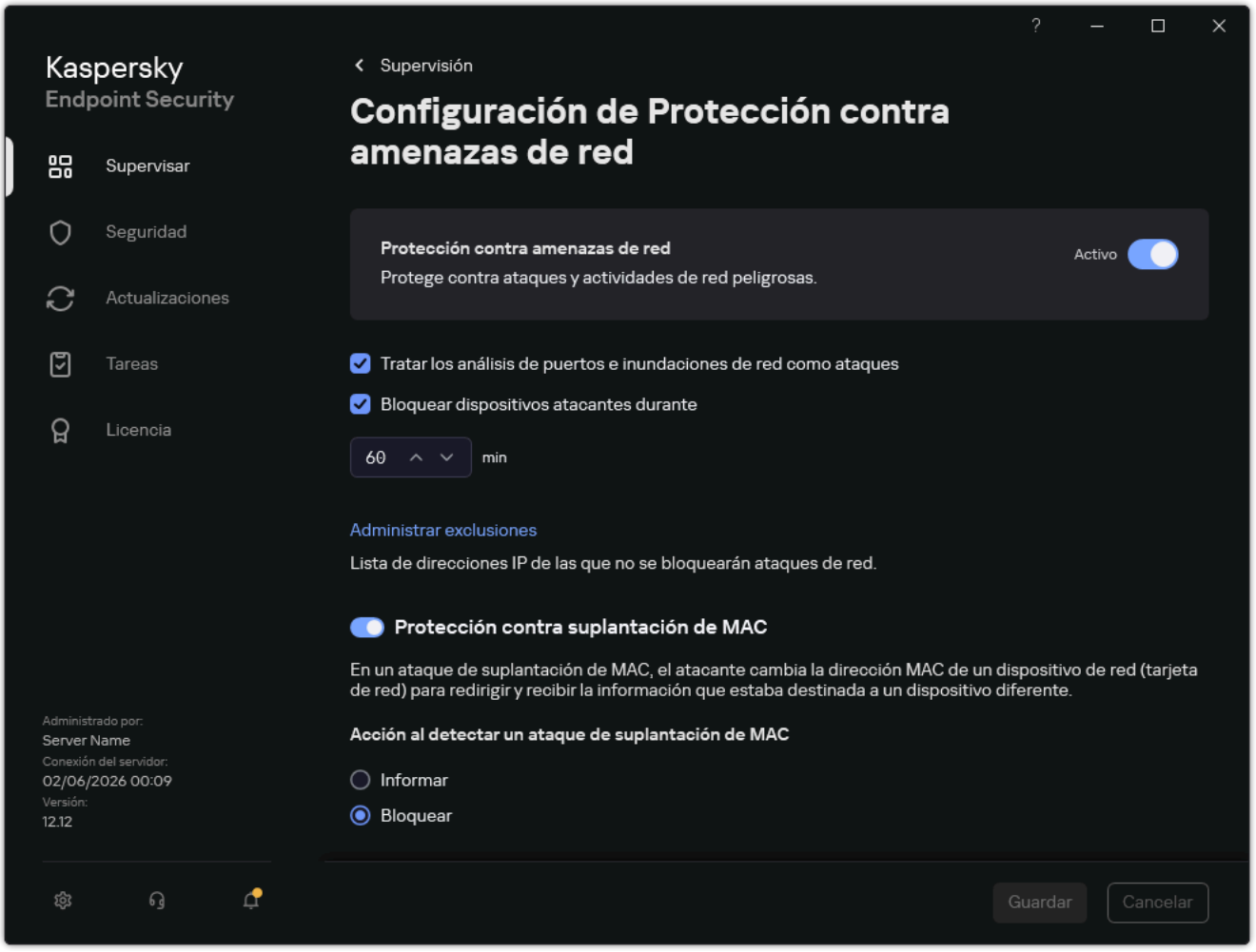
   - **Protección contra suplantación de MAC HABILITADA**.
   - **Informar**.
   - **Bloquear**.

7. Guarde los cambios.

Cómo configurar Protección contra amenazas de red por tipo en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.



Configuración de Protección contra amenazas de red

3. Use el interruptor **Tratar los análisis de puertos e inundaciones de red como ataques** para habilitar o deshabilitar la detección de estas clases de ataque.

   Si esta funcionalidad está habilitada, Kaspersky Endpoint Security supervisa el tráfico de red para detectar escaneo de puertos y saturación de red. Si se detecta este tipo de comportamientos, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación ofrece información sobre el equipo que está realizando las solicitudes. Esta información es necesaria para brindar una respuesta oportuna. Sin embargo, Kaspersky Endpoint Security no bloquea el equipo que está realizando las solicitudes, ya que este tráfico puede ser algo normal en la red corporativa.

4. Use el interruptor **Protección contra suplantación de MAC** para habilitar o deshabilitar la detección de estas clases de ataque.

5. En el bloque **Acción al detectar un ataque de suplantación de MAC**, seleccione una de las siguientes opciones:

   - **Informar**.

   - **Bloquear**.

6. Guarde los cambios.

Firewall

El componente Firewall impide que se establezcan conexiones no autorizadas cuando el equipo está conectado a una red local o a Internet. Firewall también controla la actividad de red de las aplicaciones instaladas en el equipo. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el servicio de nube Kaspersky Security Network y las *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. El firewall crea automáticamente las reglas de red necesarias para que la aplicación y el Agente de red funcionen. Como resultado, el firewall abre varios puertos en la computadora. Los puertos que se abren dependen de la función de la computadora (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en la computadora, consulte la Ayuda de Kaspersky Security Center.

Reglas de red

Las reglas de red se pueden configurar en distintos niveles:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security incluye una serie de reglas predefinidas, con permisos configurados según las recomendaciones de los expertos de Kaspersky.

- *Reglas de red de aplicaciones*. Las reglas de red de la aplicación imponen restricciones en la actividad de la red de una aplicación específica. Tienen en cuenta no solo las características del paquete de red, sino también la aplicación específica a la cual se dirige este paquete de red o que los emitió.

Controlar el acceso de las aplicaciones a los datos personales, a los procesos y a los recursos del sistema operativo es tarea del componente Prevención de intrusiones en el host, que utiliza los *derechos* asignados a las aplicaciones para tal fin.

Cuando una aplicación se ejecuta por primera vez, Firewall realiza las siguientes acciones:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.

2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Firewall, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima* o *No confiables*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea la actividad de red de la aplicación si su grupo de confianza así lo requiere. Por ejemplo, las aplicaciones del grupo *Restricción máxima* no tienen permitido usar ninguna conexión de red.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Si la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están definidas para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más arriba en la lista se encuentra una regla, mayor es su prioridad. Cuando un mismo tipo de actividad de red se describe en varias reglas, Firewall se basa en la regla de mayor prioridad para regular la actividad.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si las reglas de paquetes de red y las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se procesa según las reglas de paquetes de red.

Las reglas de red para las aplicaciones funcionan de una manera particular. La regla de red para las aplicaciones incluye reglas de acceso según el estado de la red: *Red pública*, *Red local*, *Red de confianza*. Las aplicaciones del grupo de confianza *Restricción máxima*, por ejemplo, no tienen permitido realizar ninguna clase de actividad de red, independientemente de que el equipo esté conectado a una red pública, local o de confianza. Cuando se crea una regla de red para una aplicación individual (aplicación principal), dicha regla afecta también a los procesos secundarios de otras aplicaciones. Cuando no existe una regla de red para una aplicación, los procesos secundarios quedan sujetos a la regla de acceso de red correspondiente al grupo de confianza de la aplicación.

Supóngase, por ejemplo, que se prohíbe el tráfico en redes de cualquier estado para todas las aplicaciones, a excepción del navegador X. El navegador X (aplicación principal) se utiliza luego para iniciar la instalación de un navegador Y (proceso secundario). En este caso, el instalador del navegador Y tendrá acceso a la red y podrá descargar los archivos que hagan falta. Tras la instalación, sin embargo, Firewall no permitirá que el navegador Y establezca conexiones de red. Para que el instalador del navegador Y no pueda acceder a la red valiéndose de su condición de proceso secundario, será necesario agregar una regla de red que cubra ese programa específico.

Tipos de las conexiones de red

Firewall puede controlar la actividad de red basándose en el tipo de la conexión. Kaspersky Endpoint Security obtiene el tipo de la conexión del sistema operativo. El tipo informado por el sistema operativo es el que el usuario configura cuando la conexión se establece por primera vez. Si lo desea, puede cambiar el tipo de la conexión de red en la configuración de Kaspersky Endpoint Security. El Firewall controlará la actividad de red según el tipo de red especificado en la configuración de Kaspersky Endpoint Security, y no en el sistema operativo.

Están disponibles los siguientes tipos de conexión de red:

- **Red pública**. Una red que no está protegida por una aplicación antivirus, un filtro o un firewall (un ejemplo podría ser la red Wi-Fi de una cafetería). Cuando el usuario opera un equipo conectado a una red de ese tipo, el Firewall bloquea el acceso a archivos e impresoras de este equipo. Los usuarios externos tampoco tienen acceso a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella.

  De forma predeterminada, Firewall asigna el tipo *Red pública* a Internet. No puede cambiar el tipo de Internet.

- **Red local**. Una red en la que los usuarios tienen restricciones para acceder a los archivos y las impresoras del equipo (un ejemplo podría ser una LAN corporativa u hogareña).

- **Red de confianza**. Una red segura, en la que el equipo no está expuesto a ningún ataque o a intentos no autorizados de acceder a los datos que contiene. Firewall permite cualquier actividad de red dentro de las redes con este estado.

Habilitación o deshabilitación del Firewall

Por defecto, el Firewall está habilitado y funciona en modo óptimo.

Cómo habilitar o deshabilitar el 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.

4. Utilice la casilla **Firewall** para habilitar o deshabilitar el componente.

5. Guarde los cambios.

Cómo habilitar o deshabilitar el Firewall 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 ficha **Configuración de la aplicación**.

4. Seleccione **Comunicación y Protección web** → **Firewall**.

5. Use el interruptor **Firewall HABILITADO** para habilitar o deshabilitar el componente.

6. Guarde los cambios.

Cómo habilitar o deshabilitar el Firewall en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.

3. Use el interruptor **Firewall** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

Como resultado, si el Firewall está habilitado, Kaspersky Endpoint Security controla la actividad de la red y bloquea las conexiones de red no autorizadas a su equipo. También bloquea la actividad de red no autorizada de las aplicaciones en su equipo. El componente Protección contra amenazas de red también controla la actividad de red. El componente Protección contra amenazas de red (también llamado Sistema de detección de intrusiones, 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 de Firewall. Aunque el Firewall bloquee la conexión de red mediante reglas y, por lo tanto, evite un ataque a la red, el componente Protección contra amenazas de red registra los eventos del ataque a la red. Es obligatorio para obtener información estadística sobre los ataques de red en los equipos de su organización.

Cambio del tipo de la conexión de red

De forma predeterminada, Firewall asigna el tipo *Red pública* a Internet. No puede cambiar el tipo de Internet.

Para cambiar el tipo de la conexión de red:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en **Redes disponibles**.

4. Seleccione la conexión de red cuyo tipo quiera cambiar.

5. En la columna **Tipo de red**, seleccione el tipo de la conexión de red:

   - **Red pública**. Una red que no está protegida por una aplicación antivirus, un filtro o un firewall (un ejemplo podría ser la red Wi-Fi de una cafetería). Cuando el usuario opera un equipo conectado a una red de ese tipo, el Firewall bloquea el acceso a archivos e impresoras de este equipo. Los usuarios externos tampoco tienen acceso a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella.

   - **Red local**. Una red en la que los usuarios tienen restricciones para acceder a los archivos y las impresoras del equipo (un ejemplo podría ser una LAN corporativa u hogareña).

   - **Red de confianza**. Una red segura, en la que el equipo no está expuesto a ningún ataque o a intentos no autorizados de acceder a los datos que contiene. Firewall permite cualquier actividad de red dentro de las redes con este estado.

6. Guarde los cambios.

Administración de reglas de paquetes de red

Puede realizar las siguientes acciones mientras administra las reglas de paquetes de red:

- Crear una nueva regla de paquetes de red.

  Puede crear una nueva regla de paquetes de red al crear un conjunto de condiciones y acciones que se aplicará a los paquetes de red y flujos de datos.

- Habilitar o deshabilitar una regla de paquetes de red.

  Todas las reglas de paquetes de red creadas por el Firewall por defecto presentan el estado *Habilitado*. Cuando se habilita una regla de paquetes de red, el Firewall aplica esta regla.

  Puede deshabilitar cualquier regla de paquetes de red seleccionada en la lista de reglas de paquetes de red. Cuando se deshabilita una regla de paquetes de red, el Firewall deja temporariamente de aplicar esta regla.

  > Cuando se agrega una nueva regla de paquetes de red personalizada a la lista de reglas de paquetes de red, por defecto aparece con estado *Habilitado*.

- Editar la configuración de una regla de paquetes de red existente.

  Luego de crear una nueva regla de paquetes de red, siempre puede volver a editar su configuración y modificarla según sea necesario.

- Cambiar la acción del Firewall para una regla de paquetes de red.

  En la lista de reglas de paquetes de red, puede editar la acción que realizará el Firewall al detectar actividad de red que no coincide con una regla de paquetes de red específica.

- Cambiar la prioridad de una regla de paquetes de red.

  Puede elevar o disminuir la prioridad de una regla de paquetes de red seleccionada en la lista.

- Eliminar una regla de paquetes de red.

  Puede eliminar una regla de paquetes de red para que el Firewall deje de aplicar esta regla al detectar actividad de red y para evitar que aparezca esta regla en la lista de reglas de paquetes de red con estado *Deshabilitado*.

Creación de 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 o protocolo) que el Firewall aplica para controlar las conexiones de red del equipo. Las reglas de paquetes de red también especifican la acción que el Firewall realiza 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, pero recomendamos usar direcciones IP e intervalos de direcciones IP. 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 malicioso también puede falsificar mensajes DNS y eludir las reglas del Firewall.

Puede controlar las conexiones de red mediante nombres DNS utilizando reglas de Control web. Si necesita especificar un nombre DNS en las reglas del Firewall:

- Compruebe que la LAN corporativa sea segura.
- Compruebe que el almacenamiento en caché y los servidores DNS autorizados sean seguros.
- Habilite la protección del registro DNS contra modificaciones.

Al crear reglas de paquetes de red, recuerde que estas tienen prioridad sobre las reglas de red para aplicaciones.

Métodos para crear reglas de paquetes de red

Existen distintos métodos para crear una regla de paquetes de red:

- Utilizar la herramienta Monitor de red.

  El *Monitor de red* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de red del equipo de un usuario. Si opta por utilizar esta herramienta, no necesitará configurar todos los ajustes de la regla. Algunos de los ajustes de Firewall se tomarán de los datos del Monitor de red y se insertarán automáticamente. Para usar el Monitor de red, debe tener acceso a la interfaz de la aplicación.

- Configurar los ajustes de Firewall.

  Este método permite configurar cada parámetro de Firewall en detalle. Podrá crear reglas que cubran cualquier clase de actividad de red, aunque se trate de tráfico que no se haya registrado al momento de crear la regla.

Cómo usar la herramienta Monitor de red para crear una regla de paquetes de red mediante la interfaz de la aplicación

1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Monitor de red**.
2. Vaya a la pestaña **Actividad de red**.

   En la ficha **Actividad de red** se muestran todas las conexiones de red actuales del equipo. Se muestran las conexiones de red entrantes y salientes.
3. En el menú contextual de una conexión de red, seleccione **Crear regla de paquetes de red**.

   Se abren las propiedades de la regla de red.
4. Establezca el estado **Activo** para la regla del paquete.
5. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
6. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el vínculo **Plantilla de regla de red**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
7. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
8. Haga clic en **Guardar**.

   La nueva regla de red se agregará a la lista.
9. Utilice los botones **Subir**/**Abajo** para configurar la prioridad de la regla de red.
10. Guarde los cambios.

Cómo crear una regla de paquetes de red desde la configuración de Firewall en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en **Reglas de paquetes**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
4. En la lista desplegable **Agregar**, seleccione la ubicación de la regla en la lista: en la parte superior de la lista, en la parte inferior de la lista o al lado de la regla seleccionada.

   La posición de la regla en la lista determina su prioridad. La regla que aparece en la parte superior de la lista tiene la prioridad más alta.
5. Establezca el estado **Activo** para la regla del paquete.
6. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el vínculo **Plantilla de regla de red**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.

8. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

9. Haga clic en **Guardar**.

   La nueva regla de red se agregará a la lista.

10. Utilice los botones **Subir**/**Abajo** para configurar la prioridad de la regla de red.

11. Guarde los cambios.

Cómo crear una regla de paquetes de red 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.

4. En el bloque **Configuración de Firewall**, haga clic en el botón **Configuración**.

   Se abre una lista con las reglas de paquetes de red y otra lista con las reglas de red para aplicaciones.

5. Vaya a la pestaña **Reglas de paquetes de red**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.

6. En la lista desplegable **Agregar**, seleccione la ubicación de la regla en la lista: en la parte superior de la lista, en la parte inferior de la lista o al lado de la regla seleccionada.

   La posición de la regla en la lista determina su prioridad. La regla que aparece en la parte superior de la lista tiene la prioridad más alta.

7. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.

8. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el botón , podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.

9. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

10. Guarde la nueva regla de red.

11. Utilice los botones **Subir**/**Bajar** para configurar la prioridad de la regla de red.

12. Guarde los cambios.

Firewall controlará los paquetes de red según lo indique la regla. Para que Firewall deje de procesar una regla, en lugar de eliminarla de la lista, puede deshabilitarla. Para hacerlo, desactive la casilla ubicada junto al objeto.

Cómo crear una regla de paquetes de red 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 ficha **Configuración de la aplicación**.

4. Seleccione **Comunicación y Protección web** → **Firewall**.

5. Seleccione la ficha **Reglas de paquetes de red**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.

6. Haga clic en **Agregar**.

   Se abre el formulario para una nueva regla de red.

7. Ingrese manualmente el nombre del servicio de red en el campo **Nombre de la regla**.

8. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el vínculo **Seleccionar plantilla de regla**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.

9. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

10. Guarde la regla de red.

    La nueva regla de red se agregará a la lista.

11. Utilice el botón **Mover** para establecer la prioridad de la regla de red.

12. Guarde los cambios.

Firewall controlará los paquetes de red según lo indique la regla. Para que Firewall deje de procesar una regla, en lugar de eliminarla de la lista, puede deshabilitarla. Use el interruptor de la columna **Estado** para habilitar o deshabilitar la regla de paquetes.

Parámetros de las reglas de paquetes de red

Parámetro	Descripción
Acción	**Permitir**. **Bloquear**. **Según reglas de aplicaciones**. Si elige esta opción, Firewall aplicará las reglas de red de aplicaciones a la conexión de red.
Protocolo	Controle la actividad de la red en el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE. Si se selecciona ICMP o ICMPv6 como protocolo, puede definir el tipo y el código del paquete ICMP. Si selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto que usarán el equipo local y el equipo remoto para establecer la conexión a supervisar. Rango de valores posibles para los números de puerto: 0–65535. En cada campo, puede ingresar varios valores separados por `,` o especificar un rango de valores usando `-`. Por ejemplo: • `100,101` • `100-130` • `100,110-130`
Sentido	**Entrante (paquete)**. 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 a través de una conexión establecida por un equipo remoto. **Entrante/Saliente**. Firewall aplica la regla de red a todos los paquetes de red entrantes y salientes. **Saliente (paquete)**. Firewall aplica la regla de red a todos los paquetes de red salientes. **Saliente**. Firewall aplica la regla de red a todos los paquetes de red enviados a través de una conexión establecida por el equipo del usuario.
Adaptadores de red	Adaptadores de red disponibles para enviar o recibir paquetes de red. Al especificar la configuración de los adaptadores de red, es posible diferenciar entre paquetes de red enviados o recibidos por 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).

Parámetro	Descripción
Direcciones remotas	Direcciones de red asignadas a equipos remotos que pueden enviar y recibir paquetes de red. Firewall aplicará la regla de red a las direcciones de red remotas que estén dentro del intervalo especificado. Puede optar por incluir todas las direcciones IP en una regla de red, crear una lista de direcciones IP separada, especificar un rango de direcciones IP o seleccionar una subred (Redes de confianza, Redes locales o Redes públicas). También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos de red LAN o servicios internos. La interacción con los servicios en la nube (como Microsoft Azure) y otros recursos de Internet debe ser procesado por el componente Control web. Si en la regla de paquete de red agregó un nombre DNS para el cual no se pudo determinar la dirección IP, Kaspersky Endpoint Security mostrará una advertencia. En la lista de reglas de paquetes de red en Web Console, se agrega una columna con una descripción del error. En la Consola de administración (MMC), la descripción del error no está disponible. Este tipo de reglas de paquetes están resaltadas en color.
Direcciones locales	Direcciones de red asignadas a equipos que pueden enviar y recibir paquetes de red. Firewall aplica una regla de red al rango especificado de direcciones de redes locales. Puede optar por incluir todas las direcciones IP en una regla de red, crear una lista de direcciones IP separada o especificar un rango de direcciones IP. La aplicación almacena las direcciones locales solo si se especifica una lista de direcciones remotas. Es decir, se seleccionó el valor **Direcciones de la lista** para **Direcciones remotas** y se agregó al menos una dirección. A veces no puede obtenerse la dirección local para las aplicaciones. Cuando esto ocurre, este parámetro no se tiene en cuenta.

Habilitación o deshabilitación de una regla de paquetes de red

Para habilitar o deshabilitar una regla de paquetes de red:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en **Reglas de paquetes**.
   Esto abre una lista de reglas de paquetes de red predeterminados que son establecidas por el Firewall.
4. Seleccione la regla de paquetes de red necesaria en la lista.
5. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la regla.
6. Guarde los cambios.

Cambio de la acción del Firewall para una regla de paquetes de red

Para cambiar la acción del Firewall que se aplica a una regla de paquetes de red.

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en **Reglas de paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminados que son establecidas por el 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 el Firewall al detectar este tipo de actividad de red:

   - **Permitir**.
   - **Bloquear**.
   - **Según reglas de aplicaciones**. Si elige esta opción, Firewall aplicará las reglas de red de aplicaciones a la conexión de red.

6. Guarde los cambios.

Cambio de la prioridad de una regla de paquetes de red

La prioridad de una regla de paquetes de red se determina por su posición en la lista de reglas de paquetes de red. La regla de paquetes de red superior de la lista de reglas de paquetes de red tiene la prioridad mayor.

Toda regla de paquetes de red creada manualmente se agrega al final de la lista de reglas de paquetes de red y es de prioridad menor.

El Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba a abajo. Según la regla de paquetes de red procesada que se aplica a una conexión de red en particular, el Firewall permite o bloquea el acceso a la red a la dirección y al puerto que se indican en la configuración de la conexión de red.

Para modificar la prioridad de la regla de paquetes de red:

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

2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en **Reglas de paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminados que son establecidas por el Firewall.

4. En la lista, seleccione la regla de paquetes de red cuya prioridad quiera cambiar.

5. Utilice los botones **Subir**/**Abajo** para configurar la prioridad de la regla de red.

6. Guarde los cambios.

Exportar e importar reglas de paquetes de red

Puede exportar la lista de reglas de paquetes de red a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 otro servidor.

Cómo exportar e importar una lista de reglas de paquetes de red a la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.
4. En el bloque **Configuración de Firewall**, haga clic en el botón **Configuración**.

   Se abre una lista con las reglas de paquetes de red y otra lista con las reglas de red para aplicaciones.
5. Vaya a la pestaña **Reglas de paquetes de red**.
6. Para exportar la lista de reglas de paquetes de red:

   a. Seleccione la regla de acceso que desea 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 vínculo **Exportar**.

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.
7. Para importar una lista de reglas para paquetes de red:

   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 ficha **Configuración de la aplicación**.
4. Seleccione **Comunicación y Protección web** → **Firewall**.

5. Para exportar la lista de reglas, en el bloque **Reglas de paquetes de red**:

   a. Seleccione la regla de acceso que desea 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 que se usará para importar la lista de reglas.

   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

7. Guarde los cambios.

Definir las reglas de paquetes de red en XML

Firewall permite exportar reglas de paquetes de red en formato XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de reglas del mismo tipo.

El archivo XML incluye dos nodos principales: `Rules` y `Resources`. El nodo `Rules` enumera las reglas de paquetes de red. Este nodo incluye las reglas configuradas de manera predeterminada (*reglas predefinidas*) y también las reglas agregadas por el usuario (*reglas personalizadas*).

Revisión de las 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 el valor, mayor la prioridad.	Entero El valor de prioridad debe tener 4 dígitos. Los nodos del archivo XML se deben organizar por valor de prioridad, a partir de `0000`.
`RuleId`	Id. de la regla.	**Reglas predefinidas** `100`: **Solicitudes para el servidor DNS por medio de TCP**. `101`: **Solicitudes para el servidor DNS por medio 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 de TCP a través de puertos locales**. `132`: **Conexiones de UDP a través de puertos locales**. `133`: **Flujo de TCP entrante**. `134`: **Flujo de UDP entrante**. `137`: **Respuestas entrantes de destino inaccesible de ICMP**. `138`: **Paquetes entrantes de respuestas de eco ICMP**. `140`: **Respuestas entrantes de tiempo superado de ICMP**. `142`: **Flujo de ICMP entrante**. `266`: **Paquetes entrantes de solicitudes de eco ICMPv6**.
`RuleState`	Estado de la regla.	`0`: la regla predefinida está deshabilitada `1`: la regla predefinida está habilitada `2`: la regla personalizada está deshabilitada `3`: la regla personalizada está habilitada
`RuleTypeId`	Id. del tipo de regla.	`4`: regla de paquetes de red.
`AppIdEx`	Id. de la aplicación a la que pertenece la regla de paquetes de red.	Si la regla no pertenece a ninguna aplicación, el valor es `0`.
`ResIdEx`	Id. principal del recurso que tiene la configuración de reglas. Puede utilizar este identificador para encontrar un bloque que tenga una 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 la configuración de la regla de paquetes de red. La configuración de la regla personalizada de paquetes de red se enumera en el bloque `<key name="0004">`.

Revisión de la regla personalizada de paquetes de red

```
<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 la regla personalizada de paquetes de red

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 (Wi-Fi)**. • `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`: deshabilitado. `1`: **ICMP**. `2`: **IGMP**. `6`: **TCP**. `17`: **UDP**. `47`: **GRE**. `58`: **ICMPv6**.
`Direction`	Valor del parámetro **Sentido**.	`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 deshabilitado. `3`: **Destino inaccesible** (ICMP). `4`: **Mensaje de control de flujo**. `5`: **Redireccionamiento**. `6`: **Dirección del host alternativo**. `8`: **Solicitud de eco**. `9`: **Anuncio de enrutador**. `10`: **Solicitud de enrutador**. `11`: **Tiempo superado**. `12`: **Problema de parámetros**. `13`: **Marca de hora**. `14`: **Respuesta de marca de hora**. `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`: **Redireccionamiento del host móvil**. `33`: **IPv6 ¿dónde estás?**. `34`: **IPv6 aquí estoy**. `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`: **Destino inaccesible**. `2`: **Paquete demasiado grande**. `3`: **Tiempo superado**. `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 finalizada**. `133`: **Solicitud de enrutador**. `134`: **Anuncio de enrutador**. `135`: **Solicitud de vecino**. `136`: **Anuncio de vecino**. `137`: **Mensaje de redireccionamiento**. `138`: **Nueva numeración de enrutador**. `139`: **Consulta de información del nodo ICMP**. `141`: **Mensaje de solicitud de detección inversa de vecinos**. `142`: **Mensaje de anuncio de detección inversa de vecinos**. `143`: **Informe de escucha de multidifusión, versión 2**.

Parámetro	Descripción	Valor
		`144`: **Mensaje de solicitud de detección de dirección de agente principal**. `145`: **Mensaje de respuesta de detección de dirección de agente principal**. `146`: **Solicitud de prefijo móvil**. `147`: **Anuncio de prefijo móvil**. `148`: **Mensaje de solicitud de ruta de certificación**. `149`: **Mensaje de anuncio de ruta de certificación**. `151`: **Anuncio de enrutador de multidifusión**. `152`: **Solicitud de enrutador de multidifusión**. `153`: **Cierre de enrutador de multidifusión**.
`IcmpCode`	Valor del parámetro **Código ICMP**.	`0`: **Código 0** o deshabilitado. `1`: **Código 1**. `2`: **Código 2**.
`Flags`	Puntero a atributo de estructura.	Entero Se recomienda no cambiar este parámetro.
`TTL`	Valor del parámetro **Período de vida (TTL)**.	Valor en segundos. Si está deshabilitado, el valor es `0`.
`</key>`		
`Id`	Id. principal del recurso (consulte el nodo `Rules`).	Entero
`ParentID`	Id. del grupo primario.	Entero Se recomienda no cambiar este parámetro.
`Flags`	Estado de la regla.	`6`: la regla está deshabilitada. `38`: la regla está habilitada.
`Name`	Nombre de la regla de paquetes de red.	Cadena

Administración de reglas de red para aplicaciones

Por defecto, Kaspersky Endpoint Security agrupa todas las aplicaciones instaladas en el equipo por el nombre del proveedor de software cuya actividad de archivos o red se supervisa. A su vez, los grupos de aplicaciones se categorizan en grupos de confianza. Todas las aplicaciones y grupos de aplicaciones heredan propiedades de su grupo principal: reglas de control de aplicaciones, reglas de red para aplicaciones y su prioridad de ejecución.

Al igual que el componente Prevención de intrusiones en el host, de forma predeterminada, el componente Firewall aplica las reglas de red para un grupo de aplicaciones al filtrar la actividad de red de todas las aplicaciones dentro del grupo. Las reglas de red del grupo de aplicaciones definen los permisos de las aplicaciones del grupo para el acceso a diferentes conexiones de red.

Por defecto, el Firewall crea un conjunto de reglas de red para cada grupo de aplicaciones detectado por Kaspersky Endpoint Security en el equipo. Puede cambiar la acción que el Firewall aplica a las reglas de red del grupo de aplicaciones creadas por defecto. No puede editar, eliminar, deshabilitar ni modificar la prioridad de las reglas de red del grupo de aplicaciones creadas por defecto.

También puede crear una regla de red para una aplicación en particular. Dicha regla tendrá una prioridad más alta que la regla de red del grupo al cual pertenece la aplicación.

Creación de una regla de red para una aplicación

Por defecto, la actividad de una aplicación se controla mediante las reglas de red definidas para su grupo de confianza. El grupo de confianza de una aplicación se determina cuando esta se ejecuta por primera vez. En función de sus necesidades, puede crear reglas de red para todo un grupo de confianza, para una aplicación en particular o para un grupo de aplicaciones que pertenezcan a un grupo de confianza determinado.

Las reglas de red que se definen manualmente tienen mayor prioridad que las que se han determinado para un grupo de confianza. En otras palabras, cuando una aplicación está alcanzada por una regla definida manualmente y por una regla definida para su grupo de confianza, Firewall controla la actividad de la aplicación basándose en la regla definida manualmente.

De manera predeterminada, 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 aplica las reglas predefinidas del siguiente modo para controlar la actividad de red de las aplicaciones:

- De confianza y Restricción mínima: se permite todo tipo de actividad de red.
- Restricción máxima y No confiables: no se permite ningún tipo de actividad de red.

Las reglas predefinidas no se pueden editar ni eliminar.

Si necesita crear una regla de red para una aplicación, cuenta con distintos métodos:

- Utilizar la herramienta Monitor de red.

  El *Monitor de red* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de red del equipo de un usuario. Si opta por utilizar esta herramienta, no necesitará configurar todos los ajustes de la regla. Algunos de los ajustes de Firewall se tomarán de los datos del Monitor de red y se insertarán automáticamente. Para usar el Monitor de red, debe tener acceso a la interfaz de la aplicación.

- Configurar los ajustes de Firewall.

  Este método permite configurar cada parámetro de Firewall en detalle. Podrá crear reglas que cubran cualquier clase de actividad de red, aunque se trate de tráfico que no se haya registrado al momento de crear la regla.

A la hora de crear una regla de red para una aplicación, no olvide que estas tienen menor prioridad que las reglas de paquetes de red.

Cómo usar la herramienta Monitor de red desde la interfaz de la aplicación para crear una regla de red para una aplicación

1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Monitor de red**.
2. Vaya a la pestaña **Actividad de red** o la pestaña **Puertos abiertos**.

   En la ficha **Actividad de red** se muestran todas las conexiones de red actuales del equipo. Se muestran las conexiones de red entrantes y salientes.

   La ficha **Puertos abiertos** enumera todos los puertos de red del equipo que se encuentran abiertos.
3. En el menú contextual de una conexión de red, seleccione **Crear una regla de red para una aplicación**.

   Se abre la ventana de propiedades y reglas de la aplicación.
4. Seleccione la ficha **Reglas de red**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
5. Haga clic en **Agregar**.

   Se abren las propiedades de la regla de red.
6. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el vínculo **Plantilla de regla de red**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
8. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
9. Haga clic en **Guardar**.

   La nueva regla de red se agregará a la lista.
10. Utilice los botones **Subir/Abajo** para configurar la prioridad de la regla de red.
11. Guarde los cambios.

Cómo crear una regla de red para una aplicación desde la configuración de Firewall en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en **Reglas para aplicaciones**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.

4. En la lista de aplicaciones, seleccione la aplicación (o el grupo de aplicaciones) a la que corresponderá la nueva regla de red.

5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la ficha **Reglas de red**.

7. Haga clic en **Agregar**.

   Se abren las propiedades de la regla de red.

8. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.

9. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el vínculo **Plantilla de regla de red**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.

10. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

11. Haga clic en **Guardar**.

    La nueva regla de red se agregará a la lista.

12. Utilice los botones **Subir/Abajo** para configurar la prioridad de la regla de red.

13. Guarde los cambios.

Cómo crear una regla de red para una 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.

4. En el bloque **Configuración de Firewall**, haga clic en el botón **Configuración**.

   Se abre una lista con las reglas de paquetes de red y otra lista con las reglas de red para aplicaciones.

5. Vaya a la pestaña **Reglas de red de aplicaciones**.

6. Haga clic en **Agregar**.

7. En la ventana que se abre, ingrese un criterio para buscar la aplicación a la que corresponderá la nueva regla de red.

   Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

8. Haga clic en **Actualizar**.

   Kaspersky Endpoint Security buscará la aplicación en una lista consolidada, en la que se recogen las aplicaciones instaladas en los equipos administrados. Las aplicaciones que coincidan con los criterios de búsqueda se mostrarán en una lista.

9. Seleccione la aplicación necesaria.

10. En la lista desplegable **Agregar la aplicación seleccionada al grupo de confianza**, seleccione **Grupos por defecto** y haga clic en **Aceptar**.

    La aplicación se agregará al grupo por defecto.

11. Seleccione la aplicación de su interés, abra al menú contextual de la misma y haga clic en el elemento **Derechos de aplicaciones**.

    Se abre la ventana de propiedades y reglas de la aplicación.

12. Seleccione la ficha **Reglas de red**.

    Se abre una lista con las reglas de red que Firewall establece por defecto.

13. Haga clic en **Agregar**.

    Se abren las propiedades de la regla de red.

14. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.

15. Configure los parámetros de la regla de red (vea la tabla de más abajo).

    Si hace clic en el botón , podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de las reglas de red se completará automáticamente.

16. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

17. Guarde la nueva regla de red.

18. Utilice los botones **Subir/Bajar** para configurar la prioridad de la regla de red.

19. Guarde los cambios.

Cómo crear una regla de red para una 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 ficha **Configuración de la aplicación**.

4. Seleccione **Comunicación y Protección web** → **Firewall**.

5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.

6. Vaya a la pestaña **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.

7. En el bloque **Aplicaciones**, haga clic en el botón **Agregar**.

   Se inicia un asistente para agregar la aplicación a un grupo de confianza.

8. Seleccione el grupo de confianza correspondiente para la aplicación.

9. Seleccione el tipo **Aplicación**. Vaya al siguiente paso.

   Si desea crear una regla de red para más de una aplicación, seleccione el tipo **Grupo** y escriba un nombre para el grupo de aplicaciones.

10. En la lista de aplicaciones, seleccione las aplicaciones a las que corresponderá la nueva regla de red.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

11. Salga del Asistente.

    La aplicación se agregará al grupo de confianza.

12. En la parte izquierda de la ventana, seleccione la aplicación de su interés.

13. En la parte derecha de la ventana, dentro de la lista desplegable, elija el elemento **Reglas de red**.

    Se abre una lista con las reglas de red que Firewall establece por defecto.

14. Haga clic en **Agregar**.

    Se abren las propiedades de la regla.

15. Ingrese manualmente el nombre del servicio de red en el campo **Nombre de la regla**.

16. Configure los parámetros de la regla de red (vea la tabla de más abajo).

    Si hace clic en el vínculo **Seleccionar plantilla de regla**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de las reglas de red se completará automáticamente.

17. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

18. Guarde la regla de red.

    La nueva regla de red se agregará a la lista.

19. Utilice el botón **Mover** para establecer la prioridad de la regla de red.

20. Guarde los cambios.

Parámetros de las reglas red para aplicaciones

Parámetro	Descripción
Acción	**Permitir**. **Bloquear**.
Protocolo	Controle la actividad de la red en el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE. Si se selecciona ICMP o ICMPv6 como protocolo, puede definir el tipo y el código del paquete ICMP. Si selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto que usarán el equipo local y el equipo remoto para establecer la conexión a supervisar. Rango de valores posibles para los números de puerto: 0–65535. En cada campo, puede ingresar varios valores separados por `,` o especificar un rango de valores usando `-`. Por ejemplo: • `100,101` • `100-130` • `100,110-130`
Sentido	**Entrante**. **Entrante/Saliente**. **Saliente**.

Parámetro	Descripción
Direcciones remotas	Direcciones de red asignadas a equipos remotos que pueden enviar y recibir paquetes de red. Firewall aplicará la regla de red a las direcciones de red remotas que estén dentro del intervalo especificado. Puede optar por incluir todas las direcciones IP en una regla de red, crear una lista de direcciones IP separada, especificar un rango de direcciones IP o seleccionar una subred (Redes de confianza, Redes locales o Redes públicas). También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos de red LAN o servicios internos. La interacción con los servicios en la nube (como Microsoft Azure) y otros recursos de Internet debe ser procesado por el componente Control web. Si en la regla de paquete de red agregó un nombre DNS para el cual no se pudo determinar la dirección IP, Kaspersky Endpoint Security mostrará una advertencia. En la lista de reglas de paquetes de red en Web Console, se agrega una columna con una descripción del error. En la Consola de administración (MMC), la descripción del error no está disponible. Este tipo de reglas de paquetes están resaltadas en color.
Direcciones locales	Direcciones de red asignadas a equipos que pueden enviar y recibir paquetes de red. Firewall aplica una regla de red al rango especificado de direcciones de redes locales. Puede optar por incluir todas las direcciones IP en una regla de red, crear una lista de direcciones IP separada o especificar un rango de direcciones IP. La aplicación almacena las direcciones locales solo si se especifica una lista de direcciones remotas. Es decir, se seleccionó el valor **Direcciones de la lista** para **Direcciones remotas** y se agregó al menos una dirección. A veces no puede obtenerse la dirección local para las aplicaciones. Cuando esto ocurre, este parámetro no se tiene en cuenta.

Activación y desactivación de una regla de red para aplicaciones

Para habilitar o deshabilitar una regla de red para aplicaciones:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **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 cual quiera crear o editar una regla de red.
5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la ficha **Reglas de red**.
7. En la lista de reglas de red para un grupo de aplicaciones, seleccione la regla de red relevante.

   Se abre la ventana de propiedades de la regla de red.
8. Configure el estado **Activo** o **Inactivo** de la regla de red.

   No se puede deshabilitar una regla de red de un grupo de aplicaciones creada por el Firewall de manera predeterminada.
9. Guarde los cambios.

Cambio de la acción del Firewall para una regla de red para aplicaciones

Puede modificar la acción del Firewall que se aplica a todas las reglas de red correspondientes a una aplicación o a un grupo de aplicaciones que se crearon por defecto, y modificar la acción del Firewall para una sola regla de red personalizada para una aplicación o un grupo de aplicaciones.

Para cambiar la acción del Firewall para todas las reglas de red correspondientes a una aplicación o a un grupo de aplicaciones:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en **Reglas para aplicaciones**.

   Esto abre la lista de reglas de la aplicación.
4. Si quiere cambiar la acción del Firewall que se aplica a todas las reglas de red que se crearon de forma predeterminada, seleccione una aplicación o un grupo de aplicaciones en la lista. Las reglas de red creadas manualmente no se modifican.
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 del Firewall para una regla de red correspondiente a una aplicación o a un grupo de aplicaciones:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **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 cual quiera cambiar la acción correspondiente a una regla de red.
5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la ficha **Reglas de red**.
7. Seleccione la regla de red para la cual quiera cambiar la acción del Firewall.

8. En la columna **Permiso**, haga clic con el botón derecho para mostrar el menú contextual y seleccione la acción que desea asignar:
   - **Heredar**.
   - **Permitir**.
   - **Denegar**.
   - **Registrar eventos**.
9. Guarde los cambios.

Cambio de la prioridad de una regla de red para aplicaciones

La prioridad de una regla de red es determinada por su posición en la lista de reglas de red. El Firewall ejecuta las reglas en el orden en el que aparecen en la lista de reglas de red, de arriba a abajo. Según cada regla de red procesada que corresponde a una conexión de red específica, el Firewall permite o bloquea el acceso de red a la dirección y al puerto que se indican en la configuración de dicha conexión de red.

Las reglas de red creadas manualmente tienen una prioridad más alta que las predeterminadas.

No puede cambiar la prioridad de las reglas de red para un grupo de aplicaciones creadas por defecto.

Para cambiar la prioridad de una regla de red:

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección básica contra amenazas** → **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 cual quiera cambiar la prioridad de una regla de red.
5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.
   Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la ficha **Reglas de red**.
7. Seleccione la regla de red cuya prioridad quiera cambiar.
8. Utilice los botones **Subir**/**Abajo** para configurar la prioridad de la regla de red.
9. Guarde los cambios.

Monitor de red

El *Monitor de red* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de red del equipo de un usuario.

Para iniciar el Monitor de red:

En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Monitor de red**.

Se abre la ventana Monitor de red. En esta ventana, se muestra la información sobre la actividad de red del equipo en cuatro fichas:

- En la ficha **Actividad de red** se muestran todas las conexiones de red actuales del equipo. Se muestran las conexiones de red entrantes y salientes. Desde esta ficha también se pueden crear las reglas de paquetes de red con las que opera el Firewall.
- La ficha **Puertos abiertos** enumera todos los puertos de red del equipo que se encuentran abiertos. Desde esta ficha también se pueden crear las reglas de paquetes de red y las reglas para aplicaciones con las que opera el Firewall.
- En la ficha **Tráfico de red** se muestra el volumen del tráfico de red entrante y saliente entre el equipo del usuario y otros equipos de la red a la cual se encuentre conectado el usuario.
- En la pestaña **Equipos bloqueados** se enumeran las direcciones IP de los equipos remotos cuya actividad de red está bloqueada por el componente Protección contra amenazas de red después de detectar intentos de ataques de red desde estas 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. Por ejemplo, los exploits pueden utilizar un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malintencionado. 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 podrían representar una amenaza para la seguridad del equipo. La aplicación recibe información sobre dichos procesos y las bases de datos antivirus.

Habilitación y deshabilitación de la Prevención de exploits

De manera predeterminada, la Prevención de exploits está habilitada y funciona en modo óptimo. Kaspersky Endpoint Security supervisa los archivos ejecutables que ejecutan las aplicaciones vulnerables. Si Kaspersky Endpoint Security detecta que no fue el usuario quien ejecutó un archivo de una aplicación vulnerable, Kaspersky Endpoint Security realizará la acción seleccionada (por ejemplo, bloqueará la operación).

Cómo habilitar o deshabilitar la 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Prevención de exploits**.
4. Utilice la casilla **Prevención de exploits** para habilitar o deshabilitar el componente.
5. Seleccione la acción correspondiente en el bloque **Al detectarse un exploit**:
   - **Bloquear**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.
   - **Informar**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security, registra una entrada con información del exploit y agrega información sobre este exploit a la lista de amenazas activas.
6. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la Prevención de exploits en Web Console y Cloud Console

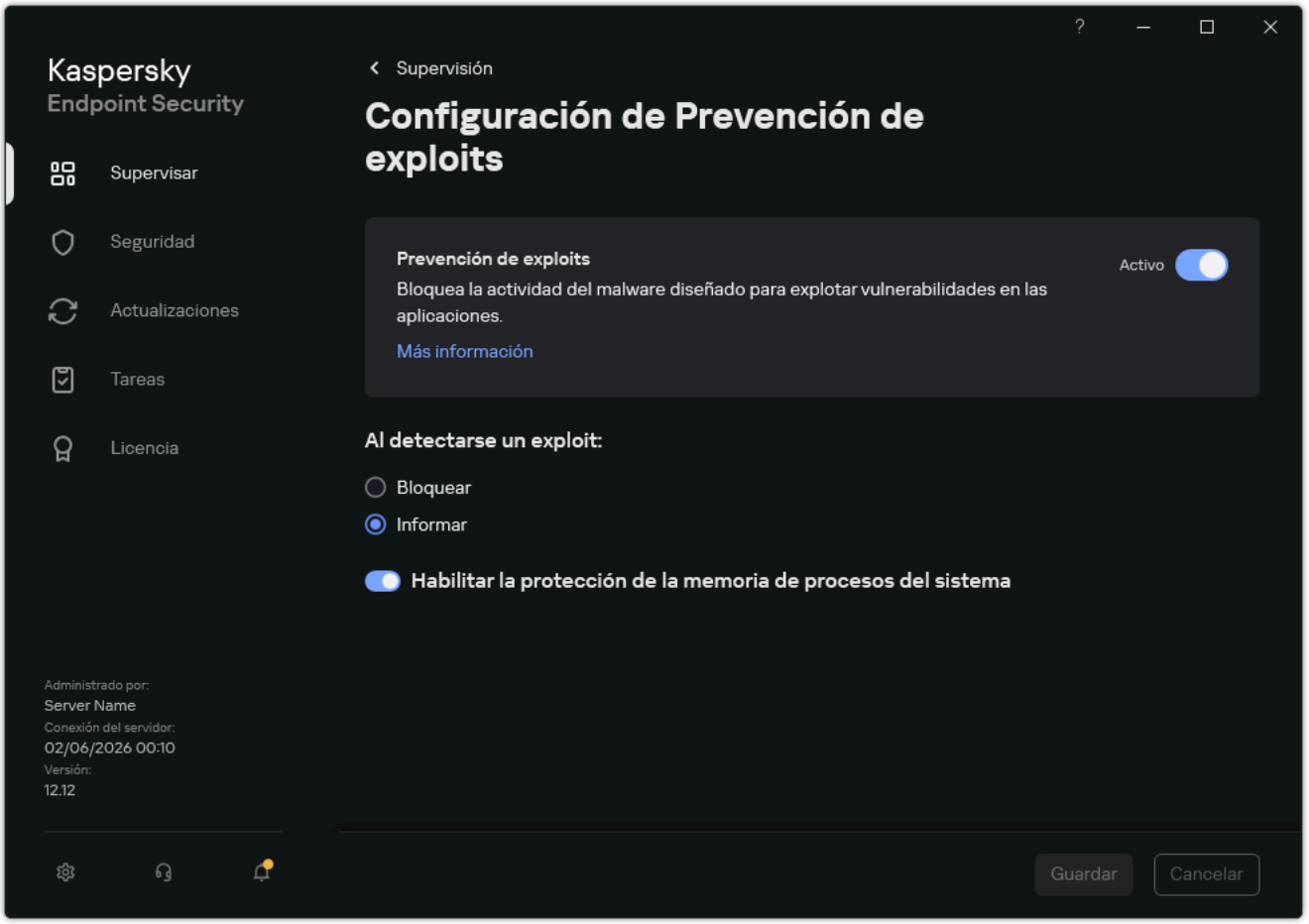
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Prevención de exploits**.
5. Use el interruptor **Prevención de exploits** para habilitar o deshabilitar el componente.
6. Seleccione la acción correspondiente en el bloque **Acción al detectar una amenaza**:
   - **Bloquear**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.
   - **Informar**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security, registra una entrada con información del exploit y agrega información sobre este exploit a la lista de amenazas activas.
7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la Prevención de exploits en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de exploits**.



Configuración de Prevención de exploits

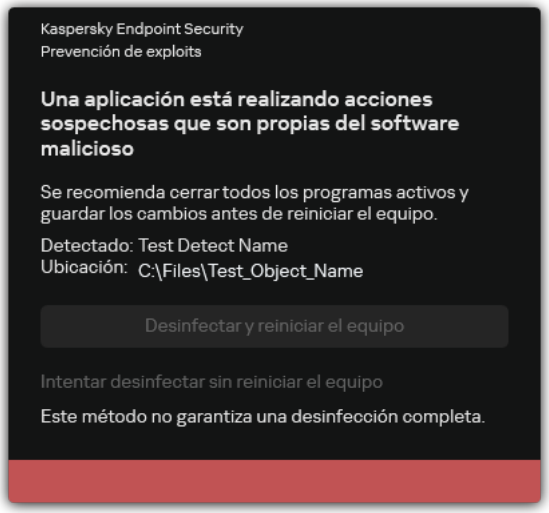
3. Use el interruptor **Prevención de exploits** para habilitar o deshabilitar el componente.

4. Seleccione la acción correspondiente en el bloque **Al detectarse un exploit**:

   - **Bloquear**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.

   - **Informar**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security, registra una entrada con información del exploit y agrega información sobre este exploit a la lista de amenazas activas.

5. Guarde los cambios.



Notificación sobre amenazas activas

Protección de la memoria de procesos del sistema

De manera predeterminada, la protección de la memoria de procesos del sistema está habilitada. Kaspersky Endpoint Security bloquea los procesos externos que intentan acceder a los procesos del sistema.

Cómo habilitar o deshabilitar la protección de la memoria de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Prevención de exploits**.

4. Utilice la casilla **Habilitar la protección de la memoria de procesos del sistema** para habilitar o deshabilitar la opción.

5. Guarde los cambios.

Cómo habilitar o deshabilitar la protección de la memoria de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Prevención de exploits**.

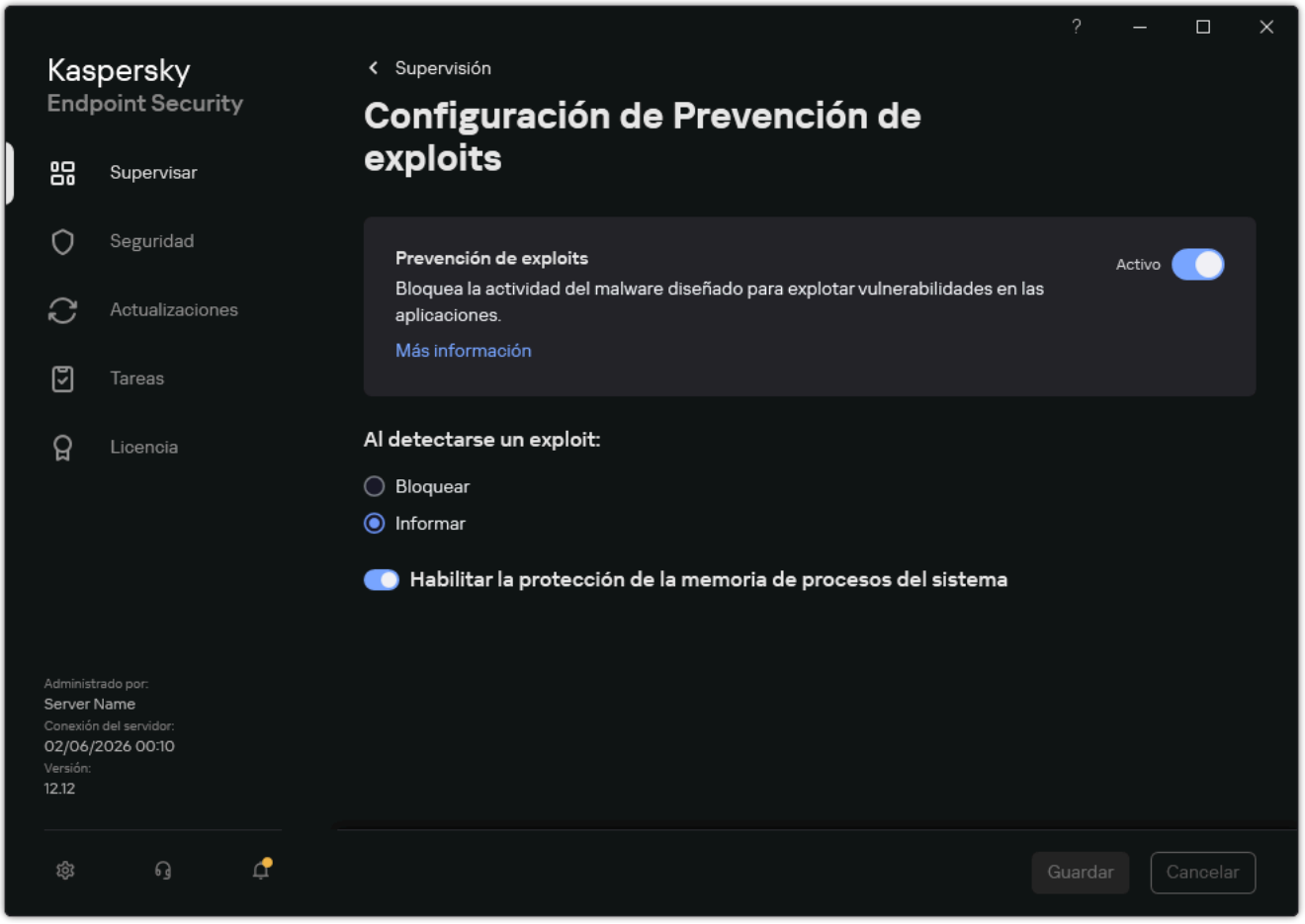
5. Utilice el interruptor **Protección de la memoria de procesos del sistema HABILITADA** para habilitar o deshabilitar esta característica.

6. Guarde los cambios.

Cómo habilitar o deshabilitar la protección de la memoria de procesos del sistema en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Prevención de exploits**.



Configuración de Prevención de exploits

3. Utilice el interruptor **Habilitar la protección de la memoria de procesos del sistema** para habilitar o deshabilitar esta característica.

4. Guarde los cambios.

Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones del equipo y transmite esta información a los demás componentes de protección para mejorar su rendimiento. El componente Detección de comportamiento utiliza firmas de patrones de comportamiento para aplicaciones. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Endpoint Security realiza la acción de respuesta especificada. Las funcionalidades de Kaspersky Endpoint Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo.

El componente Detección de comportamiento también supervisa los puertos de red en busca de procesos de aplicaciones que podrían representar una amenaza para la seguridad del equipo. La aplicación recibe información sobre dichos procesos y las bases de datos antivirus.

De manera predeterminada, el componente Detección de comportamiento está habilitado 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 deshabilitar la Detección de comportamiento a menos que sea absolutamente necesario, ya que hacerlo reduciría la eficacia de los componentes de protección. Los componentes de protección pueden solicitar datos recopilados por el componente Detección de comportamiento para detectar amenazas.

Cómo habilitar o deshabilitar la 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
4. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Detección de comportamiento**.
5. Utilice la casilla **Detección de comportamiento** para habilitar o deshabilitar el componente.
6. Seleccione la acción correspondiente en el bloque **Acción al detectar actividad de malware**:
   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.
   - **Bloquear**. Si este elemento se encuentra seleccionado, Kaspersky Endpoint Security cierra la aplicación al detectar alguna actividad de software malintencionado.
   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Endpoint Security agrega información sobre la actividad de malware a la lista de amenazas activas.
7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Detección de comportamiento**.

5. Use el interruptor **Detección de comportamiento HABILITADA** para habilitar o deshabilitar el componente.

6. Seleccione la acción correspondiente en el bloque **Acción al detectar una amenaza**:

   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.

   - **Bloquear**. Si este elemento se encuentra seleccionado, Kaspersky Endpoint Security cierra la aplicación al detectar alguna actividad de software malintencionado.

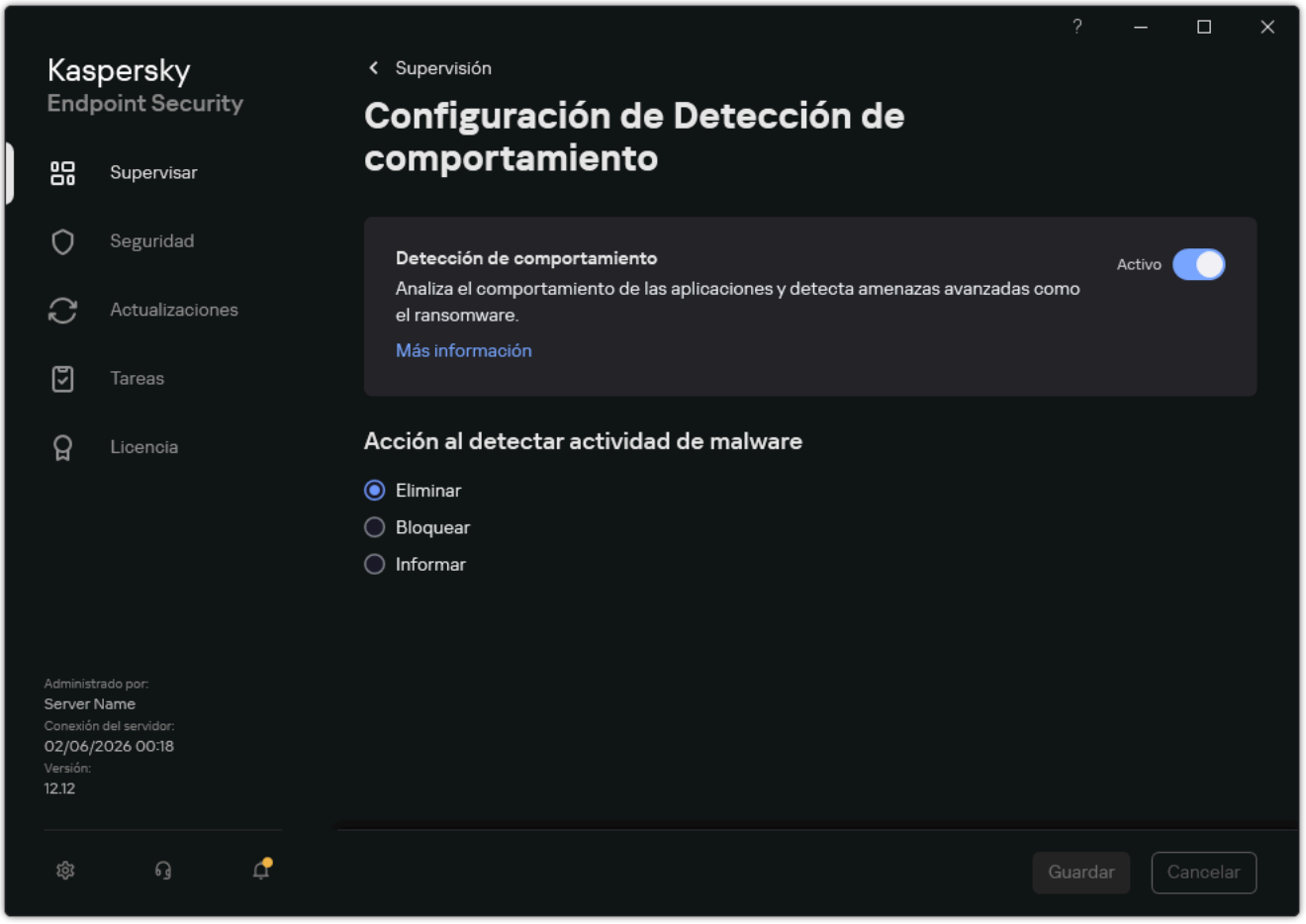
   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Endpoint Security agrega información sobre la actividad de malware a la lista de amenazas activas.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la Detección de comportamiento en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Detección de comportamiento**.



Configuración de Detección de comportamiento

3. Use el interruptor **Detección de comportamiento** para habilitar o deshabilitar el componente.

4. Seleccione la acción correspondiente en el bloque **Acción al detectar actividad de malware**:

   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.

   - **Bloquear**. Si este elemento se encuentra seleccionado, Kaspersky Endpoint Security cierra la aplicación al detectar alguna actividad de software malintencionado.

   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Endpoint Security agrega información sobre la actividad de malware a la lista de amenazas activas.

5. Guarde los cambios.

De esta manera, si la opción Detección de comportamiento está habilitada, Kaspersky Endpoint Security utilizará firmas de patrones de comportamiento para analizar la actividad de las aplicaciones en el sistema operativo.

Anticifrador

A partir de Kaspersky Endpoint Security para Windows 12.12, la protección de carpetas compartidas contra el cifrado externo que solía ser parte del componente Detección de comportamiento ahora es un componente independiente denominado Anticifrador.

Este componente supervisa solamente las operaciones realizadas con los archivos almacenados en dispositivos de almacenamiento masivo con el sistema de archivos NTFS y que no están cifrados con EFS.

El componente Anticifrador analiza la actividad en las carpetas compartidas. Cuando la actividad coincide con una firma de patrones de comportamiento que suele verse en actos de cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.

Para que funcione el componente Anticifrador, debe habilitar 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 del archivo para la sesión que originó la actividad maliciosa (el archivo será de solo lectura).
- Crea copias de seguridad de los archivos que se están modificando.
- Agrega 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 habilitado, los archivos modificados se restaurarán de sus copias de seguridad.

Habilitación y deshabilitación de la protección de carpetas compartidas contra el cifrado externo

De manera predeterminada, la protección de carpetas compartidas contra el cifrado externo está habilitada y funciona según las recomendaciones de especialistas de Kaspersky. Para configurar esta funcionalidad, puede crear un alcance de la protección y configurar exclusiones, si es necesario. De manera 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 archivos de forma externa en carpetas compartidas, Kaspersky Endpoint Security bloquea la sesión del usuario remoto durante una hora (de manera predeterminada).

Después de instalar Kaspersky Endpoint Security, la protección de carpetas compartidas contra cifrado externo será limitada hasta que se reinicie el equipo.

Cómo habilitar o deshabilitar la protección de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.

4. Utilice la casilla de verificación **Anticifrador** para habilitar o deshabilitar la detección de actividad típica del cifrado externo.

5. Seleccione la acción relevante que tomará la aplicación cuando se detecte un intento de modificar archivos en carpetas compartidas:

   - **Bloquear conexión por N min**. Si se elige esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación se habilita y la opción **Bloquear conexión por N minutos** se selecciona, los archivos modificados se restauran desde copias de seguridad.

   - **Informar**. Si esta opción está seleccionada, al detectar un intento de modificar archivos en carpetas compartidas, Kaspersky Endpoint Security agrega información sobre este intento a la lista de amenazas activas, agrega una entrada a los 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 un alcance de la protección y defina exclusiones.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la protección de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Anticifrador**.

5. Utilice el interruptor **Anticifrador HABILITADO** para habilitar o deshabilitar la detección de actividad típica del cifrado externo.

6. Seleccione la acción relevante que tomará la aplicación cuando se detecte un intento de modificar archivos en carpetas compartidas:

   - **Bloquear conexión por (min) N min**. Si se elige esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación se habilita y la opción **Bloquear conexión por (min) N minutos** se selecciona, los archivos modificados se restauran desde copias de seguridad.

   - **Informar**. Si esta opción está seleccionada, al detectar un intento de modificar archivos en carpetas compartidas, Kaspersky Endpoint Security agrega información sobre este intento a la lista de amenazas activas, agrega una entrada a los 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 un alcance de la protección y defina exclusiones.

8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar la protección de carpetas compartidas contra el cifrado externo en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.

3. Utilice la casilla de verificación **Protección de carpetas compartidas contra el cifrado externo** para habilitar o deshabilitar la detección de actividad típica del cifrado externo.

4. Utilice la casilla de verificación **Protección de carpetas compartidas contra el cifrado externo** para habilitar o deshabilitar la detección de actividad típica del cifrado externo.

5. Seleccione la acción relevante que tomará la aplicación cuando se detecte un intento de modificar archivos en carpetas compartidas:

   - **Bloquear conexión por (min) N min**. Si se elige esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación se habilita y la opción **Bloquear conexión por (min) N minutos** se selecciona, los archivos modificados se restauran desde copias de seguridad.

   - **Informar**. Si esta opción está seleccionada, al detectar un intento de modificar archivos en carpetas compartidas, Kaspersky Endpoint Security agrega información sobre este intento a la lista de amenazas activas, agrega una entrada a los 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 un alcance de la protección y defina exclusiones.

7. Guarde los cambios.

Configuración del período de bloqueo de un equipo no confiable

Un *equipo no confiable* es un equipo remoto que forma parte de actividades maliciosas o cifrado de datos. De manera predeterminada, Kaspersky Endpoint Security bloquea la sesión del usuario remoto durante una hora. Cuando el período de bloqueo caduca, 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 no confiable 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.
4. En el bloque **Acción al detectar una amenaza**, seleccione **Bloquear conexión por (N) min**.
5. Configure el período de bloqueo de un equipo no confiable que forme parte de actividades maliciosas o del cifrado de datos.
6. Guarde los cambios.

Cómo configurar el período de bloqueo de un equipo no confiable 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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Anticifrador**.
5. En **Acción al detectar una amenaza**, configure el período de bloqueo de un equipo no confiable que forme parte de actividades maliciosas o cifrado de datos.
6. Guarde los cambios.

Cómo configurar el período de bloqueo de un equipo no confiable en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.
3. En el bloque **Acción al detectar una amenaza**, seleccione **Bloquear conexión por (min)**.
4. Configure el período de bloqueo de un equipo no confiable que forme parte de actividades maliciosas o del cifrado de datos.
5. Guarde los cambios.

Como resultado, el equipo remoto se bloqueará. Para desbloquear el equipo remoto, puede reiniciar Kaspersky Endpoint Security.

Editar el alcance de la protección

El *alcance de la 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 ingresar una máscara. De manera predeterminada, la aplicación identifica automáticamente las carpetas compartidas y supervisa la actividad de los archivos en todas las carpetas.

Excluir una carpeta del alcance de la protección puede reducir la cantidad de falsos positivos si su organización utiliza el cifrado de datos cuando se intercambian archivos utilizando carpetas compartidas. Por ejemplo, Detección de comportamiento puede generar falsos positivos cuando el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Dicha actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, agregue esa carpeta a las exclusiones.

> También puede excluir equipos de los que no se deben gestionar intentos de cifrado externo.

Cómo editar el alcance de la 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.
4. En el bloque **Alcance de la protección**, seleccione **Solo las carpetas compartidas especificadas**.
5. En la lista de carpetas, haga clic en **Agregar**.
6. Esto abre una ventana. En esa ventana, ingrese la ruta a la carpeta compartida que desee incluir en el alcance de la protección (por ejemplo, `C:\Share`).

   > Para agregar una carpeta compartida al alcance de la protección, use una ruta de acceso local.

7. Haga clic en **Aceptar**.
8. Si es necesario, defina las exclusiones del alcance de la protección:

   a. En el bloque **Exclusiones de análisis**, haga clic en el botón **Por máscara**.

   b. En la ventana que se abre, haga clic en el botón **Agregar**.

   c. En la ventana que se muestra, especifique una extensión de archivo en el formato `*.<file extension>` o la ruta de acceso a una carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar 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 del análisis sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, desactive la casilla ubicada junto al objeto.

9. Guarde los cambios.

Cómo editar un alcance de la protección con 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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Anticifrador**.
5. En el bloque **Alcance de la protección**, seleccione **Solo las carpetas compartidas especificadas**.
6. En la lista de carpetas, haga clic en **Agregar**.
7. Esto abre una ventana. En esa ventana, ingrese la ruta a la carpeta compartida que desee incluir en el alcance de la protección (por ejemplo, `C:\Share`).

   > Para agregar una carpeta compartida al alcance de la protección, use una ruta de acceso local.

8. Haga clic en **Aceptar**.
9. Si es necesario, defina las exclusiones del alcance de la 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 **Agregar**.

   c. En la ventana que se muestra, especifique una extensión de archivo en el formato `*.<file extension>` o la ruta de acceso a una carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar 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 del análisis sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, desactive la casilla ubicada junto al objeto.

10. Guarde los cambios.

Cómo editar el alcance de la protección en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.
3. En el bloque **Alcance de la protección**, seleccione **Solo las carpetas compartidas especificadas**.
4. En la lista de carpetas, haga clic en **Agregar**.

5. Esto abre una ventana. En esa ventana, ingrese la ruta a la carpeta compartida que desee incluir en el alcance de la protección (por ejemplo, `C:\Share`).

   > Para agregar una carpeta compartida al alcance de la protección, use una ruta de acceso local.

6. Haga clic en **Aceptar**.

7. Si es necesario, defina las exclusiones del alcance de la 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 **Agregar**.

   c. En la ventana que se muestra, especifique una extensión de archivo en el formato `*.<file extension>` o la ruta de acceso a una carpeta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar 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 del análisis sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, desactive la casilla ubicada junto al objeto.

8. Guarde los cambios.

1. En la ventana principal de la aplicación 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 vínculo **Administrar exclusiones**.

4. Haga clic en **Agregar**.

5. Haga clic en **Examinar** y seleccione la carpeta compartida.

   También puede escribir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara:

   - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

   - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

6. En el bloque **Componentes de protección**, seleccione el componente **Detección de comportamiento**.

7. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

8. Seleccione el estado **Activo** para la exclusión.

   Puede usar 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 ficha **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 de malware**.

6. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.

7. Seleccione la casilla **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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Endpoint Security oculta la lista consolidada de exclusiones de análisis en la interfaz de usuario de la aplicación.

8. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega 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 agregaron exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las exclusiones de análisis predefinidas según el propósito del servidor protegido.

9. Seleccione cómo desea agregar la exclusión **Ruta al archivo o carpeta**.

10. Ingrese la ruta de la carpeta compartida.

También puede escribir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `C:\Users\*\Folder\`.

11. En el bloque **Aplicar exclusión a**, seleccione el componente **Detección de comportamiento**.

12. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

13. Seleccione el estado **Agregar a las exclusiones** para la exclusión.

    Puede usar 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 correspondiente 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 objetos**.

4. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Exclusiones de análisis**, haga clic en el botón **Configuración**.

   Esto abre una ventana que contiene una lista de exclusiones.

5. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.

6. Seleccione la casilla **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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Endpoint Security oculta la lista consolidada de exclusiones de análisis en la interfaz de usuario de la aplicación.

7. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega 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 agregaron exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las exclusiones de análisis predefinidas según el propósito del servidor protegido.

8. Haga clic en **Agregar**.

9. En el bloque **Propiedades**, seleccione la casilla **Archivo o carpeta**.

10. Haga clic en el vínculo para **Seleccione el archivo o la carpeta** en el bloque **Descripción de la exclusión de análisis (haga clic en los objetos subrayados para editarlos)** para abrir la ventana **Nombre de archivo o carpeta**.

11. Haga clic en **Examinar** y seleccione la carpeta compartida.

    También puede escribir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

    - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

12. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

13. Haga clic en el vínculo del bloque **Descripción de la exclusión de análisis (haga clic en los objetos subrayados para editarlos)** para abrir la ventana **Componentes de protección**.

14. Seleccione la casilla de verificación ubicada junto al componente **Detección de comportamiento**.

15. Guarde los cambios.

Agregar equipos de confianza para el cifrado de datos externo

Si su organización utiliza cifrado de datos externo 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 realizado por equipos de confianza.

El servicio Audit Logon debe estar habilitado para permitir realizar exclusiones de direcciones desde Protección de carpetas compartidas contra el cifrado externo. De manera predeterminada, el servicio Inicio de sesión de auditoría está deshabilitado (para obtener información detallada sobre la habilitación del servicio Inicio de sesión de auditoría, visite el sitio web de Microsoft).

La funcionalidad para la exclusión de direcciones desde Protección de carpetas compartidas no funcionará en un equipo remoto si dicho equipo estaba encendido antes de iniciar Kaspersky Endpoint Security. Puede reiniciar el equipo remoto después de haber iniciado Kaspersky Endpoint Security para asegurarse de que la funcionalidad de excluir direcciones desde la protección de carpetas compartidas funcione en este equipo remoto.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de equipos de confianza. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Cómo agregar un equipo de confianza para el cifrado de datos 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.

4. En el bloque **Exclusiones de análisis**, haga clic en el botón **Por nombre o dirección IP**.

5. En la ventana que se abre, haga clic en el botón **Por nombre o dirección IP**.

6. Escriba direcciones IP, intervalos de direcciones IP o nombres de equipos desde los cuales no se deben gestionar los intentos de cifrado.

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`

7. Guarde los cambios.

Cómo agregar un equipo de confianza para el cifrado de datos 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 ficha **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Anticifrador**.
5. En la parte superior de la ventana, haga clic en el vínculo **Exclusiones por nombre o dirección IP**.
6. En la ventana que se abre, haga clic en el botón **Agregar**.
7. Escriba direcciones IP, intervalos de direcciones IP o nombres de equipos desde los cuales no se deben gestionar los intentos de cifrado.

   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. Guarde los cambios.

Cómo agregar un equipo de confianza para el cifrado de datos externo en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.
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 **Agregar**.

5. Escriba direcciones IP, intervalos de direcciones IP o nombres de equipos desde los cuales no se deben gestionar los intentos de cifrado.

   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 de la protección de carpetas compartidas contra el cifrado externo

Puede exportar la lista de exclusiones a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Anticifrador**.
4. En el bloque **Exclusiones de 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, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.

   c. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Anticifrador**.

5. Haga clic en el vínculo **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 que se usará para importar la lista de exclusiones.

   b. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

8. Guarde los cambios.

Motor de reparación

El componente Motor de reparación permite a Kaspersky Endpoint Security deshacer acciones que han sido realizadas por el malware en el sistema operativo.

Al revertir la actividad del malware en el sistema operativo, Kaspersky Endpoint Security gestiona los siguientes tipos de actividad de malware:

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto 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 eliminado o modificado.

- **Actividad del sistema**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Finaliza los procesos iniciados por el malware.
  - Finaliza los procesos en los cuales ha penetrado una aplicación malintencionada.
  - No reanuda procesos que el malware haya suspendido.

- **Actividad de la 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 las acciones del malware puede iniciarse durante un análisis de malware o a pedido de los componentes Protección contra archivos peligrosos o Detección de comportamiento.

La reversión de las operaciones del malware afecta a un conjunto de datos estrictamente definido. La reversión no tiene efectos negativos en el sistema operativo ni en la integridad de los datos de su equipo.

Cómo habilitar o deshabilitar el componente Motor de reparación 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Motor de reparación**.

4. Utilice la casilla **Motor de reparación** para habilitar o deshabilitar el componente.

5. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Motor de reparación 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 ficha **Configuración de la aplicación**.

4. Vaya a **Protección contra amenazas de host** → **Análisis de comportamiento** → **Motor de reparación**.

5. Use el interruptor **Motor de reparación HABILITADO** para habilitar o deshabilitar el componente.

6. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Motor de reparación mediante la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Motor de reparación**.

3. Use el interruptor **Motor de reparación** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

De esta manera, si la opción Motor de reparación está habilitada, 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 el software 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 los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, los servicios KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web analizadas, así como información sobre la categoría y la reputación de los archivos analizados. Para obtener más detalles sobre la configuración del acceso a KSN, consulte la Ayuda de Kaspersky Security Center.

El uso de Kaspersky Security Network es voluntario. La aplicación invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios pueden iniciar o discontinuar 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. Encontrará el texto de la Declaración de Kaspersky Security Network en el archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación.

La infraestructura de las bases de datos de reputación de Kaspersky

Kaspersky Endpoint Security da soporte a 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 detectados 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).* A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky. 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;

  - 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.

Habilitación y deshabilitación del uso de Kaspersky Security Network

De manera predeterminada, Kaspersky Endpoint Security utiliza el modo KSN extendido. El *modo KSN extendido* es un modo por el cual Kaspersky Endpoint Security remite información adicional a Kaspersky.

Cómo habilitar o deshabilitar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
4. Use el interruptor **Kaspersky Security Network** para habilitar o deshabilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte los términos de uso de la Declaración de Kaspersky Security Network (KSN) si está de acuerdo con ellos.
5. Si es necesario, anule la selección de la casilla **Habilitar el modo KSN extendido**. De manera predeterminada, el modo KSN extendido está habilitado.
6. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Kaspersky Security Network**.
5. Use el interruptor **Uso de Kaspersky Security Network (KSN) HABILITADO** para habilitar o deshabilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte los términos de uso de la Declaración de Kaspersky Security Network (KSN) si está de acuerdo con ellos.
6. De ser necesario, desactive el interruptor **Utilizar el modo KSN extendido**. De manera predeterminada, el modo KSN extendido está habilitado.
7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar el uso de KSN en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
3. Use el interruptor **Kaspersky Security Network** para habilitar o deshabilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte los términos de uso de la Declaración de Kaspersky Security Network (KSN) si está de acuerdo con ellos.

4. De ser necesario, desactive el interruptor **Habilitar el modo KSN extendido**. De manera predeterminada, el modo KSN extendido está habilitado.

5. Guarde los cambios.

De esta manera, si el uso de KSN está habilitado, Kaspersky Endpoint Security usa información sobre la reputación de los archivos, los recursos web y las aplicaciones recibida de Kaspersky Security Network.

Limitaciones de Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN). A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky. 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 agregado a la base de datos de reputación local tiene mayor prioridad que uno agregado 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 confiables* 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 confiables* y realizará 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 sin conexión. Las bases de datos de reputación sin conexión 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. Expertos de Kaspersky se encargan de crear las bases de datos de reputación sin conexión basándose en datos de Kaspersky Security Network. Las aplicaciones de Kaspersky actualizan las bases de datos de reputación sin conexión con bases de datos antivirus de la aplicación específica. Si las bases de datos de reputación sin conexión 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 usa 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 definir la configuración de optimización del análisis en la interfaz de la aplicación, por ejemplo, para el componente Protección contra archivos peligrosos.

- Kaspersky Endpoint Security en el modo de Light Agent se comunica con servidores de KSN a través de un servidor proxy de KSN. No se admite la comunicación directa con KSN.

Habilitación y deshabilitación del modo nube 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.

Al utilizar Kaspersky Private Security Network, la funcionalidad del modo nube está disponible para versiones superiores o iguales a Kaspersky Private Security Network versión 3.0.

Si la aplicación funciona en el modo de Light Agent, el modo nube no está disponible.

Cómo habilitar o deshabilitar el modo nube de los componentes 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
4. Utilice la casilla **Habilitar modo nube** para habilitar o deshabilitar el componente.
5. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar el modo nube de los componentes 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Kaspersky Security Network**.
5. Use el interruptor **Usar modo nube** para habilitar o deshabilitar el componente.
6. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar o deshabilitar el modo nube de los componentes de protección en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
3. Use el interruptor **Habilitar modo nube** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security descargará una versión ligera o una versión completa de las bases de datos antivirus durante la próxima actualización.

> Si la versión ligera de bases de datos antivirus no está disponible para ser utilizada, Kaspersky Endpoint Security cambia automáticamente la versión premium de bases de datos antivirus.

Configuración del proxy de KSN

Los equipos de usuarios administrados por el Servidor de administración de Kaspersky Security Center pueden interactuar con KSN de forma directa o a través del servicio KSN Proxy.

> Si la aplicación se ejecuta en el modo de 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 capacidades:

- El equipo del usuario puede consultar KSN y enviarle información, incluso sin 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 habilitar KSN y aceptar la declaración de KSN, la aplicación utiliza un servidor proxy para conectarse a 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. Por lo tanto, si el proxy de KSN no está disponible, debe verificar lo siguiente:

- Que el servicio `ksnproxy` se esté ejecutando 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: habilite o deshabilite el KSN Proxy y configure el puerto para la conexión. Para hacerlo, debe abrir las propiedades del Servidor de administración. Para obtener más información sobre la configuración de KSN Proxy, consulte la Ayuda de Kaspersky Security Center. También puede habilitar o deshabilitar el KSN Proxy para equipos individuales en la directiva de Kaspersky Endpoint Security.

Cómo habilitar o deshabilitar el proxy de KSN 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas** → **Kaspersky Security Network**.

4. En el bloque **Configuración del proxy de KSN**, use la casilla **Usar el Servidor de administración como servidor proxy de KSN** para habilitar o deshabilitar el proxy de KSN.

5. Si es necesario, seleccione la casilla **Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible**.

   Cuando esta casilla está activada y el servicio KSN Proxy no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network).

6. Guarde los cambios.

Cómo habilitar o deshabilitar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Kaspersky Security Network**.

5. Utilice la casilla **Usar el Servidor de administración como servidor proxy de KSN** para habilitar o deshabilitar KSN Proxy.

6. Si es necesario, seleccione la casilla **Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible**.

   Cuando esta casilla está activada y el servicio KSN Proxy no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network). De manera predeterminada, la casilla está desactivada.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

La dirección del KSN Proxy coincide con la dirección del Servidor de administración. Cuando se cambia el nombre de dominio del Servidor de administración, debe actualizar de forma manual la dirección del KSN Proxy.

Para configurar la dirección del proxy de KSN, realice lo siguiente:

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**, seleccione **Propiedades**.

4. En la pestaña **General** en la ventana abierta, especifique la nueva dirección del servidor del proxy de KSN.

5. Guarde los cambios.

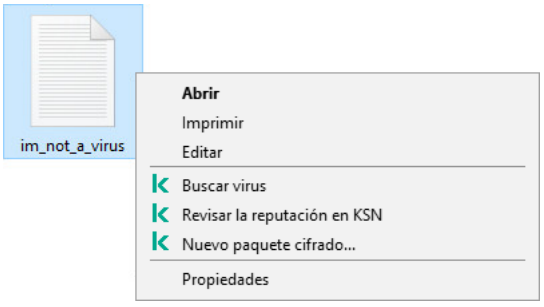
Comprobación de la reputación de un archivo en Kaspersky Security Network

Si no sabe con certeza si un archivo es seguro, puede buscar su reputación en Kaspersky Security Network.

Para buscar la reputación de un archivo, debe aceptar 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 elija la opción **Comprobar reputación en KSN** (vea la siguiente imagen).



Menú contextual del 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 cumple una o más de las siguientes condiciones:

- el archivo está firmado digitalmente por proveedores de confianza;
- el archivo tiene una reputación de confianza en Kaspersky Security Network;
- el usuario colocó el archivo en el grupo de confianza.

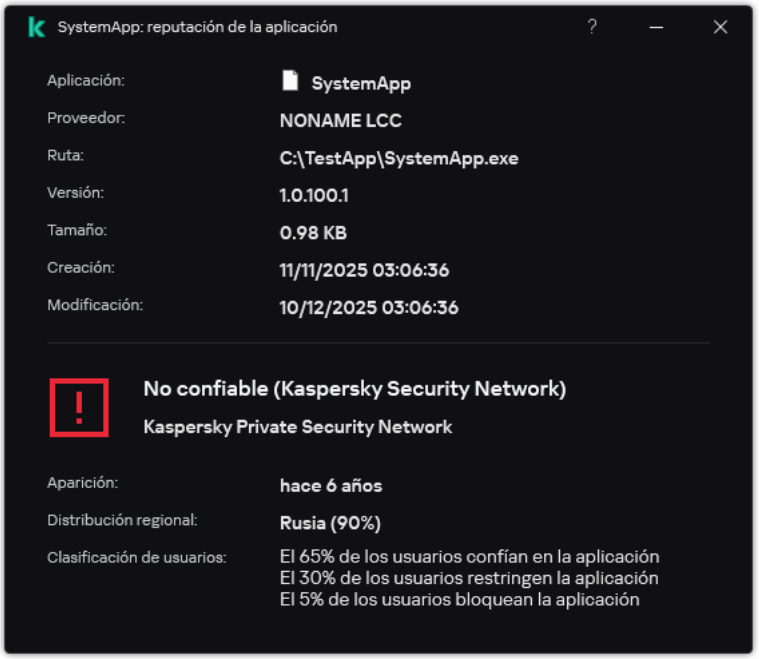
Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre el software legal que los delincuentes pueden utilizar para dañar el equipo o los datos personales de un usuario están disponibles en el sitio web de la Enciclopedia de Kaspersky. Estas aplicaciones pueden agregarse a la lista de aplicaciones de confianza.

No confiable (Kaspersky Security Network). El archivo es un virus u otra clase de aplicación que supone un riesgo.

Desconocida (Kaspersky Security Network). Kaspersky Security Network no cuenta con información sobre el archivo. Si desea analizarlo con las bases de datos antivirus, use la opción **Analizar en busca de virus** del menú contextual.

Kaspersky Endpoint Security mostrará qué solución de KSN se usó para determinar la reputación del archivo. *Kaspersky Security Network* o *Kaspersky Private Security Network*.

Kaspersky Endpoint Security también mostrará información adicional sobre el archivo (vea la siguiente imagen).



Reputación de un archivo en Kaspersky Security Network

Análisis de conexiones cifradas

Cuando termina la instalación de Kaspersky Endpoint Security, se agrega un certificado de Kaspersky al repositorio de certificados de confianza del sistema (tienda de certificados de Windows). Kaspersky Endpoint Security utiliza este certificado para analizar conexiones cifradas. El uso de este repositorio también se habilita en Firefox y Thunderbird para que el tráfico de estas aplicaciones pueda analizarse.

Los componentes Control web, Protección contra amenazas de correo, Protección contra amenazas web, Detección de comportamiento y Prevención de exploits pueden descifrar y analizar el tráfico de red que se transmite sobre conexiones cifradas en las que se utilizan los siguientes protocolos:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Cómo habilitar el análisis de conexiones cifradas

De forma predeterminada, Kaspersky Endpoint Security no siempre analiza las conexiones cifradas, solo cuando lo solicitan los componentes de protección.

Cómo habilitar 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 correspondiente 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 los sitios web cuyas direcciones comienzan con `https://`.
   - **Analizar las conexiones cifradas si lo solicitan los componentes de protección**. Kaspersky Endpoint Security analizará solo el tráfico cifrado cuando lo soliciten los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control Web.
   - **Analizar siempre las conexiones cifradas**. Kaspersky Endpoint Security analizará el tráfico de red cifrado, aunque los componentes de protección estén deshabilitados.

   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 únicamente en la interfaz de Kaspersky Endpoint Security. No puede verla en la Consola de Kaspersky Security Center.

6. De ser necesario, agregue exclusiones de análisis para las direcciones y aplicaciones que considere de confianza.
7. Configure los parámetros del análisis de conexiones cifradas (vea la tabla a continuación).
8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar 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 ficha **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 HABILITADO**.

   Si el interruptor no está activado, Kaspersky Endpoint Security no tendrá acceso al contenido de los sitios web cuyas direcciones comienzan con `https://`.

6. Haga clic en **Configuración** y seleccione el modo de análisis de conexiones cifradas:

- **Analizar las conexiones cifradas si lo solicitan los componentes de protección**.
  Kaspersky Endpoint Security analizará solo el tráfico cifrado cuando lo soliciten los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control Web.

- **Analizar siempre las conexiones cifradas**. Kaspersky Endpoint Security analizará el tráfico de red cifrado, aunque los componentes de protección estén deshabilitados.

> 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 únicamente en la interfaz de Kaspersky Endpoint Security. No puede verla en la Consola de Kaspersky Security Center.

7. De ser necesario, agregue exclusiones de análisis para las direcciones y aplicaciones que considere de confianza.

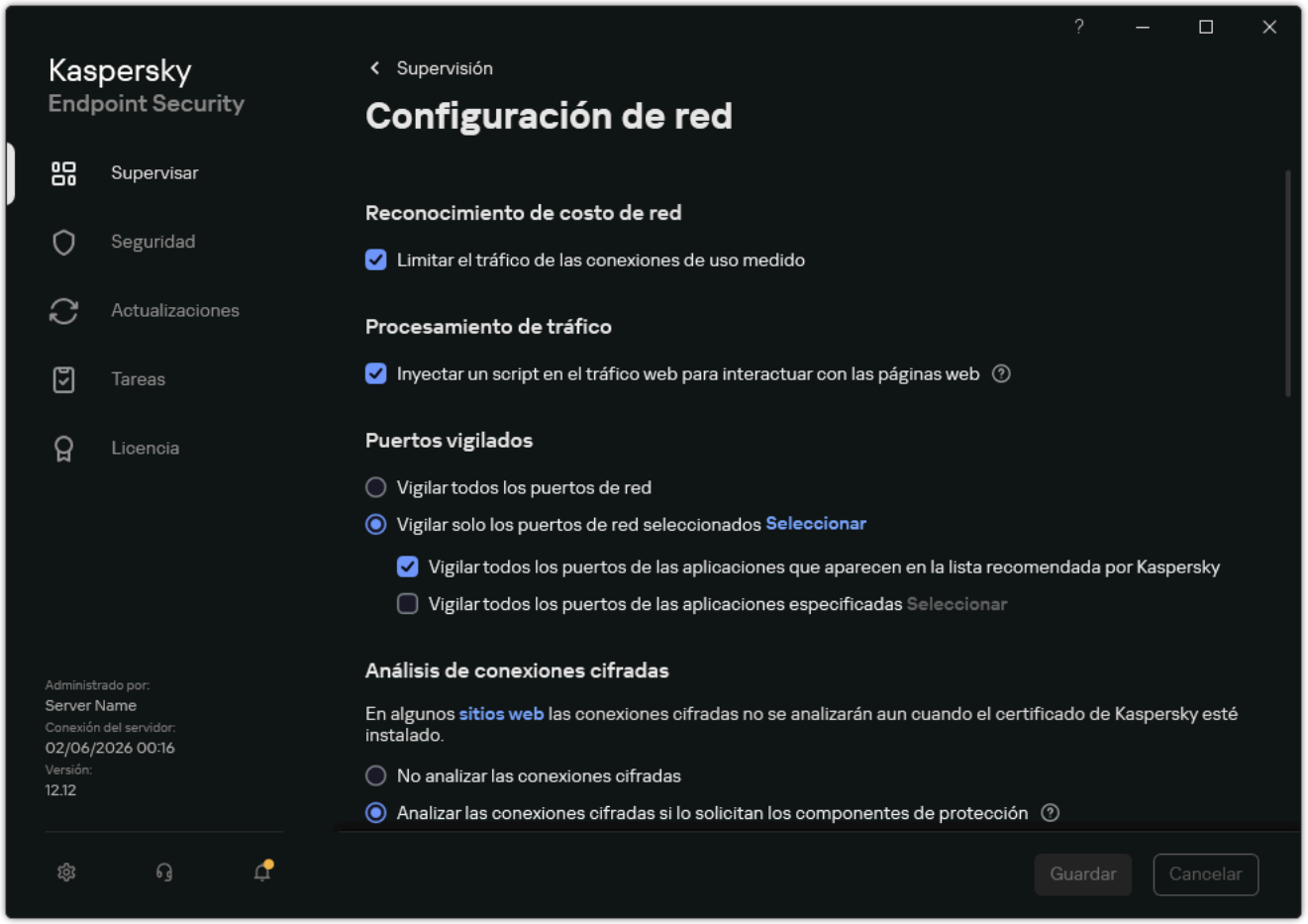
8. Configure los parámetros del análisis de conexiones cifradas (vea la tabla a continuación).

9. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar el análisis de conexiones cifradas en la interfaz de la aplicación

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

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



Parámetros 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 los sitios web cuyas direcciones comienzan con `https://`.

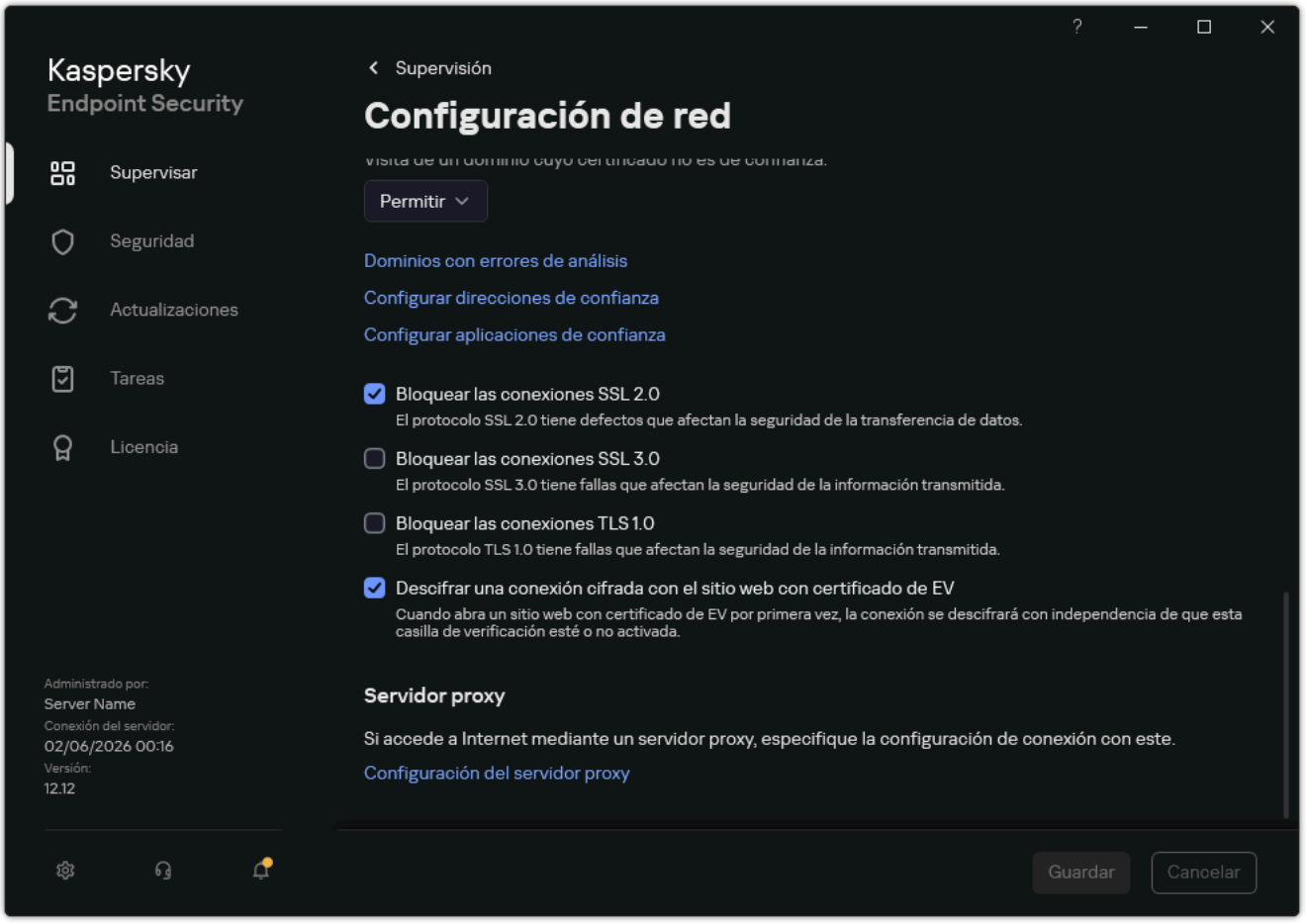
- **Analizar las conexiones cifradas si lo solicitan los componentes de protección**. Kaspersky Endpoint Security analizará solo el tráfico cifrado cuando lo soliciten los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control Web.

- **Analizar siempre las conexiones cifradas**. Kaspersky Endpoint Security analizará el tráfico de red cifrado, aunque los componentes de protección estén deshabilitados.

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 únicamente en la interfaz de Kaspersky Endpoint Security. No puede verla en la Consola de Kaspersky Security Center.

4. De ser necesario, agregue exclusiones de análisis para las direcciones y aplicaciones que considere de confianza.

5. Configure los parámetros del análisis de conexiones cifradas (vea la tabla a continuación).



Configuraciones adicionales para analizar conexiones cifradas

6. Guarde los cambios.

Parámetros del análisis de conexiones cifradas

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 agregar 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 agregar un certificado al almacén de certificados del sistema, debe utilizar directivas de grupo de Active Directory.
Visita de 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 contendrá un vínculo para obtener acceso al recurso web solicitado. Si una aplicación o un servicio de terceros establece una conexión con un dominio con un certificado no confiable, Kaspersky Endpoint Security crea su propio certificado para analizar el tráfico. El nuevo certificado tiene el estado *No confiables*. Esto es necesario para advertir a la aplicación de terceros sobre la conexión no confiable, ya que en este caso puede no mostrarse la página HTML y la conexión se puede establecer en segundo plano. • **Bloquear**. Cuando se elige esta opción y se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security bloquea 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.
Visita de un dominio con un error de análisis de conexiones cifradas	• **Bloquear**. Si se produce un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red. • **Permitir y agregar el dominio a exclusiones**. Si se produce un error al analizar una conexión cifrada, Kaspersky Endpoint Security agrega el dominio que provocó el error a la lista de dominios con errores de análisis y no supervisa el tráfico de red cifrado cuando se visita este dominio. La lista de dominios con errores de análisis 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 las conexiones SSL 2.0	Si la casilla está seleccionada, la aplicación supervisa y bloquea las conexiones de red que se establecen con el protocolo SSL 2.0. Si la casilla está desactivada, 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 las conexiones SSL 3.0	Si la casilla está seleccionada, la aplicación bloquea las conexiones de red que se establecen con el protocolo SSL 3.0. Si la casilla está desactivada, 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 las conexiones TLS 1.0	Si la casilla está seleccionada, la aplicación bloquea las conexiones de red que se establecen con el protocolo TLS 1.0. Si la casilla está desactivada, 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 una conexión cifrada con el sitio web con certificado de EV	Los certificados de EV (Extended Validation Certificate) confirman la autenticidad de los sitios web y mejoran la seguridad de la conexión. Los navegadores utilizan un icono de candado en su barra de direcciones para indicar que un sitio web tiene un certificado de validación extendida. Además, es posible que en los navegadores se vea toda la barra de direcciones en color verde o una parte de ella. Si la casilla está seleccionada, la aplicación descifra y controla las conexiones cifradas que se establecen con sitios web que utilizan certificados de EV. Cuando esta casilla no está activada, la aplicación no tiene acceso al contenido del tráfico HTTPS. Esto significa que la aplicación únicamente puede controlar el tráfico HTTPS basándose en la dirección del sitio web (por ejemplo, `https://bing.com`). Si abre un sitio web con un certificado de validación extendida por primera vez, la conexión cifrada se descifrará sin importar si se seleccionó la casilla.

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 agregar 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 agregar un certificado al almacén de certificados del sistema, debe utilizar directivas de grupo de Active Directory.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de certificados root de confianza. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

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 correspondiente 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 **Agregar**.
5. Se abre una ventana donde debe seleccionar un certificado raíz de confianza.
   Kaspersky Endpoint Security admite certificados con extensiones PEM, DER y CRT.
6. Guarde los cambios.

Cómo instalar certificados raíz 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de red**.
5. Haga clic en el vínculo **Certificados raíz de confianza**.

6. Se abre una ventana donde debe hacer clic en **Agregar** y seleccionar un certificado raíz de confianza.
   Kaspersky Endpoint Security admite 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 principal de la aplicación 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. Se abre una ventana donde debe hacer clic en **Agregar** y seleccionar un certificado raíz de confianza.
   Kaspersky Endpoint Security admite certificados con extensiones PEM, DER y CRT.
5. Guarde los cambios.

De esta manera, cuando se analiza el tráfico Kaspersky Endpoint Security utiliza su propia tienda de certificados, además de la tienda de certificados del sistema.

Análisis de conexiones cifradas con un certificado no confiable

Cuando termina la instalación de Kaspersky Endpoint Security, se agrega un certificado de Kaspersky al repositorio de certificados de confianza del sistema (tienda de certificados de Windows). Kaspersky Endpoint Security utiliza este certificado para analizar conexiones cifradas. Al visitar un dominio con un certificado no confiable, puede permitir o rechazar el acceso de los usuarios a ese dominio (consulte las instrucciones a continuación).

Si permitió 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 (consulte la figura a continuación). La página contendrá un vínculo para obtener acceso al recurso web solicitado. Una vez que el usuario hace clic en el vínculo, 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 no confiable.

  En algunos casos, Kaspersky Endpoint Security no puede mostrar técnicamente una página HTML con una advertencia en el navegador (consulte la siguiente figura). Por ejemplo, si un recurso web usa una versión desactualizada de un protocolo de red y un puerto no estándar. En esos casos, Kaspersky Endpoint Security bloquea el acceso a este dominio, y el navegador muestra la ventana estándar `ERR_CONNECTION_RESET`. Para acceder a un recurso web, puede agregar el dominio a las exclusiones o usar un certificado de confianza.

- Si *una aplicación o un servicio de terceros* establece una conexión con un dominio con un certificado no confiable, Kaspersky Endpoint Security crea su propio certificado para analizar el tráfico. El nuevo certificado tiene el estado *No confiable*. Esto es necesario para advertir a la aplicación de terceros sobre la conexión no confiable, ya que en este caso puede no mostrarse la página HTML 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 finalice 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 agregar 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 no confiable.

Cómo configurar el análisis de conexiones cifradas con un certificado no confiable 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 correspondiente 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 se visite un dominio cuyo certificado no sea de confianza: **Permitir** o **Bloquear**.
6. Guarde los cambios.

Cómo configurar el análisis de conexiones cifradas con un certificado no confiable 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de red**.

5. En el bloque **Análisis de conexiones cifradas**, haga clic en el vínculo **Configuración**.

6. En la ventana que se abre, seleccione el modo de funcionamiento de la aplicación cuando se visite un dominio cuyo certificado no sea de confianza: **Permitir conexión** o **Bloquear conexión**.

7. Guarde los cambios.

Cómo configurar el análisis de conexiones cifradas con un certificado no confiable en la interfaz de aplicación

1. En la ventana principal de la aplicación 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 se visite un dominio cuyo certificado no sea de confianza: **Permitir** o **Bloquear**.

4. Guarde los cambios.

Advertencia cuando visita un dominio cuyo certificado no es de confianza

Cómo agregar el certificado de Kaspersky a un almacén de certificados propio

Los navegadores y clientes de correo utilizan el certificado para verificar la seguridad y la 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 el almacén de certificados de confianza (almacén de certificados de Windows). Por ejemplo, Google Chrome. Algunos navegadores y clientes de correo utilizan su propio almacén de certificados de manera predeterminada en lugar del almacén de certificados de Windows. Por ejemplo, Firefox y Thunderbird.

Cuando termina la instalación de Kaspersky Endpoint Security, se agrega un certificado de Kaspersky al repositorio de certificados de confianza del sistema (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 del almacén de certificados de Windows en los navegadores y clientes de correo para analizar el tráfico de estas aplicaciones. Si no se aplica una directiva a un equipo, puede elegir el almacén de certificados que utilizarán los navegadores y clientes de correo. Si selecciona un almacén de certificados propio, agregue el certificado de Kaspersky al almacén de forma manual. 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 habilitar el Análisis de conexiones cifradas. Si el Análisis de conexiones cifradas está deshabilitado, la aplicación no analiza el tráfico del navegador Mozilla Firefox ni el cliente de correo Thunderbird. El análisis de conexiones cifradas también debe habilitarse para analizar el tráfico de los clientes de correo MyOffice Mail y R7-Office Organizer.

Antes de agregar un certificado al almacén de certificados propios del navegador o del agente de correo, exporte el certificado de Kaspersky desde el Panel de control de Windows (propiedades de Internet). Puede obtener más información acerca de cómo agregar un certificado a la tienda, por ejemplo, en el sitio web de Soporte técnico de Mozilla.

Puede elegir el almacén de certificados solo en la interfaz local de la aplicación.

Para elegir un almacén de certificados con el fin de analizar conexiones cifradas en navegadores y clientes de correo:

1. En la ventana principal de la aplicación 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 **Para analizar conexiones cifradas en aplicaciones con su almacén de certificados propios, use**.
4. Seleccione una tienda de certificados:
   - **Almacén de certificados de Windows (recomendado)**. El certificado raíz de Kaspersky se agrega a esta tienda durante la instalación de Kaspersky Endpoint Security.
   - **Almacén de certificados propios**. Mozilla Firefox y Thunderbird utilizan sus propios almacenes de certificados. Si se selecciona el almacén de certificados de Mozilla, debe agregar manualmente el certificado raíz de Kaspersky a este almacén a través de las propiedades del navegador.

     Los clientes de correo MyOffice Mail y R7-Office Organizer también usan su propio almacén de certificados.
5. Guarde los cambios.

Creación de exclusiones para el análisis de conexiones cifradas

La mayoría de los recursos web utilizan conexiones cifradas. Los especialistas de Kaspersky recomiendan habilitar la característica de análisis de conexiones cifradas. Si descubre que esta función interfiere con su trabajo, puede agregar las direcciones de los sitios web con los que tenga problemas como *direcciones de confianza*; al hacerlo, esos sitios web quedarán excluidos del análisis. En este caso, Kaspersky Endpoint Security no analiza el tráfico HTTPS de las direcciones web de confianza cuando los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control web están haciendo su trabajo.

De manera similar, si una aplicación que considera fiable utiliza una conexión cifrada, puede deshabilitar el análisis de conexiones cifradas para la misma. Un caso típico que puede requerir una exclusión sería el de una aplicación de almacenamiento en la nube que utilice su propio certificado para la autenticación de dos factores.

> Las propiedades de la directiva principal pueden bloquear la modificación de la lista de direcciones de confianza. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

> Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Cómo excluir una dirección web de los análisis de conexiones cifradas 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 correspondiente 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 **Configurar direcciones de confianza**.
5. Haga clic en **Agregar**.
6. Escriba 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 ingresar una máscara en el nombre de dominio.

   > Kaspersky Endpoint Security no admite el símbolo `*` para direcciones IP. Puede seleccionar un intervalo de direcciones IP con 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 no incluye 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 no incluye el dominio `domain.com`.
   - `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro no incluye el dominio `domain.com`.
7. Guarde los cambios.

Cómo excluir una dirección web de los análisis de conexiones cifradas 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 ficha **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 **Agregar**.
7. Escriba 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 ingresar una máscara en el nombre de dominio.

   > Kaspersky Endpoint Security no admite el símbolo `*` para direcciones IP. Puede seleccionar un intervalo de direcciones IP con una máscara de subred (por ejemplo, 198.51.100.0/24).

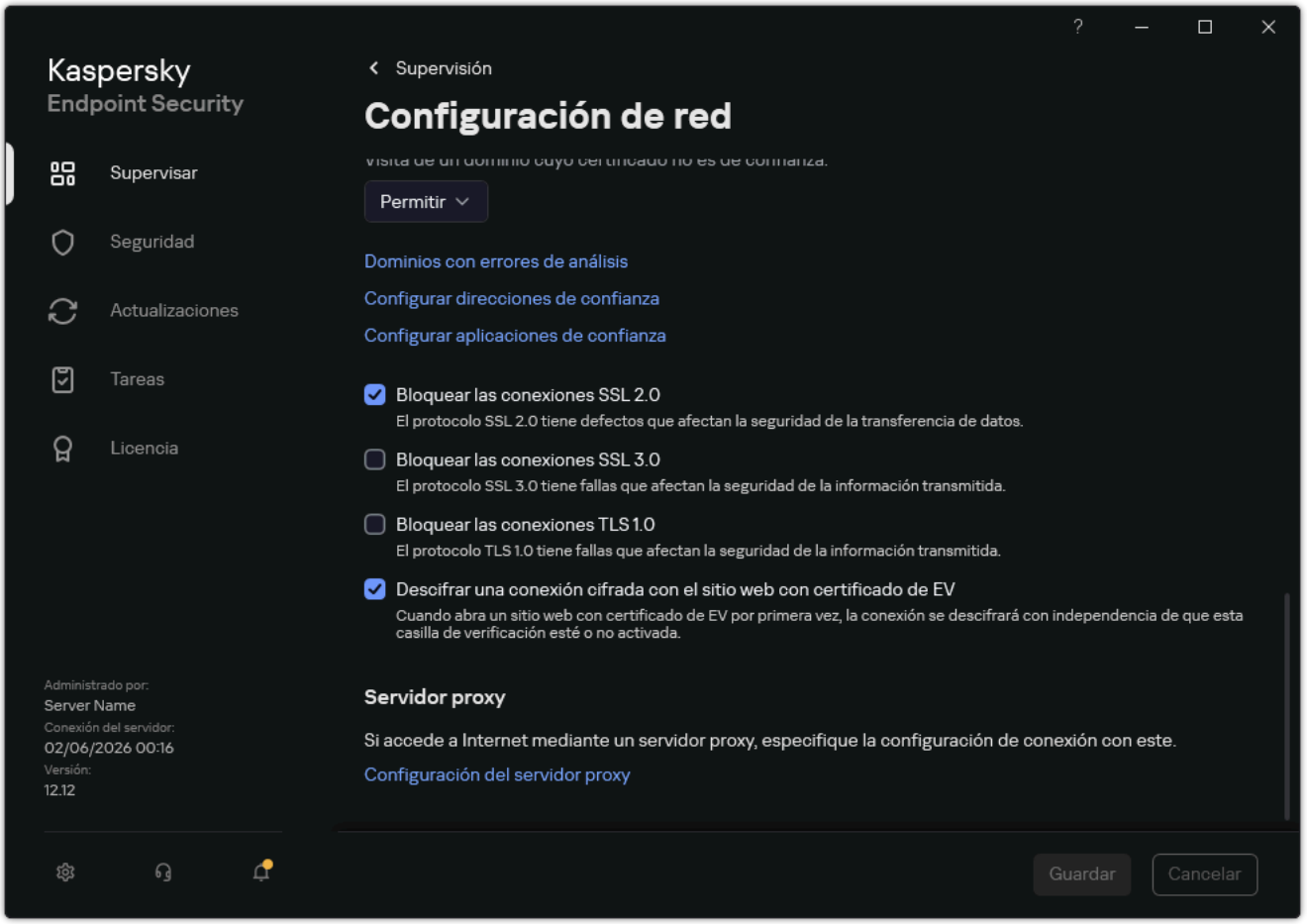
   Ejemplos:

   - `domain.com`: el registro incluye las siguientes direcciones: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. El registro no incluye 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 no incluye el dominio `domain.com`.
   - `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro no incluye el dominio `domain.com`.
8. Guarde los cambios.

Cómo excluir una dirección web de los análisis de conexiones cifradas en la interfaz de la aplicación

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

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



Parámetros de la configuración de red para aplicaciones

3. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Configurar direcciones de confianza**.

4. Haga clic en **Agregar**.

5. Escriba 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 ingresar una máscara en el nombre de dominio.

> Kaspersky Endpoint Security no admite el símbolo `*` para direcciones IP. Puede seleccionar un intervalo de direcciones IP con 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 no incluye 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 no incluye el dominio `domain.com`.
- `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro no incluye el dominio `domain.com`.

6. Guarde los cambios.

De manera predeterminada, si ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security desiste de analizar la conexión y agrega el dominio problemático a la lista *Dominios con errores de análisis*. Kaspersky Endpoint Security crea una lista separada para cada usuario. La información no se transmite a Kaspersky Security Center. Si lo prefiere, la aplicación puede en cambio bloquear las conexiones que no puede analizar correctamente. La lista de dominios con errores de análisis 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 principal de la aplicación 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 abrirá una lista de dominios con errores de análisis. Si desea vaciar la lista, habilite el bloqueo de conexiones con errores de análisis en la directiva, aplique la directiva, restablezca el valor inicial del parámetro y aplique nuevamente la directiva.

La aplicación cuenta con una lista de *excepciones globales*, en la que los especialistas de Kaspersky recogen los sitios web que se consideran de confianza y que siempre estarán exceptuados de los análisis, independientemente de lo que indique la configuración de Kaspersky Endpoint Security.

Para ver las exclusiones globales aplicadas al análisis de tráfico cifrado:

1. En la ventana principal de la aplicación 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 vínculo de la lista 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 modificarse cada vez que se actualizan las bases de datos y los módulos de Kaspersky Endpoint Security.

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 opera:

- en forma silenciosa,
- 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 por un tiempo prolongado.

No es posible configurar una eliminación de datos programada a través de las propiedades de la tarea. La eliminación solo puede suceder en forma inmediata (lo cual ocurre cuando la tarea se inicia manualmente) o en forma pospuesta (cuando no hay conexión con Kaspersky Security Center).

Limitaciones

La característica de 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.
- Cuando el sistema de archivos de una unidad es NTFS, Kaspersky Endpoint Security solo puede eliminar los nombres de las secuencias de datos principales. Los nombres de las secuencias de datos alternativas no se pueden eliminar.
- Cuando Kaspersky Endpoint Security elimina un archivo de vínculo simbólico, elimina también los archivos que se encuentran en las rutas especificadas en dicho vínculo.

Creación de una tarea de 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

   > Si se agregan nuevos equipos a un grupo de administración alcanzado por 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. Salga del 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 de propiedades de la tarea.

7. Seleccione la ficha **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. La información que se elimine será, a fines prácticos, imposible de recuperar.

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 por el período definido.

Al configurar la eliminación de datos pospuesta, tenga en cuenta que el personal puede trabajar en diferentes horarios. 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 estuvo inactiva durante más tiempo que el tiempo configurado, cuando el equipo se enciende, Kaspersky Endpoint Security no elimina los datos de inmediato. La aplicación espera sincronizarse con Kaspersky Security Center durante una hora. Esto es necesario para evitar la eliminación no autorizada de datos en los equipos de quienes apagaron sus equipos, por ejemplo, antes de irse de vacaciones.

Si esta casilla queda desactivada, la tarea se ejecutará en cuanto 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 los archivos de las siguientes áreas:

  - **Documentos**. Archivos que se encuentren en la carpeta *Documentos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.

  - **Cookies**. Archivos en los que el navegador guarda información sobre los sitios web que el usuario ha visitado (por ejemplo, datos de autorización).

  - **Escritorio**. Archivos que se encuentren en la carpeta *Escritorio* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.

  - **Archivos temporales de Internet Explorer**. Archivos temporales vinculados al funcionamiento de Internet Explorer: copias de páginas web, imágenes, archivos multimedia, etc.

  - **Archivos temporales**. Archivos temporales vinculados al funcionamiento de las aplicaciones instaladas en el equipo. Aquí se incluyen, por ejemplo, las copias de seguridad temporales que se crean al trabajar con documentos en las aplicaciones de Microsoft Office.

  - **Archivos de Outlook**. Archivos vinculados al funcionamiento del cliente de correo electrónico Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de las libretas de direcciones sin conexión (OAB) y archivos de las libretas de direcciones personales (PAB).

  - **Perfil del usuario**. Grupo de archivos y carpetas en los que el sistema operativo almacena la configuración asociada a la cuenta local del usuario.

Para crear la lista de objetos que se eliminarán, utilice las distintas pestañas. Kaspersky Endpoint Security generará una lista consolidada y eliminará todos los archivos que figuren en ella 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. Esto permite reducir el tráfico y el uso inadecuado del tiempo de trabajo. Cuando un usuario intente abrir un sitio web restringido por Control web, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia (vea la siguiente imagen).

Para utilizar Control web, debe completar la configuración inicial de la aplicación:

- Para que la aplicación pueda supervisar el tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitada de manera predeterminada).
- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación controla todos).
- Seleccione las aplicaciones cuyo tráfico desee que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya figuran en la lista de aplicaciones que recomienda Kaspersky. Si el navegador que utiliza no está en la lista, agréguelo.
- Recomendamos inyectar un script de interacción de página web en el tráfico web (la inyección de script está deshabilitada de forma predeterminada). Esta secuencia de comandos 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. Puede impedir que sus usuarios accedan a sitios catalogados como *Redes sociales*, por ejemplo, o a otras categorías.
- **Tipo de datos**. Puede restringir el acceso a ciertos tipos de datos y, por ejemplo, ocultar las imágenes de un sitio web. 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 de almacenamiento* 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 la 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.

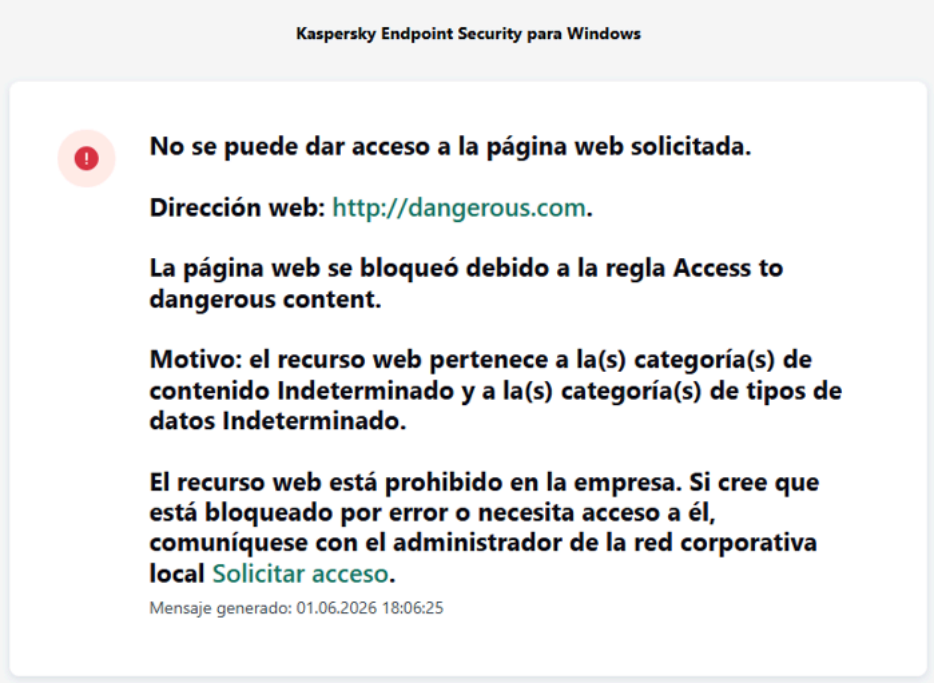
  Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.

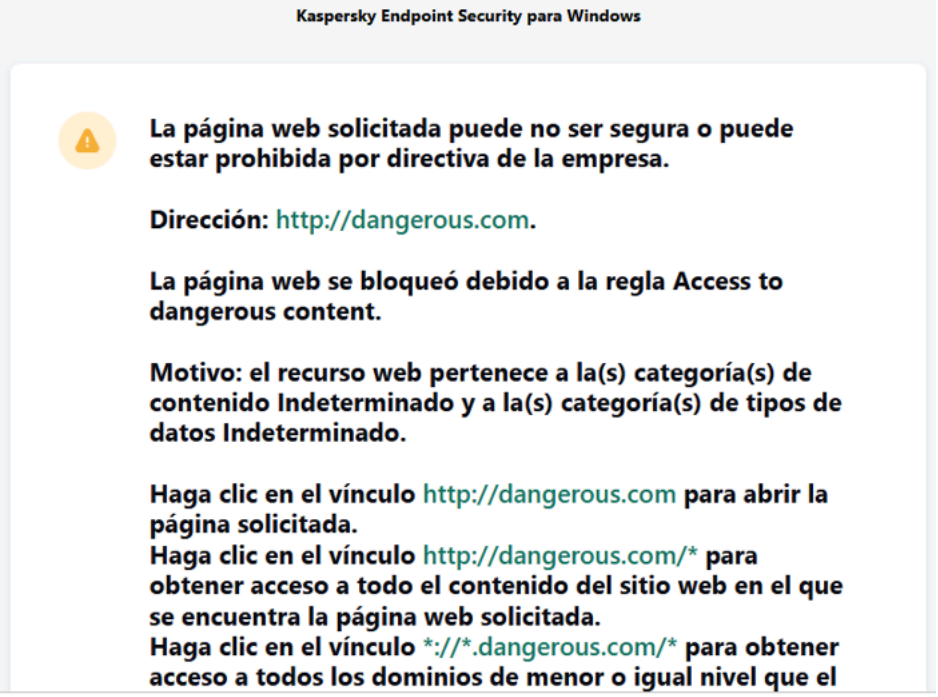
- Programación de la regla.

  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 arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado 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

Agregar 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 programación de la regla.

No se recomienda crear más de 1000 reglas de acceso a recursos web, ya que podría causar inestabilidades en el sistema.

Una regla de acceso a recursos web es un conjunto de filtros y acciones que Kaspersky Endpoint Security implementa cuando un usuario visita recursos web que están descritos en la regla durante el intervalo que se indica en la programación de la regla. Los filtros le permiten especificar con precisión un grupo de recursos web cuyo acceso está controlado mediante el componente Control web.

Están disponibles los siguientes filtros:

- **Filtrar por contenido**. Control web categoriza recursos web por contenido y tipo de datos. Puede controlar el acceso de los usuarios a los recursos web que tengan el contenido y los tipos de datos definidos en esas categorías. Cuando un usuario visita recursos web que pertenecen a la categoría de contenido o a la categoría de tipos de datos seleccionadas, Kaspersky Endpoint Security realiza la acción que se especifica 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 filtrado por contenido y por direcciones de recursos web y las direcciones o grupos de direcciones de recursos web especificados pertenecen a las categorías de contenido o tipos de datos seleccionadas, Kaspersky Endpoint Security no controla el acceso a todos los recursos web de las categorías de contenido o tipos de datos seleccionadas. En cambio, la aplicación solamente controla el acceso a las direcciones o grupos de direcciones de recursos web especificados.

- **Filtrar por nombres de usuarios y grupos de usuarios**. Puede especificar el nombre de los usuarios o grupos de usuarios para los cuales el acceso a los recursos web se controla conforme a la regla.

- **Programación de la regla**. Puede especificar la programación de la regla. La programación de reglas determina el intervalo durante el cual Kaspersky Endpoint Security controla el acceso a los recursos web cubiertos por la regla.

Una vez instalado Kaspersky Endpoint Security, la lista de reglas del componente Control web no está vacía. Se preestablece *Regla predeterminada*. 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 arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado 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 agregar 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 correspondiente 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 de verificación **Control web**.

5. En el bloque **Configuración de Control web**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de acceso a recursos web**.

6. Configure la regla de acceso a recursos web (consulte la tabla a continuación).

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

   > Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

   Si anula la selección de la casilla, Control web solo restringe las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

8. Guarde los cambios.

Cómo agregar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control web**.

5. Active el interruptor de **Control web HABILITADO**.

6. En el bloque **Lista de reglas**, haga clic en el botón **Agregar**.

7. Configure la regla de acceso a recursos web (consulte la tabla a continuación).

8. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

   > Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

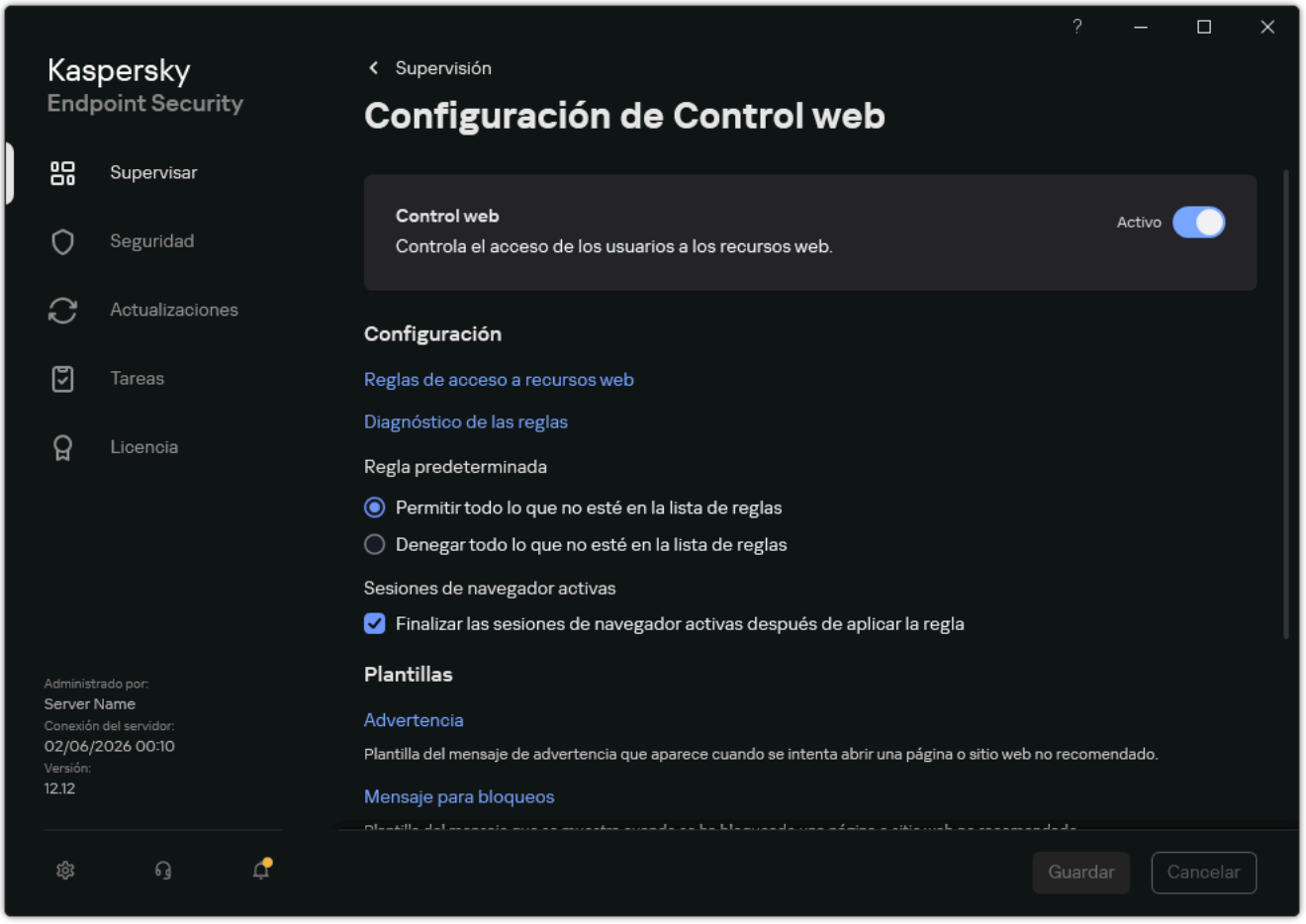
   Si anula la selección de la casilla, Control web solo restringe las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

9. Guarde los cambios.

Cómo agregar una regla de acceso a recursos web en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 el interruptor de **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 **Agregar**.

   Se abre la ventana **Regla de acceso a recursos web**.

6. Configure la regla de acceso a recursos web (consulte la tabla a continuación).

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

   > Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

   Si anula la selección de la casilla, Control web solo restringe 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 agrega a la lista. Si es necesario, cambie la prioridad de la regla de Control web. También puede usar el conmutador del interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

Parámetros de la 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 deshabilitar la regla de acceso a recursos web en cualquier momento.
Acción	• **Permitir**. Control web permite el acceso 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 denegado al sitio web. • **Advertir**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.
Contenido de filtro	• **Por categorías de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, *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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio. Si Análisis de conexiones cifradas está deshabilitado, 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.
Programación de la regla	La programación de reglas determina el intervalo durante el cual Kaspersky Endpoint Security controla 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. Durante la creación de una lista de direcciones web, puede ingresar las direcciones URL o utilizar máscaras.

Las reglas pueden incluir una programación de la regla y una lista de usuarios a los que se les aplica la regla. Por ejemplo, puede restringir el acceso a sitios web solo durante el horario laboral o permitir que usuarios de determinados grupos visiten sitios web.

Cómo habilitar un filtro de dirección de un recurso 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 correspondiente 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 de verificación **Control web**.
5. En el bloque **Configuración de Control web**, haga clic en el botón **Agregar**.
   Se abre la ventana **Regla de acceso a recursos web**.
6. Configure la regla de acceso a recursos web:
   a. En el campo **Nombre**, escriba el nombre de la regla.
   b. En la lista desplegable **Aplicar a las direcciones**, seleccione **A direcciones individuales**.
   c. Cree 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 Análisis de conexiones cifradas está deshabilitado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

   d. En la lista desplegable **Aplicar a los usuarios**, seleccione el filtro relevante para los usuarios:
      - **A todos los usuarios**. Control web no filtrará los recursos web por dirección.
      - **A usuarios o grupos 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

e. En la lista desplegable **Acción**, seleccione una opción:

- **Permitir**. Control web permite el acceso 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 denegado al sitio web.
- **Advertir**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

f. En la lista desplegable **Programación de la regla**, seleccione una programación o cree una nueva.

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

   Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

   Si anula la selección de la casilla, Control web solo restringe las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

8. Guarde los cambios.

Cómo habilitar un filtro de dirección de un recurso 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 ficha **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control web**.
5. Active el interruptor de **Control web HABILITADO**.
6. En el bloque **Lista de reglas**, haga clic en el botón **Agregar**.
7. Configure la regla de acceso a recursos web:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. Seleccione el estado **Habilitado** para la regla de acceso a recursos web.

   Puede usar el conmutador del interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

c. En el bloque **Acción**, seleccione la opción relevante:

- **Permitir**. Control web permite el acceso 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 denegado al sitio web.
- **Informar**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

d. En **Alcance**, seleccione **Sitios web individuales**.

e. Configure el filtrado de contenidos:

- **Dirección individual**. Cree 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 Análisis de conexiones cifradas está deshabilitado, 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 desee 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

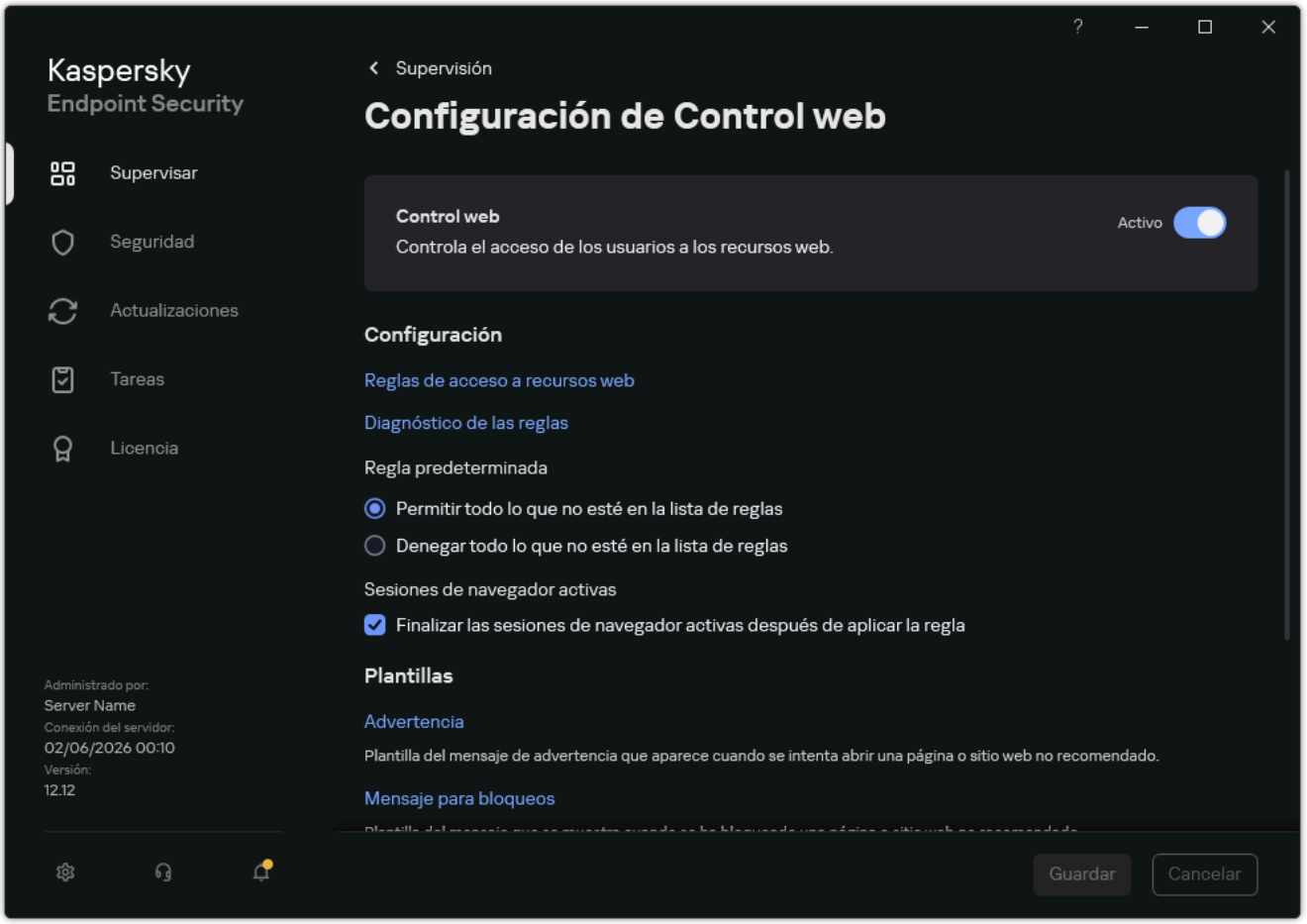
g. En el bloque **Programación de acceso**, seleccione una programación o cree una nueva.

8. Guarde los cambios.

Cómo habilitar un filtro de dirección de recurso web en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 **Agregar**.

   Se abre la ventana **Regla de acceso a recursos web**.

5. En el campo **Nombre de la regla**, escriba el nombre de la regla.

6. Seleccione el estado **Activo** para la regla de acceso a recursos web.

   Puede usar el interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento.

7. En el bloque **Acción**, seleccione la opción relevante:

   - **Permitir**. Control web permite el acceso 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 denegado al sitio web.

   - **Advertir**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

8. En **Direcciones**, seleccione **A direcciones individuales**.

Cree 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 Análisis de conexiones cifradas está deshabilitado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

9. En el bloque **Usuarios**, seleccione el filtro relevante 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

10. En la lista desplegable **Programación de la regla**, seleccione una programación o cree una nueva.

11. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

    > Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

    Si anula la selección de la casilla, Control web solo restringe 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 agrega a la lista. Si es necesario, cambie la prioridad de la regla de Control web. También puede usar el conmutador del interruptor para deshabilitar 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 según el contenido de recursos web, Control web proporciona un filtro de categoría 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. Puede impedir que sus usuarios accedan a sitios catalogados como *Redes sociales*, por ejemplo, o a otras categorías.

Puede restringir el acceso del usuario a un sitio web según el 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:

- Video

- Sonido

- Archivos de aplicaciones de Office
- Archivos ejecutables
- Archivos de almacenamiento
- 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 de almacenamiento* en lugar de *Imágenes*.

Las reglas pueden incluir una programación de la regla y una lista de usuarios a los que se les aplica la regla. Por ejemplo, puede restringir el acceso a sitios web solo durante el horario laboral o permitir que usuarios de determinados grupos visiten sitios web.

Cómo habilitar un filtro de contenido de un recurso 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 correspondiente 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 de verificación **Control web**.
5. En el bloque **Configuración de Control web**, haga clic en el botón **Agregar**.
   Se abre la ventana **Regla de acceso a recursos web**.
6. Configure la regla de acceso a recursos web:
   a. En el campo **Nombre**, escriba 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, *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**. Se habilitan los filtros por categorías de contenido y tipos de datos.

      Después de seleccionar los filtros, configure los parámetros del filtro.

c. En la lista desplegable **Aplicar a los usuarios**, seleccione el filtro relevante para los usuarios:

- **A todos los usuarios**. Control web no filtrará los recursos web por dirección.
- **A usuarios o grupos 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

d. En la lista desplegable **Acción**, seleccione una opción:

- **Permitir**. Control web permite el acceso 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 denegado al sitio web.
- **Advertir**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

e. En la lista desplegable **Programación de la regla**, seleccione una programación o cree una nueva.

7. Si desea que Control web finalice la conexión con el recurso web prohibido inmediatamente después de que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

   Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

   Si anula la selección de la casilla, Control web solo restringe las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.

8. Guarde los cambios.

Cómo habilitar un filtro de contenido de un recurso 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 ficha **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Control web**.
5. Active el interruptor de **Control web HABILITADO**.
6. En el bloque **Lista de reglas**, haga clic en el botón **Agregar**.

7. Configure la regla de acceso a recursos web:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. Seleccione el estado **Habilitado** para la regla de acceso a recursos web.

      Puede usar el interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento.

   c. En el bloque **Acción**, seleccione la opción relevante:

      - **Permitir**. Control web permite el acceso 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 denegado al sitio web.
      - **Informar**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

   d. En **Alcance**, seleccione **Categoría de contenido**.

   e. Configure el filtrado de contenidos:

      - **Categoría de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, *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 desee 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

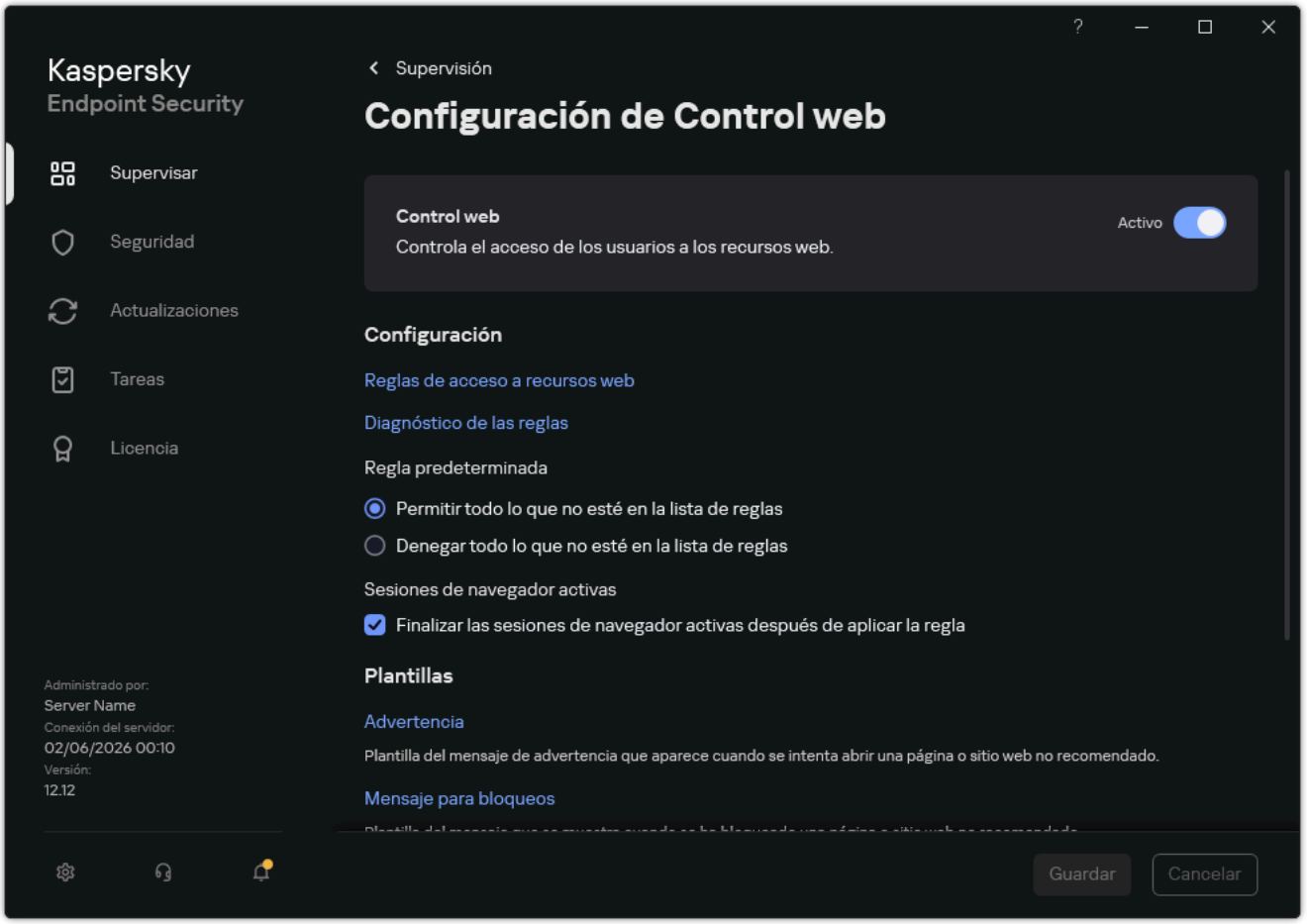
   g. En el bloque **Programación de acceso**, seleccione una programación o cree una nueva.

8. Guarde los cambios.

Cómo habilitar un filtro de contenido de un recurso web en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 **Agregar**.

   Se abre la ventana **Regla de acceso a recursos web**.

5. En el campo **Nombre de la regla**, escriba el nombre de la regla.

6. Seleccione el estado **Activo** para la regla de acceso a recursos web.

   Puede usar el interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento.

7. En el bloque **Acción**, seleccione la opción relevante:

   - **Permitir**. Control web permite el acceso 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 denegado al sitio web.

   - **Advertir**. Cuando el usuario intenta obtener acceso a un recurso web que coincide con la regla, Control web muestra una advertencia que indica que no se aconseja visitar el recurso web. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

8. En el bloque **Contenido de filtro**, seleccione el filtro de contenido correspondiente:

   - **Por categorías de contenido**. Puede controlar el acceso de los usuarios a los recursos web por categoría (por ejemplo, *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 vínculo **Configuración**.

   b. Seleccione las casillas junto a los nombres de las categorías de contenido y/o tipos de datos que desee.

   Al seleccionar la casilla junto al nombre de una categoría de contenido y/o tipo de datos, Kaspersky Endpoint Security aplicará la regla para controlar el acceso a los recursos web que pertenecen a las categorías de contenido y/o tipos de datos seleccionados.

   c. Regrese a la ventana para configurar la regla de acceso a recursos web.

9. En el bloque **Usuarios**, seleccione el filtro relevante 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio. Para crear una lista de usuarios a los que desea aplicar la regla:

     a. Haga clic en **Agregar**.

     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 **Programación de la regla**, seleccione el nombre de la programación necesaria o genere una programación nueva basada en la programación de la regla seleccionada. Para hacerlo:

    a. Haga clic en **Editar o agregar nuevo**.

    b. En la ventana que se abre, haga clic en el botón **Agregar**.

    c. En la ventana que se abre, ingrese el nombre de la programación de la regla.

    d. Configure la programación 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 que se aplique la directiva, seleccione la casilla **Finalizar las sesiones de navegador activas después de aplicar la regla**.

Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones.

Si anula la selección de la casilla, Control web solo restringe 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 agrega a la lista. Si es necesario, cambie la prioridad de la regla de Control web. También puede usar el conmutador del interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento sin eliminarla de la lista.

Prueba de las reglas de acceso a recursos web

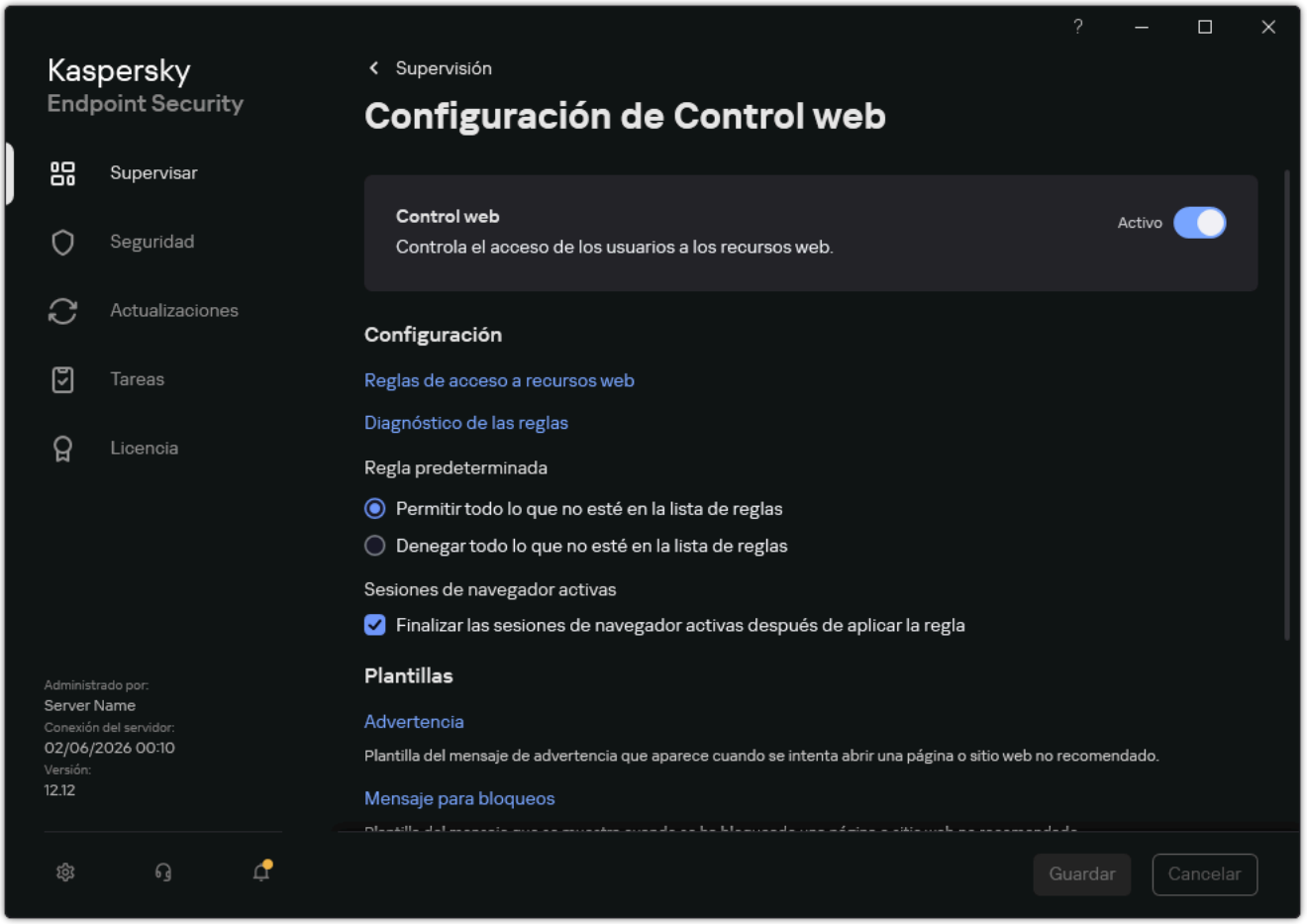
Durante la configuración de Control web, es posible que bloquee involuntariamente el acceso a recursos web que los usuarios necesitan para realizar su trabajo. Para averiguar cuál es la regla de Control web que bloquea el acceso a recursos web, puede usar la herramienta *Diagnóstico de las reglas de Control web*. Diagnóstico de las reglas de Control web solo está disponible en la interfaz de Kaspersky Endpoint Security. En la consola de Kaspersky Security Center, no puede averiguar cuál es la regla de Control web que incluye un determinado recurso.

Si el usuario considera que el recurso web fue bloqueado por error, puede hacer clic en el vínculo del mensaje de notificación de bloqueo del recurso web para enviar un mensaje generado previamente al administrador de la red corporativa local.

Para probar las reglas de acceso a recursos web:

1. En la ventana principal de la aplicación 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 vínculo **Diagnóstico de las reglas**.

   Se abre la ventana **Diagnóstico de las reglas**.

4. Si desea probar las reglas que Kaspersky Endpoint Security utiliza para controlar el acceso a un recurso web específico, seleccione la casilla **Especificar dirección**. Ingrese la dirección del recurso web en el campo a continuación.

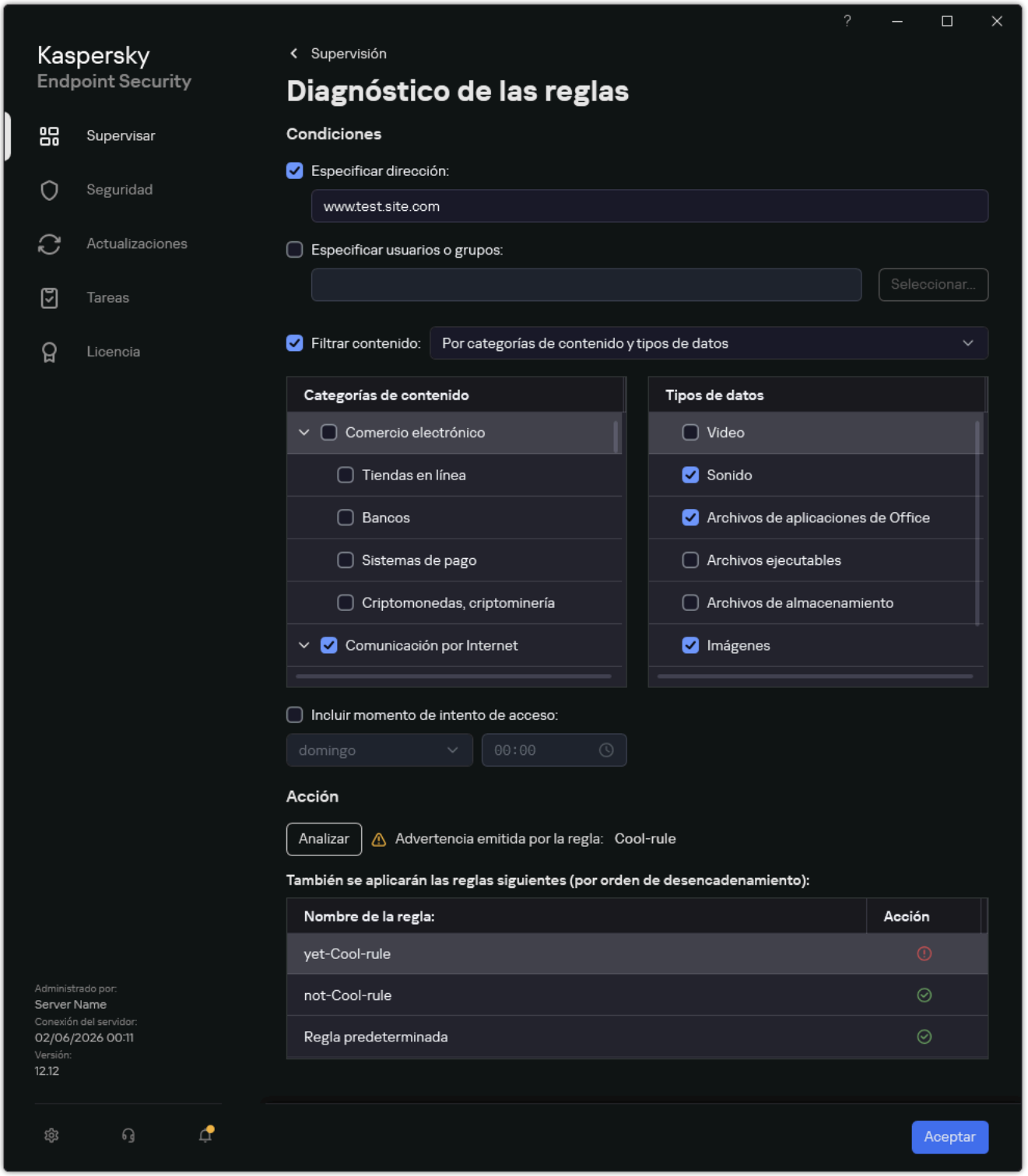
5. Si desea probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a recursos web de usuarios o grupos de usuarios especificados, especifique una lista de usuarios o grupos de usuarios.

6. Si desea probar las reglas que Kaspersky Endpoint Security usa para controlar el acceso a recursos web de categorías de contenido o categorías de tipos de datos determinadas, seleccione la casilla **Filtrar contenido** y elija la opción correspondiente en la lista desplegable (**Por categorías de contenido**, **Por tipos de datos** o **Por categorías de contenido y tipos de datos**).

7. Si desea probar las reglas teniendo en cuenta la hora y el día de la semana en que se intentó acceder a los recursos web que se especifican en las condiciones del diagnóstico de reglas, seleccione la casilla **Incluir momento de intento de acceso**. Luego, especifique el día de la semana y la hora.

8. Haga clic en **Analizar**.

Al completarse la prueba, aparece un mensaje con información sobre la acción realizada por Kaspersky Endpoint Security según la primera regla que se aplica sobre el intento de acceso a los recursos web especificados (autorizar, bloquear o advertir). La primera regla que se aplica es la que tiene un lugar en la lista de reglas del Control Web que es superior al de las otras reglas que cumplen las condiciones del diagnóstico. El mensaje se muestra a la derecha del botón **Analizar**. La siguiente tabla enumera las reglas activadas restantes, especificando la acción llevada a cabo por Kaspersky Endpoint Security. Las reglas están enumeradas en orden de prioridad decreciente.



Resultado de la prueba de acceso al recurso web

Exportar e importar reglas de control web

Puede exportar la lista de reglas de Control web a un archivo XML o JSON. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 otro servidor.

Cómo exportar e importar una lista de reglas de Control web a la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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:
   a. Seleccione la regla de acceso que desea 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 vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.
5. Para importar la lista de reglas de Control web:
   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
6. Guarde los cambios.

Cómo exportar e importar una lista de reglas de Control web a 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 ficha **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 la regla de acceso que desea 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 que se usará para importar la lista de reglas.

   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

7. Guarde los cambios.

Exportar e importar direcciones de recursos web de la regla de Control web

Si creó una lista de direcciones de recursos web en una regla de acceso a recursos web, puede exportarla a un archivo:

- en formato TXT en la Consola de administración (MMC);
- en formato CSV en la interfaz de la aplicación.

Posteriormente, puede importar la lista de este archivo para evitar crear una nueva lista de direcciones de recursos web manualmente cuando configure la regla de acceso. La opción de exportar e importar la lista de direcciones de recursos web puede ser útil si, por ejemplo, crea reglas de acceso con parámetros similares.

También puede exportar o importar todas las reglas de Control web y no solo las direcciones de recursos web de una regla individual.

> No puede exportar ni importar direcciones de recursos web de una regla de Control web en Web Console o Cloud Console.

Cómo exportar o importar direcciones de recursos web de la regla 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 correspondiente 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 Control web**, seleccione la regla cuyas direcciones de recursos web desea exportar o importar.

   Se muestran las propiedades de la regla de Control web.

5. Para exportar 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, escriba el nombre del archivo TXT en el que desea exportar la lista de direcciones de recursos web, y seleccione la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exporta la lista de direcciones de recursos web a un archivo TXT.

6. 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 que desea usar para importar la lista de recursos web.

   b. Abra el archivo.

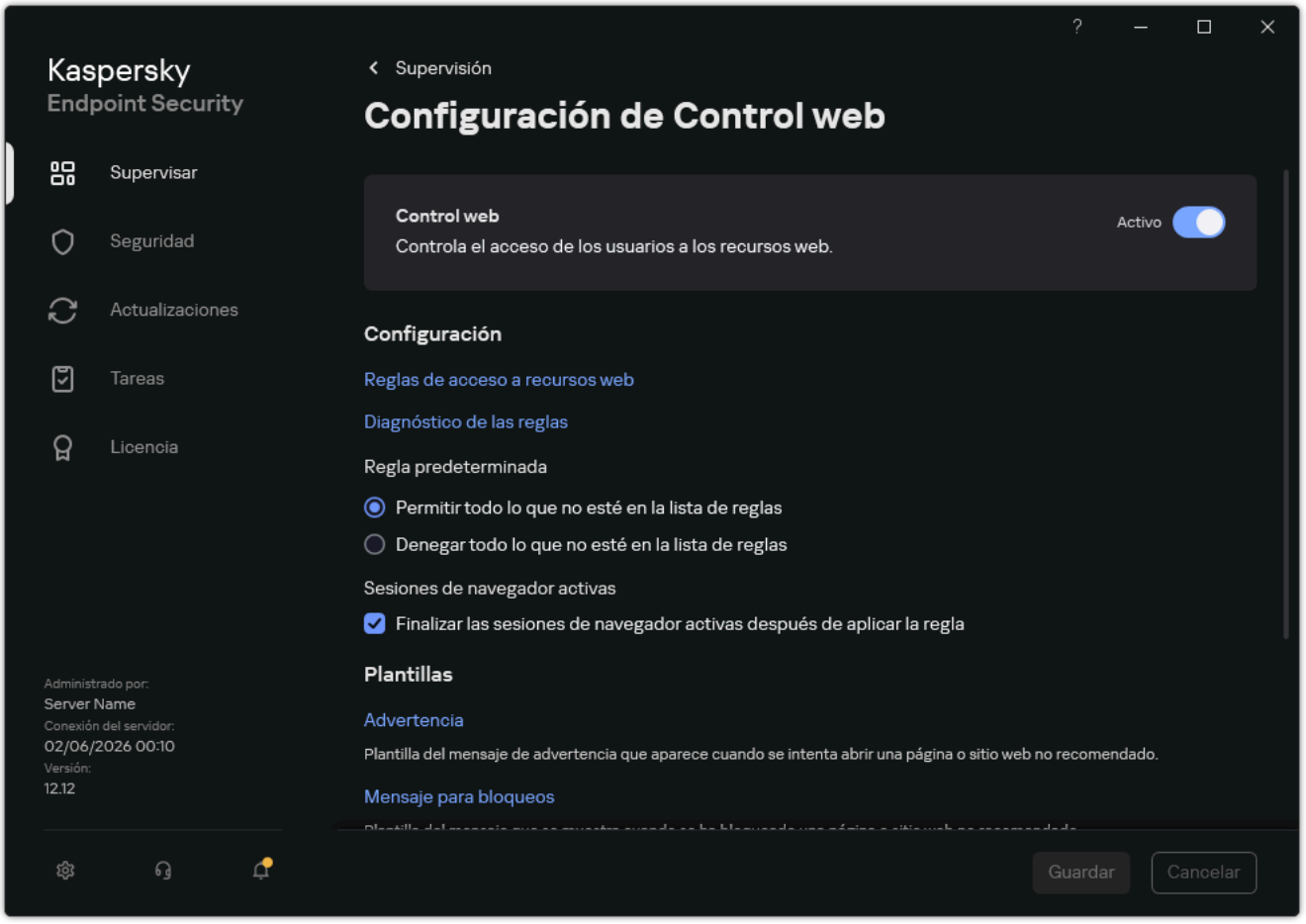
      Cuando ya exista una lista de direcciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo TXT.

7. Guarde los cambios.

Cómo exportar o importar direcciones de recursos web de la regla de Control web en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 cuyas direcciones de recursos web desea 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, escriba el nombre del archivo CSV en el que desea exportar la lista de direcciones de recursos web, y seleccione la carpeta en la que se guardará 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 que desea usar para importar la lista de recursos web.

b. Abra el archivo.

Cuando ya exista una lista de direcciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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. Ello 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 compatibles con la función de monitoreo: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. El monitoreo de la actividad del usuario no funciona en otros navegadores.

Cuando un usuario utiliza Internet, Kaspersky Endpoint Security crea los siguientes eventos:

- Bloqueo de un sitio web (estado ⓘ, correspondiente a *Crítico*).
- Visita a un sitio web no recomendado (estado ⚠, correspondiente a las *Advertencia*).
- Visita a un sitio web permitido (estado ⓘ, correspondiente a *Información*).

Antes de habilitar 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 registrar eventos de Control web.
- Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario habilitar el análisis de conexiones cifradas.

Inyección de un script de interacción de página web

Cómo inyectar un script de interacción de 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 correspondiente 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 **Inyectar un script en el tráfico web para interactuar con las páginas web**.

5. Guarde los cambios.

Cómo inyectar un script de interacción de 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 ficha **Configuración de la aplicación**.

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

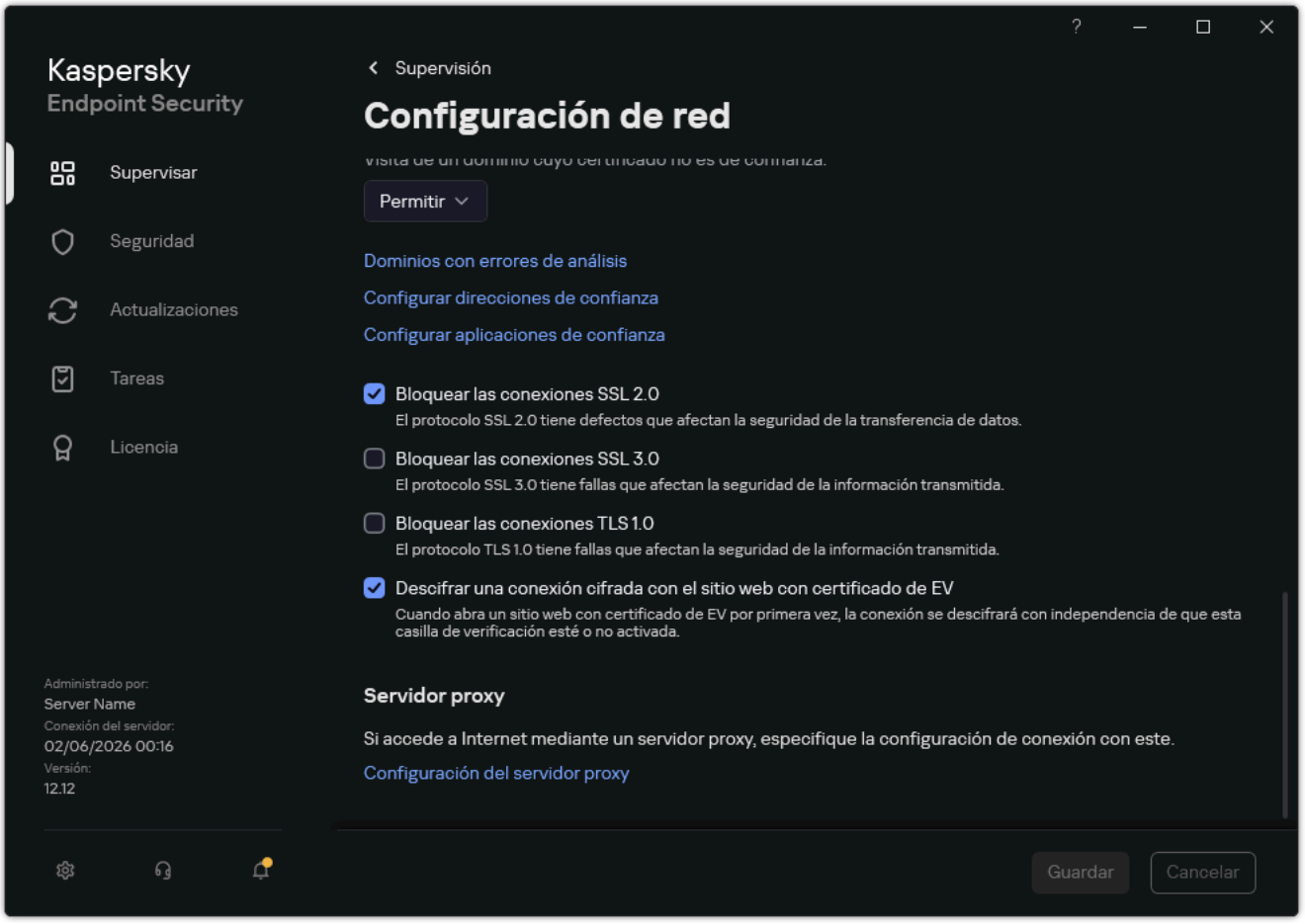
5. En **Supervisión de conexiones a Internet**, active el interruptor **Supervisión de conexiones a Internet HABILITADA**.

6. Guarde los cambios.

Cómo inyectar un script de interacción de página web en el tráfico web en la interfaz de la aplicación

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

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



Parámetros de la configuración de red para aplicaciones

3. En el bloque **Procesamiento de tráfico**, seleccione la casilla **Inyectar un script en el tráfico web para interactuar con las páginas web**.

4. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security inyectará un script de interacción de la página web en el tráfico web. Esta secuencia de comandos 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 principal de la aplicación 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 las 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 habilitar 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 comunica las actividades de los usuarios a Kaspersky Security Center de este modo:

- Cuando se utiliza Kaspersky Security Center, Control web envía un evento por cada objeto que forma parte de una 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 siguientes objetos: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js, entre otros.

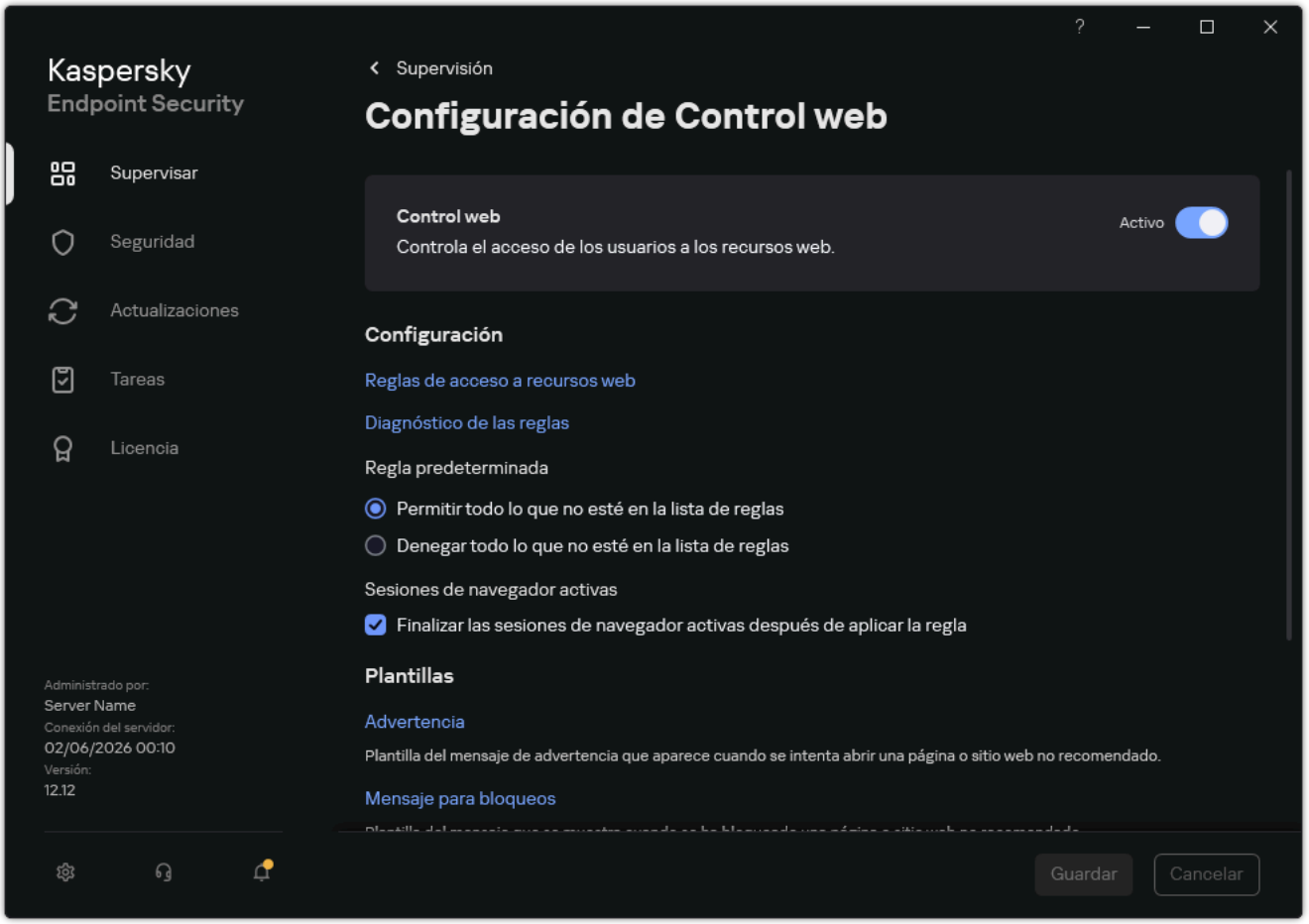
- Cuando se utiliza Kaspersky Security Center Cloud Console, Control web agrupa los eventos y transfiere solo el protocolo y el dominio del sitio web. Por ejemplo, si un usuario visita las páginas web no recomendadas http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, Kaspersky Endpoint Security enviará un único evento, con el objeto http://www.example.com.

Registro de eventos cuando se visiten los sitios web permitidos

Para que se registren los eventos cuando se visiten los sitios web permitidos:

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

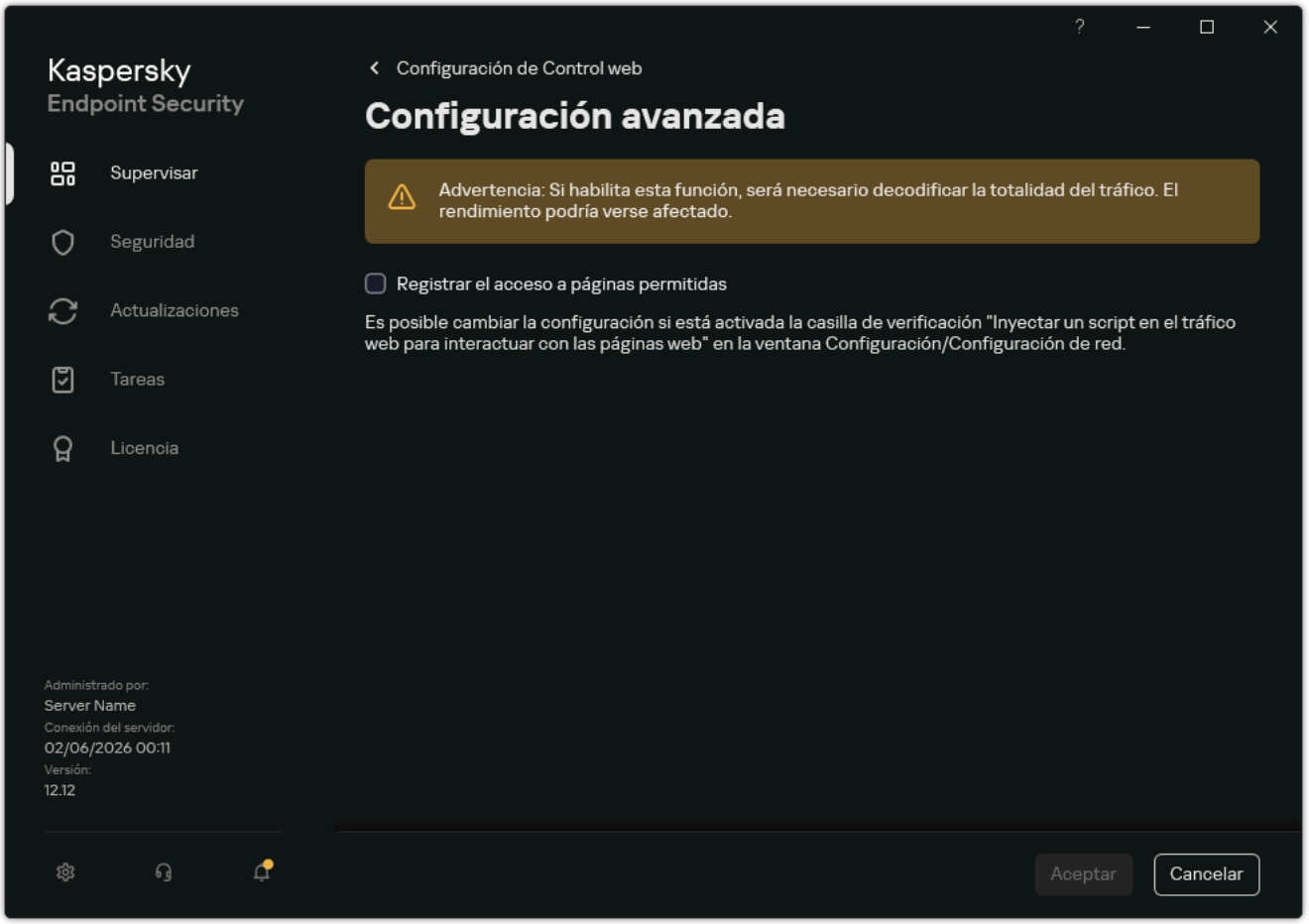
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control web**.



Configuración de Control web

3. En el bloque **Adicional**, haga clic en el botón **Configuración avanzada**.

4. En la ventana que se abre, seleccione 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 del Control web

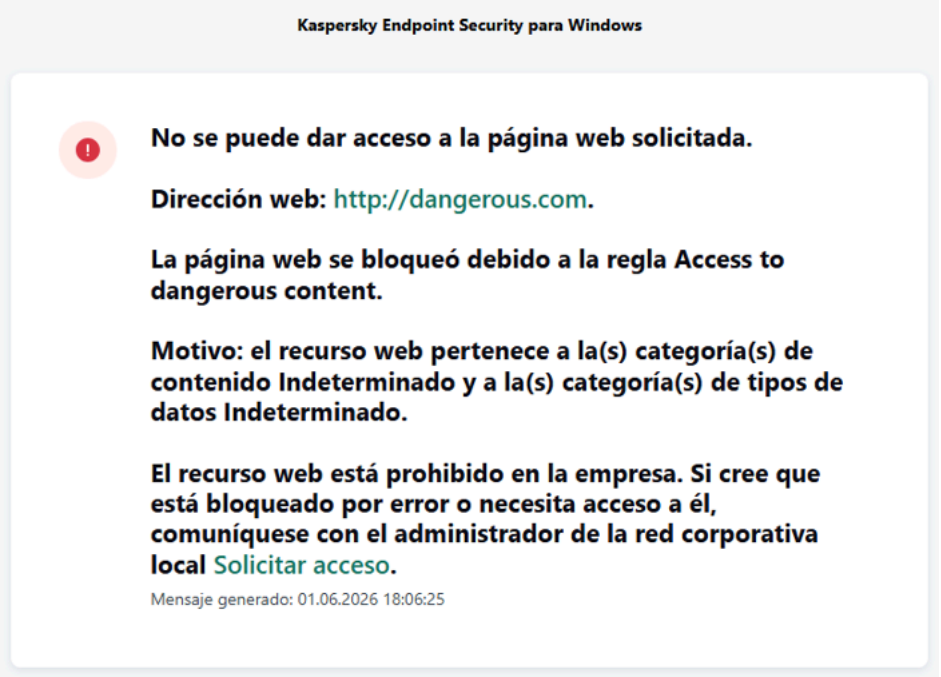
Según el tipo de acción que se especifique en las propiedades de las reglas de Control Web, Kaspersky Endpoint Security muestra un mensaje de uno de los siguientes tipos cuando los usuarios intentan acceder a recursos de Internet (la aplicación sustituye una página HTML con un mensaje para la respuesta del servidor HTTP):

- Mensaje de advertencia. Este mensaje advierte al usuario que la visita al recurso web no es recomendable o no cumple con la directiva de seguridad corporativa. 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 considera que la advertencia es errónea, puede hacer clic en el vínculo de la advertencia para enviar un mensaje generado previamente al administrador de la red corporativa local.

- Mensaje sobre el bloqueo de un recurso web. Kaspersky Endpoint Security muestra un mensaje en el que se indica que un recurso web está bloqueado (consulte la imagen a continuación) si la opción **Bloquear** está seleccionada en la configuración de la regla que describe este recurso web.

Si el usuario considera que el recurso web fue bloqueado por error, puede hacer clic en el vínculo del mensaje de notificación de bloqueo del recurso web para enviar un mensaje generado previamente al administrador de la red corporativa local.



Mensaje para bloqueos de recursos web

Se ofrecen plantillas especiales para el mensaje de advertencia, para el mensaje en el que se informa que un recurso web está bloqueado y para el mensaje que se envía enviar al administrador de la red LAN. Se proporcionan variables especiales para administrar las plantillas de mensajes (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensajes para diferentes equipos. 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 que coincide con el equipo, el usuario y el evento específicos.

Cómo cambiar la plantilla de mensajes 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 correspondiente 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 consiste en una plantilla del mensaje que se muestra si se activa una regla de advertencia acerca de intentos para acceder a un recurso web no deseado.

   - **Mensaje para bloqueos**. El campo de entrada contiene la plantilla del mensaje que se muestra si se activa una regla que bloquea el acceso a un recurso web.

   - **Mensaje para el administrador**. Plantilla del mensaje que se enviará al administrador de LAN si el usuario considera que se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del acceso a una página web para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada utilizando el botón **Predeterminado**.

6. Guarde los cambios.

Cómo cambiar la plantilla de mensajes de Control web 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 ficha **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 el bloqueo del sitio web** y configure las plantillas de los mensajes de Control web:

   - **Advertencia**. El campo de entrada consiste en una plantilla del mensaje que se muestra si se activa una regla de advertencia acerca de intentos para acceder a un recurso web no deseado.

   - **Mensaje para bloqueos**. El campo de entrada contiene la plantilla del mensaje que se muestra si se activa una regla que bloquea el acceso a un recurso web.

   - **Mensaje para el administrador**. Plantilla del mensaje que se enviará al administrador de LAN si el usuario considera que se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del acceso a una página web para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

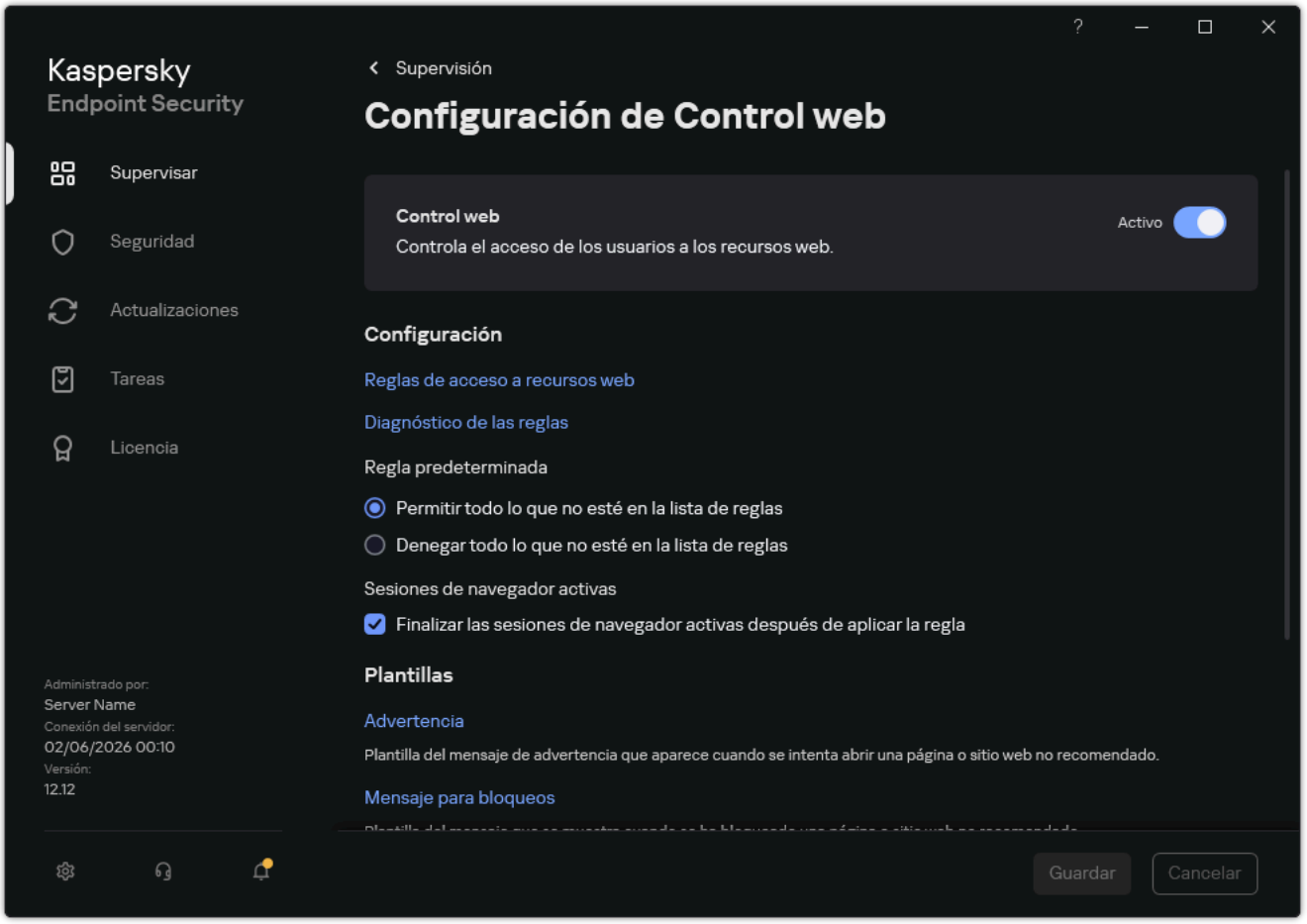
También puede restaurar el texto de la plantilla predeterminada utilizando el botón **Restaurar configuración predeterminada**.

6. Guarde los cambios.

Cómo cambiar la plantilla de mensajes de Control web en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 consiste en una plantilla del mensaje que se muestra si se activa una regla de advertencia acerca de intentos para acceder a un recurso web no deseado.

   - **Mensaje para bloqueos**. El campo de entrada contiene la plantilla del mensaje que se muestra si se activa una regla que bloquea el acceso a un recurso web.

   - **Mensaje para el administrador**. Plantilla del mensaje que se enviará al administrador de LAN si el usuario considera que se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del acceso a una página web para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

También puede restaurar el texto de la plantilla predeterminada 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 ser útil si necesita escribir varias direcciones de recursos web similares cuando crea una regla de acceso a recursos web. Si está bien diseñada, una máscara de dirección puede sustituir a una gran cantidad de direcciones de recursos web.

Al crear una máscara de dirección, siga las reglas a continuación:

1. El carácter `*` reemplaza cualquier secuencia que no tenga caracteres o que tenga uno o más caracteres.

   Por ejemplo, si crea una regla de acceso con la máscara `*abc*`, la regla se aplicará a todos los recursos web que tengan la secuencia `abc` en su dirección. Ejemplo: `http://www.example.com/page_0-9abcdef.html`.

2. El par de caracteres `*.` (combinación conocida como *máscara de dominio*) permite abarcar todos los dominios de una dirección. La máscara de dominio `*.` representa cualquier nombre de dominio, subdominio o 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 línea en blanco.

3. La secuencia de caracteres `www.` al comienzo de la máscara de dirección se interpreta como una secuencia `*.`

   Ejemplo: la máscara `www.example.com` se interpreta como `*.example.com`. La máscara comprende las direcciones `www2.example.com` y `www.pictures.example.com`.

4. Si una máscara de dirección no comienza con el carácter `*`, el contenido de la máscara de dirección es equivalente al mismo contenido con el prefijo `*.`.

5. Si una máscara de dirección termina con un carácter que no sea `/` o `*`, el contenido de la máscara de dirección es equivalente al mismo contenido con el postfijo `/*`.

   Ejemplo: la máscara `http://www.example.com` comprende direcciones como `http://www.example.com/abc` (entendiéndose que `a`, `b` y `c` pueden ser cualquier carácter).

6. Si una máscara de dirección termina con el carácter `/`, el contenido de la máscara de dirección es equivalente al mismo contenido con el postfijo `/*`.

7. La secuencia de caracteres `/*` al final de una máscara de dirección se interpreta como `/*` o como una cadena vacía.

8. Las direcciones de recursos web se comprueban con una máscara de dirección, teniendo en cuenta el protocolo (http o https):

   - Si la máscara de dirección no contiene un protocolo de red, esta máscara de red abarca las direcciones con cualquier protocolo de red.

     Ejemplo: la máscara de dirección `example.com` cubre las direcciones `http://example.com` y `https://example.com`.

   - Si la máscara de dirección contiene un protocolo de red, esta máscara de dirección solo abarca las direcciones que tienen el mismo protocolo de red que la máscara de dirección.

     Ejemplo: la máscara `http://*.example.com` comprende la dirección `http://www.example.com`, pero no la dirección `https://www.example.com`.

9. Una máscara de dirección encerrada entre comillas dobles se trata sin considerar ninguna sustitución adicional, excepto el carácter `*` si se lo ha incluido inicialmente en la máscara de dirección. Las reglas 5 y 7 no se aplican a máscaras de dirección entre comillas dobles (consulte los ejemplos 14 al 18 de la tabla que se incluye a continuación).

10. El nombre de usuario y la contraseña, el puerto de conexión y las mayúsculas o minúsculas de los caracteres no se tienen en cuenta durante la comparación con la máscara de dirección de un recurso web.

Ejemplos de uso de reglas para crear máscaras de dirección

Número	Máscara de dirección	Dirección de recurso web para comprobar	¿La máscara de dirección abarca la dirección?	Comentario
1	*.example.com	http://www.123example.com	No	Consulte la regla 1.
2	*.example.com	http://www.123.example.com	Sí	Consulte la regla 2.
3	*example.com	http://www.123example.com	Sí	Consulte la regla 1.
4	*example.com	http://www.123.example.com	Sí	Consulte la regla 1.
5	http://www.*.example.com	http://www.123example.com	No	Consulte la regla 1.
6	www.example.com	http://www.example.com	Sí	Consulte las reglas 3, 2, 1.
7	www.example.com	https://www.example.com	Sí	Consulte las reglas 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Sí	Consulte las reglas 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Sí	Consulte las reglas 3, 5, 1.
10	example.com	http://www.example.com	Sí	Consulte las reglas 3, 1.
11	http://example.com/	http://example.com/abc	Sí	Consulte la regla 6.
12	http://example.com/*	http://example.com	Sí	Consulte la regla 7.
13	http://example.com	https://example.com	No	Consulte la regla 8.
14	"example.com"	http://www.example.com	No	Consulte la regla 9.
15	"http://www.example.com"	http://www.example.com/abc	No	Consulte la regla 9.
16	"*.example.com"	http://www.example.com	Sí	Consulte las reglas 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Sí	Consulte las reglas 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Sí	Consulte las reglas 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	Una máscara de dirección contiene más información que 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 de forma local en el equipo. Esto funciona sin 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 mediante una regla de Control web, en un navegador en la *máquina virtual*, la aplicación instalada en el sistema operativo host del *equipo* deniega el acceso a dicho 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 de Oracle VM VirtualBox sin limitaciones. La aplicación puede controlar todo el tráfico de la máquina virtual. Si el usuario configura un filtro 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 de VMware Workstation con limitaciones. La aplicación no admite reglas con un filtro configurado por el usuario. Los procesos de la máquina virtual se ejecutan en virtud del usuario del sistema (SYSTEM). Por este motivo, es imposible identificar al usuario que intenta abrir el sitio web en la máquina virtual.

Microsoft Hyper-V

Kaspersky Endpoint Security no admite reglas de Control web en máquinas virtuales de Microsoft Hyper-V.

Variables en las plantillas de mensajes de Control web

Puede utilizar las siguientes variables en las plantillas de mensajes del usuario o del administrador:

- **Usuario**: `%USER_NAME%`.

  Nombre de la cuenta de usuario actual en el equipo en el que se generó el mensaje, con el 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 enviar un mensaje**: `%COMPLAIN_EMAIL%`.

  Dirección de correo electrónico donde recibir comentarios sobre los bloqueos de recursos web. Al hacer clic en la dirección de correo electrónico, se abre una ventana donde el usuario puede escribir un mensaje al administrador.

- **Nombre de categoría de contenido**: `%CONTENT_CATEGORY_LIST%`.

  Categoría de sitio web a la que pertenece el recurso bloqueado (por ejemplo, *Sistemas de pago*).

- **Nombre de categoría de tipos de datos**: `%TYPE_CATEGORY_LIST%`.

  Categoría del tipo de datos en el recurso web bloqueado (por ejemplo, *Archivos de imagen*).

- **Vínculo a recurso web solicitado**: `%CONTINUE_PAGE%`.

  Vínculo a la página web solicitada (por ejemplo, `http://www.example.com/pagename.html`).

- **Vínculo a sitio web**: `%CONTINUE_SITE%`.

  Vínculo al sitio web que contiene la página web solicitada (por ejemplo, `http://www.example.com/`).

- **Vínculo para acceder a dominios**: `%CONTINUE_DOMAIN%`.

  Vínculo en 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`. Si se hace clic en este vínculo, 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 (incluso una cadena vacía).

Control de dispositivos

El Control de dispositivos administra el acceso de los usuarios a los dispositivos que se instalan o se conectan al equipo (por ejemplo, discos duros, cámaras o módulos Wi-Fi). Esto impide la infección del equipo cuando se conectan dichos dispositivos y evita las pérdidas o fugas de datos.

Si el componente Control de dispositivos está habilitado, 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

El 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 de la siguiente manera:

  - Permitir – ✓.
  - Bloquear – ⊘.
  - Por reglas (solo impresoras y dispositivos portátiles) – .

- Depende del bus de conexión (excepto Wi-Fi) – .
- Bloquear con excepciones (solo Wi-Fi) – .

- **Bus de conexión**. El *bus de conexión* es una interfaz utilizada 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 de la siguiente manera:

  - 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 completo en todo momento.

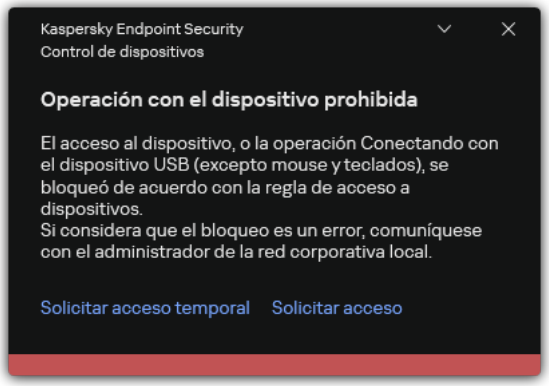
  Puede agregar dispositivos de confianza en función de los siguientes datos:

  - **Dispositivos por Id**. Cada dispositivo tiene un identificador único (id. de hardware, también denominado HWID). Puede ver el Id. en las propiedades del dispositivo usando las herramientas del sistema operativo. Un Id. de dispositivo típico podría ser: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id.
  - **Dispositivos por modelo**. Cada dispositivo tiene un id. de proveedor (VID) y un id. de producto (PID). Puede ver los ID. en las propiedades del dispositivo usando las herramientas del sistema operativo. Los valores VID y PID deben especificarse en este formato: `VID_1234&PID_5678`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.
  - **Dispositivos por máscara de id**. Si está usando varios dispositivos con Id. similares, puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `WDC_C*`.
  - **Dispositivos por máscara de modelo**. Si está usando varios dispositivos con VID o PID similares (por ejemplo, dispositivos del mismo fabricante), puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `VID_05AC&PID_*`.

El Control de dispositivos regula el acceso de los usuarios a los dispositivos usando *reglas de acceso*. El Control de dispositivos también le permite guardar eventos relacionados con la 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 los eventos relacionados con la conexión/desconexión de dispositivos, autorice el acceso al tipo de dispositivo correspondiente (estado) o agregue el dispositivo a la lista de dispositivos de confianza.

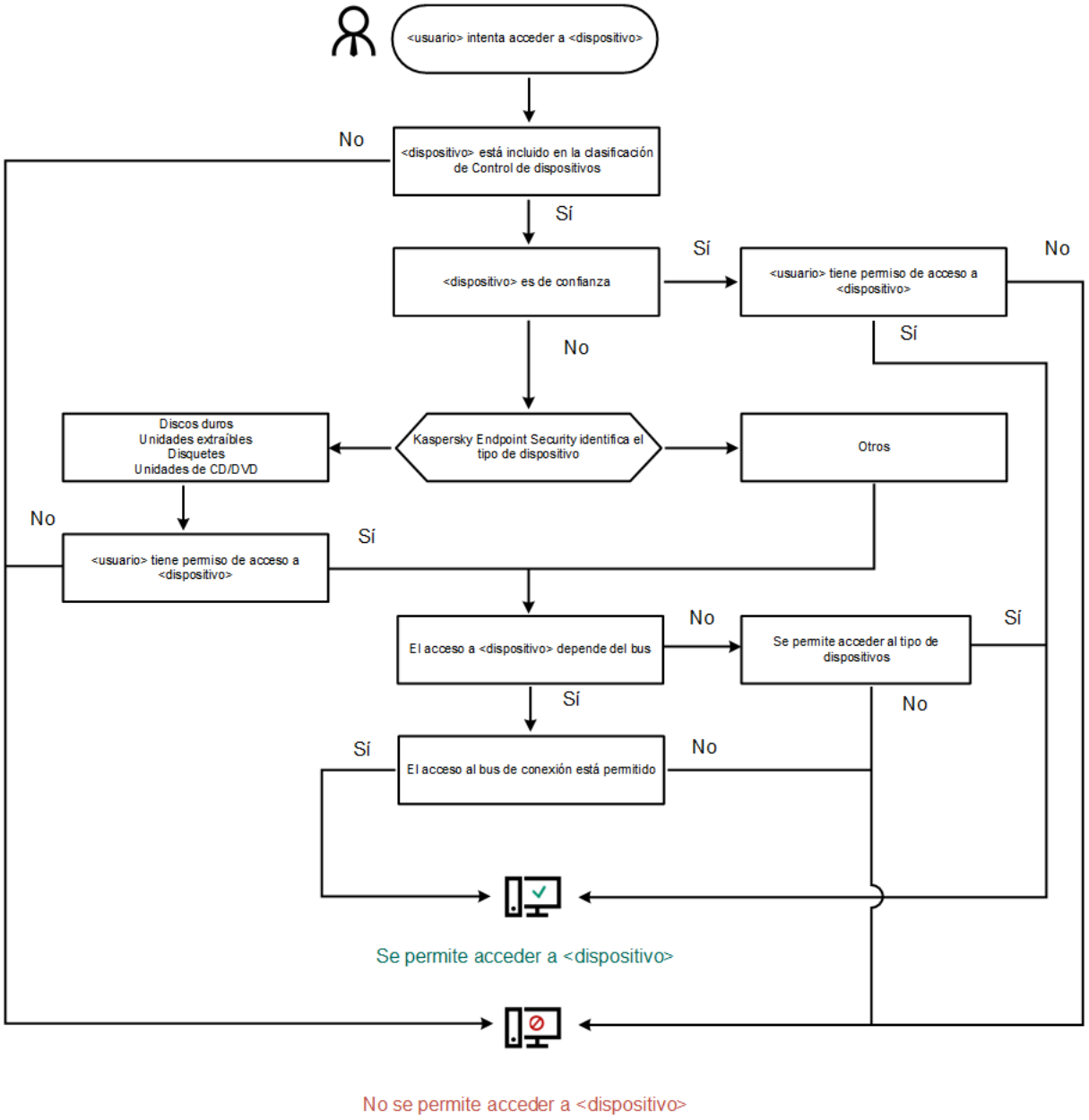
Cuando se conecta al equipo un dispositivo que está bloqueado por el Control de dispositivos, Kaspersky Endpoint Security bloqueará el acceso y mostrará que una notificación (consulte la figura a continuación).



Notificación del Control de dispositivos

Algoritmo de funcionamiento del Control de dispositivos

Kaspersky Endpoint Security decide si permitirá el acceso a un dispositivo después de que el usuario conecta el dispositivo al equipo de la siguiente imagen.



Algoritmo de funcionamiento del 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 un sistema de archivos se bloqueará solo la próxima vez que el dispositivo se conecte.

Si un usuario del equipo con Kaspersky Endpoint Security instalado debe solicitar acceso a un dispositivo que cree fue bloqueado por error, envíe al usuario las instrucciones para solicitar acceso.

Acerca de las reglas de acceso

Una *regla de acceso a dispositivos* es un grupo de configuraciones que determinan de qué forma los usuarios pueden acceder a los dispositivos que están instalados o conectados al equipo. Estas configuraciones incluyen el acceso a un dispositivo específico, una programación de acceso y permisos de lectura o escritura. No puede agregar un dispositivo que esté fuera de la clasificación del Control de dispositivos. Está permitido el acceso de todos los usuarios a dichos dispositivos.

Reglas de acceso a dispositivos

El grupo de configuraciones para una regla de acceso varía según el tipo de dispositivo (consulte la tabla a continuación).

Configuración de las reglas de acceso

Dispositivos	Control de acceso	Programación de acceso a un dispositivo	Asignación de usuarios y/o un grupo de usuarios	Prioridad	Lea/escriba el permiso
Discos duros	✓	✓	✓	✓	✓
Unidades extraíbles (incluidas las unidades flash USB)	✓	✓	✓	✓	✓
Disquetes	✓	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓	✓
Dispositivos portátiles (MTP)	✓	✓	✓	✓	✓
Impresoras locales	✓	–	✓	✓	–
Impresoras de red	✓	–	✓	✓	–
Módems	✓	–	–	–	–
Dispositivos de cinta	✓	–	–	–	–
Dispositivos multifunción	✓	–	–	–	–
Lectores de tarjetas inteligentes	✓	–	–	–	–
Dispositivos USB ActiveSync de Windows CE	✓	–	–	–	–
Adaptadores de red externos	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Cámaras y escáneres	✓	–	–	–	–

Reglas de acceso para redes Wi-Fi

Una regla de acceso para redes Wi-Fi determina si se permite (✓ estado) o se prohíbe (⊘ estado) el uso de redes Wi-Fi. Puede agregar una *red Wi-Fi de confianza* (estado) a una regla. El uso de una red Wi-Fi de confianza está permitido sin restricciones. Por defecto, una regla del acceso para redes Wi-Fi permite el acceso a cualquier red Wi-Fi.

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. Por defecto, se crean reglas que permiten el acceso a los buses para todos los buses de conexión incluidos en la clasificación del componente Control de dispositivos.

Las reglas del acceso a los buses de conexión determinan si se permite (✓ estado) o se prohíbe (⊘ estado) la conexión de dispositivos. La prioridad de las reglas de acceso al tipo de dispositivo es mayor que la prioridad de las reglas de acceso a los buses de conexión.

El teclado y el mouse no se pueden bloquear mediante Control de dispositivos. Si prohíbe el acceso al bus de conexión USB, el usuario seguirá trabajando con un teclado y un mouse conectados a través de USB. El componente Prevención de ataques BadUSB está diseñado para impedir que los dispositivos USB infectados que emulan un teclado se conecten al equipo.

Administrar el acceso a dispositivos según su tipo

Control de dispositivos permite administrar el acceso a los dispositivos por tipo. El sistema operativo determina el tipo de dispositivo al conectarlo. Puede buscar el tipo de dispositivo con la herramienta Administrador de dispositivos que se incluye en el sistema operativo. Para administrar el acceso a los dispositivos, debe configurar reglas. Una *regla de acceso a dispositivos* es un grupo de configuraciones que determinan de qué forma los usuarios pueden acceder a los dispositivos que están instalados o conectados al equipo. Estas configuraciones incluyen el acceso a un dispositivo específico, una programación de acceso y permisos de lectura o escritura. No puede agregar un dispositivo que esté fuera de la clasificación del Control de dispositivos. Está permitido el acceso de todos los usuarios a dichos dispositivos.

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 acceso completo a los dispositivos a todos los usuarios.

- **Bloquear**.

  Kaspersky Endpoint Security bloquea las conexiones del dispositivo. 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 según el estado de la conexión del bus. La aplicación también permite conectar dispositivos de confianza.

- **Por reglas**.

  En algunos tipos de dispositivos, puede elegir usuarios individuales o grupos de usuarios que pueden usar dispositivos, establecer una programación de acceso a dispositivos y configurar los permisos de lectura y escritura. La aplicación también permite conectar dispositivos de confianza.

Tenga cuidado al configurar el acceso a los dispositivos del tipo **Discos duros**. Si bloquea el acceso al disco del sistema, la aplicación puede causar un bloqueo (BSOD) cuando se inicia el sistema operativo.

Si un dispositivo no se corresponde con el esquema de clasificación de Control de dispositivos, no se puede restringir el acceso a dicho dispositivo.

Cómo administrar el acceso a los dispositivos según su 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 correspondiente 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 pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de Control de dispositivos.

6. Configure las reglas de acceso a los dispositivos:

   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por reglas**.

      Para seleccionar el modo de acceso **Por reglas**, haga doble clic para abrir las propiedades de las reglas 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, soportes extraíbles), puede configurar los permisos de acceso de usuarios individuales. También puede configurar una programación de acceso a dispositivos y los permisos de lectura y escritura.

      Puede agregar dispositivos a la lista de aplicaciones de confianza. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

   d. Si es necesario, configure las reglas de impresión.

   e. Si es necesario, configure las reglas de acceso a dispositivos con Bluetooth.

   f. Si es necesario, configure las reglas de conexión Wi-Fi del equipo.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo administrar el acceso a los dispositivos según su 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 ficha **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 Wi-Fi**.

   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 a los dispositivos:

   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Depende del bus** o **Personalizada**.

      Si el modo de acceso no aparece en el menú desplegable, haga doble clic en el tipo de dispositivo para abrir las propiedades de la regla de acceso.

   b. Si selecciona el modo de acceso **Depende 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, soportes extraíbles), puede configurar los permisos de acceso de usuarios individuales. También puede configurar una programación de acceso a dispositivos y los permisos de lectura y escritura.

      Puede agregar dispositivos a la lista de aplicaciones de confianza. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

   d. Si es necesario, configure las reglas de impresión.

   e. Si es necesario, configure las reglas de acceso a dispositivos con Bluetooth.

   f. Si es necesario, configure las reglas de conexión Wi-Fi del equipo.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo administrar el acceso a los dispositivos en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **Dispositivos y redes Wi-Fi**.

   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 a los dispositivos:

   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por reglas**.

      Si el modo de acceso no aparece en el menú desplegable, haga doble clic en el tipo de dispositivo 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, soportes extraíbles), puede configurar los permisos de acceso de usuarios individuales. También puede configurar una programación de acceso a dispositivos y los permisos de lectura y escritura.

   Puede agregar dispositivos a la lista de aplicaciones de confianza. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

d. Si es necesario, configure las reglas de impresión.

e. Si es necesario, configure las reglas de acceso a dispositivos con Bluetooth.

f. Si es necesario, configure las reglas de conexión Wi-Fi del equipo.

5. Guarde los cambios.

Entonces, cuando un usuario intente obtener acceso a un dispositivo, la aplicación bloqueará el acceso según las reglas. Kaspersky Endpoint Security también registra el evento correspondiente. Si desea conceder acceso a dispositivos individuales, puede agregar estos dispositivos a la lista de dispositivos de confianza.

Administrar el acceso a los dispositivos mediante el bus de conexión

Para editar una regla de acceso a buses de conexión:

1. En la ventana principal de la aplicación 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 que se abre 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 desea editar.

5. En la columna **Acceso**, seleccione si desea permitir o no el acceso al bus de conexión: **Permitir** o **Bloquear**.

   Si cambió 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.

Diferentes derechos de acceso de usuarios a los dispositivos

Puede configurar los derechos de acceso de los usuarios según el tipo de dispositivo o para dispositivos de confianza.

Diferentes derechos de acceso de usuarios por tipo de dispositivo

Control de dispositivos permite configurar los derechos de acceso de los usuarios a los datos en los *dispositivos de almacenamiento*. Para estos dispositivos, puede configurar permisos de lectura y escritura. Control de dispositivos admite los siguientes tipos de *dispositivos de almacenamiento*:

- Discos duros.
- Unidades extraíbles (incluidas las unidades extraíbles USB).
- Disquetes.
- Unidades de CD/DVD.
- Dispositivos portátiles (MTP). Los dispositivos portátiles (MTP) abarcan, entre otros, dispositivos móviles, cámaras fotográficas, reproductores multimedia.

De esta manera, puede, por ejemplo, permitir que solo el grupo de administradores utilice soportes extraíbles. Para otros dispositivos, puede denegar o permitir el acceso a todos los usuarios. También puede configurar los derechos de acceso de los usuarios para usar impresoras.

Cómo configurar los derechos de acceso de los usuarios a los datos de 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 correspondiente 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 pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de Control de dispositivos.
6. Para configurar las 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 **Agregar**.

      Esto abre una ventana para agregar una nueva regla de acceso a dispositivos de almacenamiento.

   b. En el campo **Prioridad de la regla**, establezca 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 agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

d. Haga clic en **Aceptar**.

8. En **Programaciones para la regla de acceso seleccionada**, configure una programación de acceso a dispositivos de almacenamiento para los usuarios.

   Por ejemplo, puede permitir que los usuarios usen dispositivos de almacenamiento únicamente durante el horario laboral.

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 íconos de candado y guarde los cambios.

Cómo configurar los derechos de acceso de los usuarios a los datos de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En el bloque **Reglas de acceso a dispositivos**, en la tabla de reglas de acceso, abra las propiedades de las reglas de acceso para los dispositivos de almacenamiento.

6. En el bloque **Reglas de acceso a dispositivos**, seleccione **Personalizada**.

7. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Usuarios y sus derechos**, haga clic en el botón **Agregar**.

      Esto abre una ventana para agregar una nueva regla de acceso a dispositivos de almacenamiento.

   b. En el campo **Prioridad**, establezca 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 agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

d. En **Programación de acceso**, configure una programación de acceso a dispositivos de almacenamiento para los usuarios.

Por ejemplo, puede permitir que los usuarios usen dispositivos de almacenamiento únicamente durante el horario laboral.

e. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Leer**/**Escribir**).

f. Haga clic en **Guardar**.

8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar los derechos de acceso de los usuarios a los datos de los dispositivos de almacenamiento en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **Dispositivos y redes Wi-Fi**.

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 las 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 **Agregar**.

Esto abre una ventana para agregar una nueva regla de acceso a dispositivos de almacenamiento.

b. En el campo **Prioridad**, establezca 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 agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

c. En **Usuarios**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory o ingresar el nombre de un usuario local de forma manual. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

d. Haga clic en **Aceptar**.

6. En **Programación de acceso a dispositivos**, configure una programación de acceso a dispositivos de almacenamiento para los usuarios.

   Por ejemplo, puede permitir que los usuarios usen dispositivos de almacenamiento únicamente durante el horario laboral.

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.

Diferentes derechos de acceso de usuarios a dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento. Puede conceder acceso a los dispositivos de confianza a un usuario específico, a un grupo de usuarios o a todos los usuarios de su organización. Puede configurar los derechos de acceso de los usuarios en las propiedades del dispositivo de confianza.

Administrar el acceso a los dispositivos móviles

Kaspersky Endpoint Security le permite controlar el acceso a los datos en dispositivos móviles con Android e iOS. Los dispositivos móviles pertenecen a la categoría de dispositivos portátiles (MTP). Por lo tanto, para configurar el acceso a 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 Android Debug Bridge (ADB), iTunes o sus aplicaciones equivalentes están instaladas en el equipo, 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 el resto de los casos, el Control de dispositivos permite el acceso a los dispositivos móviles de acuerdo con las reglas de acceso de dispositivos portátiles (MTP).

Acceso a los dispositivos móviles

Los dispositivos móviles pertenecen a la categoría de dispositivos portátiles (MTP), por lo 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 usando 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 conectar dispositivos móviles según el estado de conexión de USB (**Permitir** ✓ o **Bloquear** ⊘).

- **Por 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 acceder a dispositivos móviles, y configurar una programación de acceso para dispositivos móviles. También puede restringir el acceso a los datos en dispositivos móviles a través de las aplicaciones ADB e iTunes.

Configurar 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 programación para la aplicación de las reglas. En el caso de los dispositivos iTunes, no puede hacerlo. 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 correspondiente 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 tipo de dispositivo **Dispositivos portátiles (MTP)**, configure el modo de acceso a dispositivos móviles: **Permitir** ✓, **Bloquear** ⊘ o **Depende del bus de conexión**.

6. Para configurar las reglas de acceso a dispositivos móviles, haga doble clic para abrir la lista de reglas.

7. Configure la regla de acceso de dispositivos móviles:

   a. En el bloque **Reglas de acceso**, haga clic en el botón **Agregar**.

      Esto abre una ventana para agregar una nueva regla de acceso a dispositivos móviles.

   b. En el campo **Prioridad**, establezca la prioridad de escritura de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura/acceso ADB) y prioridad.

      Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

      La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

   d. Haga clic en **Aceptar**.

8. En **Programaciones para la regla de acceso seleccionada**, configure una programación de acceso a dispositivos móviles para los usuarios.

   No es posible configurar una programación de acceso separado para dispositivos ADB. Puede configurar una programación de 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 (**Lectura**/**Escritura**).

10. Configure el acceso a los datos en un dispositivo móvil a través de la aplicación ADB mediante la casilla **Acceder a través de ADB**.

    Si la casilla no está seleccionada, la aplicación ADB no podrá detectar el dispositivo móvil cuando esté conectado.

11. En **Acceso a través de 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 a dispositivos móviles a través de la aplicación iTunes para todos los usuarios. No es posible configurar una programación de acceso aparte 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 ficha **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 vínculo **Dispositivos y redes Wi-Fi**.

   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 de dispositivos móviles: **Permitir**, **Bloquear**, **Depende del bus** o **Personalizada**.

8. Utilice el interruptor **Acceso a través de iTunes para todos los usuarios HABILITADO** 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 a dispositivos móviles a través de la aplicación iTunes para todos los usuarios. No es posible configurar una programación de acceso aparte para dispositivos iTunes.

9. Si selecciona el modo **Personalizada**, debe agregar reglas de acceso para los dispositivos. Para ello, en **Usuarios y sus derechos**, haga clic en el botón **Agregar** y configure la regla de acceso de dispositivos móviles:

   a. En el campo **Prioridad**, establezca la prioridad de escritura de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura/acceso ADB) y prioridad.

      Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

      La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

   b. En **Usuario o grupo**, seleccione los usuarios o los grupos de usuarios que podrán acceder a los dispositivos móviles. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

c. En **Programación de acceso**, configure una programación de acceso a dispositivos móviles para los usuarios.

> No es posible configurar una programación de acceso separado para dispositivos ADB. Puede configurar una programación de 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 (**Leer**/**Escribir**).

e. Configure el acceso a los datos en un dispositivo móvil a través de la aplicación ADB mediante la casilla **Acceder a través de ADB**.

Si la casilla no está seleccionada, la aplicación ADB no podrá detectar el dispositivo móvil cuando esté conectado.

10. Guarde los cambios.

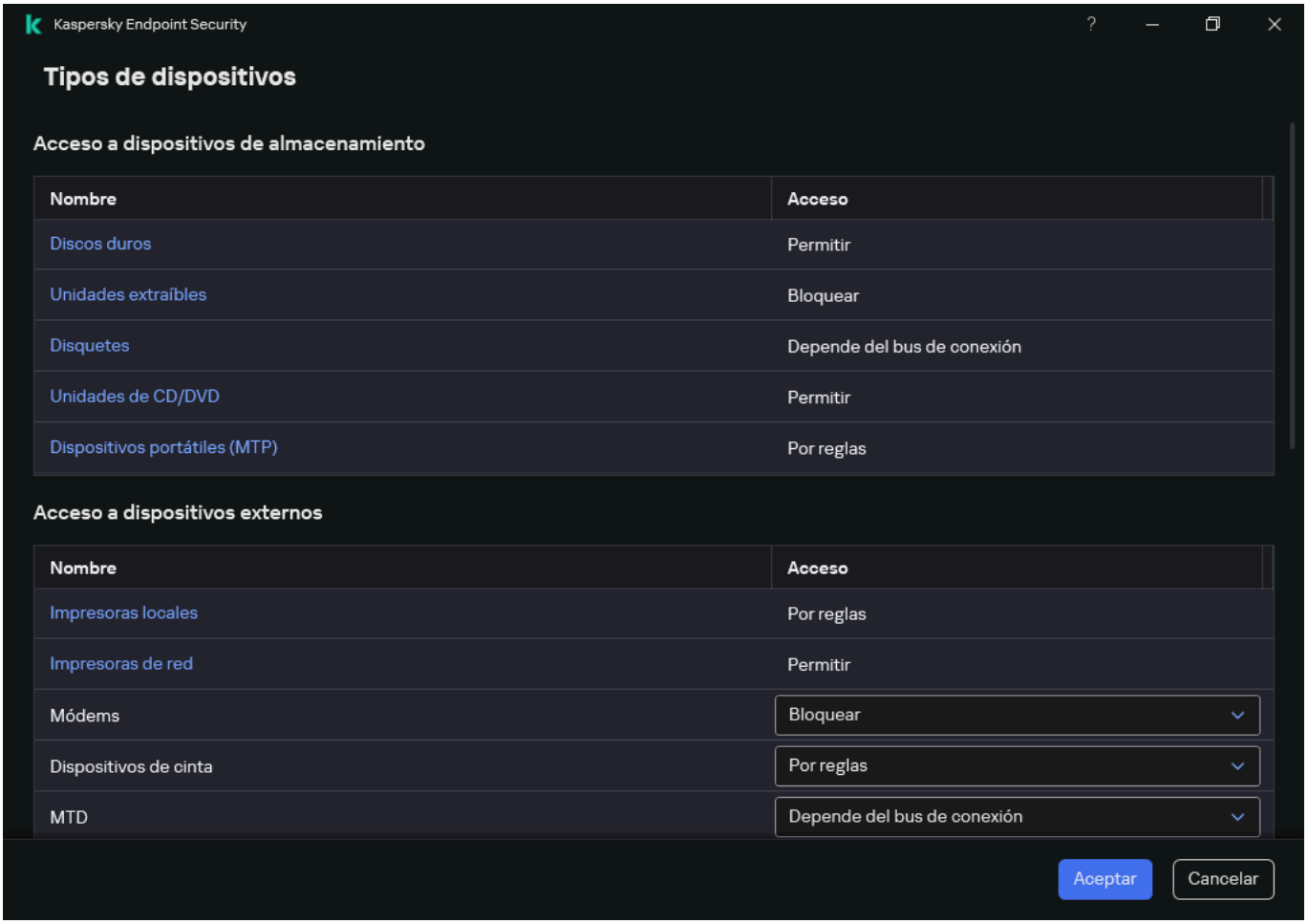
Cómo configurar reglas de acceso a dispositivos móviles en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 Wi-Fi**.

La ventana que se abre 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 vínculo **Dispositivos portátiles (MTP)**.

   Esto abre una ventana que contiene las reglas de acceso de dispositivos portátiles (MTP).

5. En **Acceso**, configure el modo de acceso de los dispositivos móviles: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por reglas**.

6. Si selecciona el modo **Por reglas**, debe agregar reglas de acceso para los dispositivos:

   a. En el bloque **Derechos de los usuarios**, haga clic en el botón **Agregar**.

      Esto abre una ventana para agregar una nueva regla de acceso a dispositivos móviles.

   b. En el campo **Prioridad**, establezca la prioridad de escritura de la regla. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura/acceso ADB) y prioridad.

      Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

      La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

   c. En **Condición**, active la regla de acceso a los dispositivos móviles.

   d. En **Reglas de acceso**, configure los permisos de acceso a los dispositivos móviles para los 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 mediante la casilla **Acceso a través de ADB**.

        Si la casilla no está seleccionada, la aplicación ADB no podrá detectar el dispositivo móvil cuando esté conectado.

   e. En **Usuarios**, seleccione los usuarios o los grupos de usuarios que podrán acceder a los dispositivos móviles. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

   f. En **Programación de acceso a dispositivos**, configure una programación de acceso a los dispositivos para los usuarios.

      No es posible configurar una programación de acceso separado para dispositivos ADB. Puede configurar una programación de acceso común para dispositivos ADB y dispositivos portátiles (MTP).

g. En **Acceso a través de 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 a dispositivos móviles a través de la aplicación iTunes para todos los usuarios. No es posible configurar una programación de acceso aparte para dispositivos iTunes.

7. Guarde los cambios.

Como resultado, el acceso de los usuarios a los dispositivos móviles está restringido de acuerdo con las reglas. Si prohibió 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

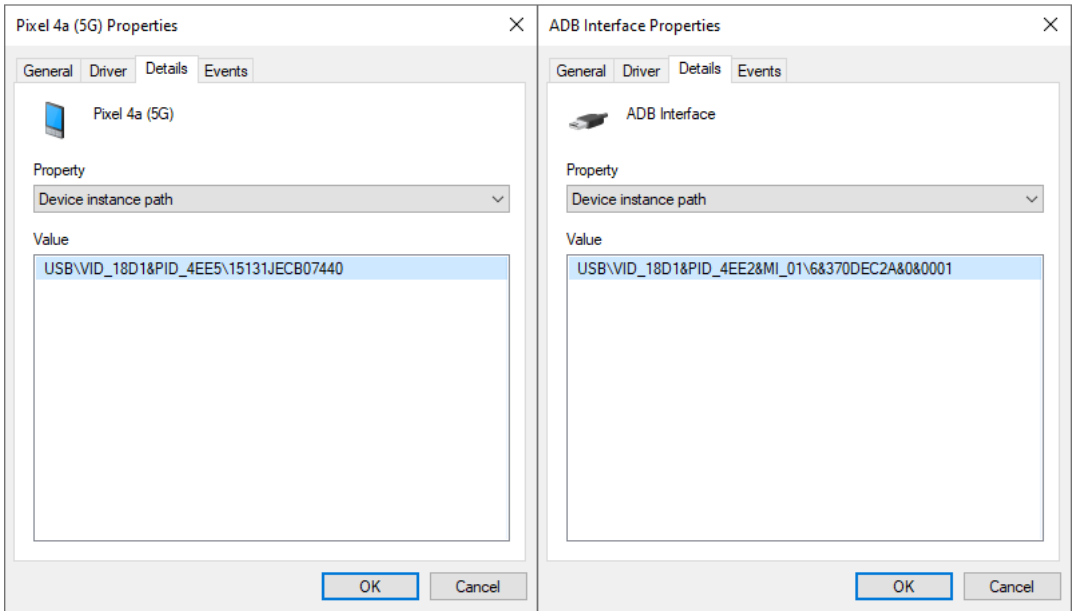
Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

El procedimiento para agregar dispositivos móviles de confianza es exactamente igual al de otros tipos de dispositivos de confianza. Puede agregar un dispositivo móvil por Id. o por modelo de dispositivo.

Para agregar un dispositivo móvil de confianza por ID, necesitará un ID único (Hardware ID: HWID). Para buscar el Id. en las propiedades del dispositivo, utilice las herramientas del sistema operativo (vea la figura a continuación). Puede hacerlo con la herramienta Administrador de dispositivos. 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 verse así: `15131JECB07440`. El Id. de un dispositivo ADB puede verse así: `6&370DEC2A&0&0001`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id. También puede usar máscaras.

> Si conecta un dispositivo al equipo y luego instala las aplicaciones ADB o iTunes, el identificador único de dicho dispositivo podría restablecerse. Si esto ocurre, Kaspersky Endpoint Security lo identificará como dispositivo nuevo. Si el dispositivo estaba catalogado como de confianza, deberá agregarlo a la lista de dispositivos de confianza una segunda vez.

Para agregar un dispositivo móvil de confianza por modelo de dispositivo, necesitará su Vendor ID (VID) y Product ID (PID). Puede buscar los Id. en las propiedades del dispositivo utilizando las herramientas del sistema operativo (vea la figura a continuación). Los valores VID y PID deben especificarse en este formato: `VID_18D1&PID_4EE5`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.



Id. de dispositivo en el Administrador de dispositivos

Administrar el acceso a los dispositivos Bluetooth

Kaspersky Endpoint Security permite administrar el acceso a dispositivos Bluetooth. Los dispositivos Bluetooth incluyen teclados, mouses, auriculares, impresoras, etc. inalámbricos. También puede utilizar Bluetooth para comunicarse, por ejemplo, con un dispositivo móvil.

Cuando se conectan o desconectan los dispositivos Bluetooth, la aplicación puede crear múltiples eventos sobre el dispositivo. El motivo 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 se conecta el dispositivo como un dispositivo independiente. Es por eso que la aplicación crea un evento para cada uno de los dispositivos detectados.

Puede seleccionar uno de los siguientes modos de acceso a dispositivos Bluetooth:

- **Permitir y no registrar** . Kaspersky Endpoint Security permite conectar cualquier dispositivo Bluetooth y no guarda información sobre la conexión en el registro de eventos. Puede conectar dispositivos de entrada Bluetooth (teclados, mouses, etc.), enviar datos a través de Bluetooth y administrar otros dispositivos Bluetooth (auriculares, audífonos, etc.).

- **Permitir** . Kaspersky Endpoint Security permite conectar cualquier dispositivo Bluetooth. Puede conectar dispositivos de entrada Bluetooth (teclados, mouses, etc.), enviar datos a través de Bluetooth y administrar otros dispositivos Bluetooth (auriculares, audífonos, etc.).

- **Bloquear** . Kaspersky Endpoint Security restringe el acceso a los dispositivos Bluetooth. Solo se permite la conexión de dispositivos de entrada Bluetooth (la clase Human Interface Devices). Estos dispositivos incluyen teclados, ratones, joysticks, etc.

No es posible crear una lista de dispositivos Bluetooth de confianza. Si tiene acceso restringido a dispositivos Bluetooth, solo puede conectar dispositivos de entrada Bluetooth.

Cómo configurar reglas de acceso a dispositivos 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 correspondiente 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 de tipo de dispositivo **Bluetooth**, configure el modo de acceso a dispositivos Bluetooth: **Permitir** , **Bloquear** , **Permitir y no registrar** .

7. Si selecciona el modo **Bloquear**, puede permitir la conexión solo de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para eso, en **Exclusiones**, seleccione la casilla de verificación **Dispositivos de entrada (ratones y teclados)**.

8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar reglas de acceso a dispositivos 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 ficha **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 vínculo **Dispositivos y redes Wi-Fi**.

   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 a dispositivos Bluetooth.

7. Configure el modo de acceso de dispositivos Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**.

8. Si selecciona el modo **Bloquear**, puede permitir la conexión solo de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para eso, en **Exclusiones**, seleccione la casilla de verificación **Dispositivos de entrada (ratones y teclados)**.

9. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

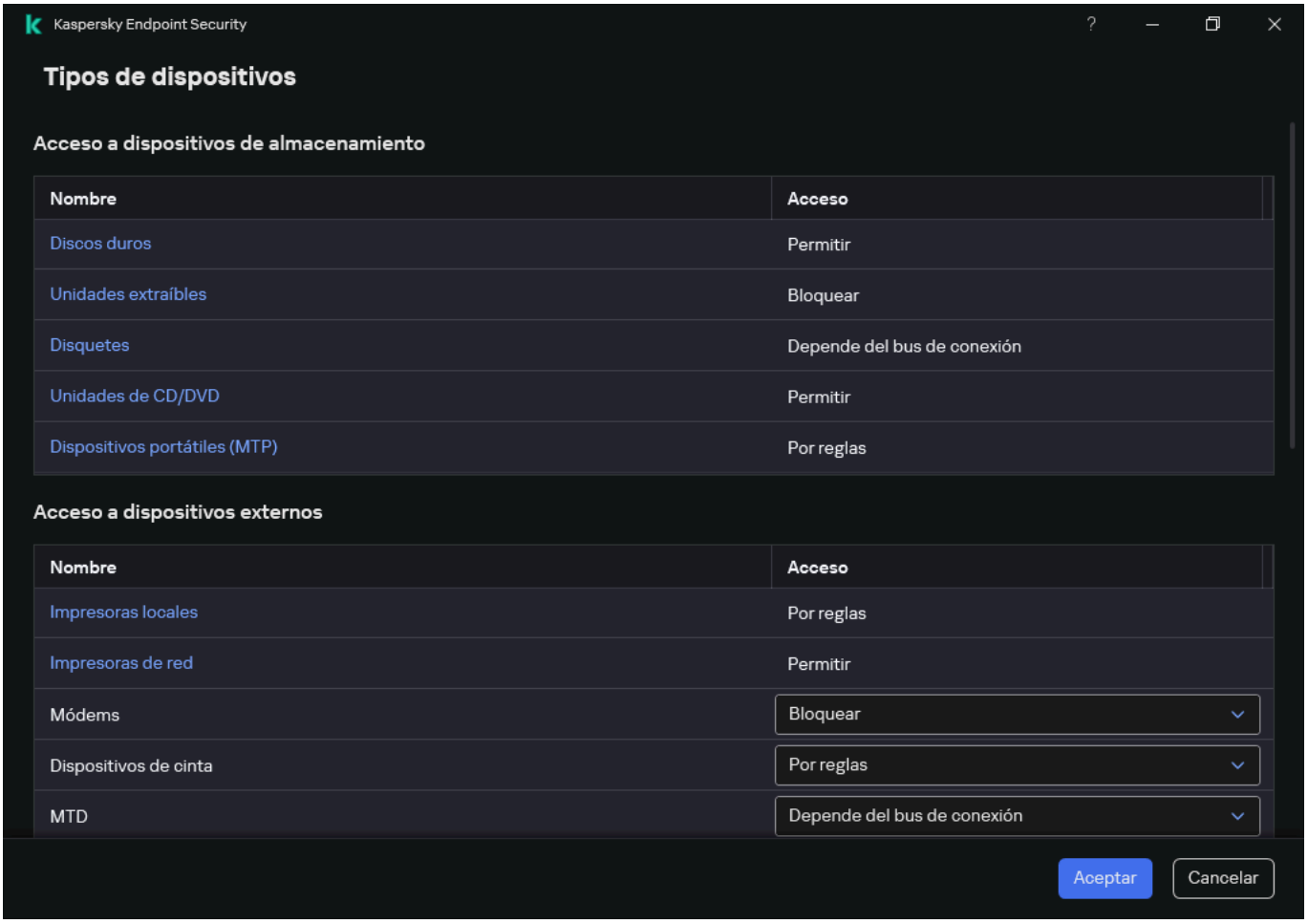
Cómo configurar reglas de acceso a dispositivos Bluetooth en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 Wi-Fi**.

   La ventana que se abre 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 vínculo **Bluetooth**.

   Esto abre la configuración de acceso a dispositivos Bluetooth.

5. En **Acceso**, configure el modo de acceso de los dispositivos Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**.

6. Si selecciona el modo **Bloquear**, puede permitir la conexión solo de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para eso, en **Exclusiones**, seleccione la casilla de verificación **Dispositivos de entrada (ratones y teclados)**.

7. Guarde los cambios.

Control de impresión

El control de impresión no es compatible con equipos basados en la arquitectura Arm.

Puede usar Control de impresión para configurar el acceso de los usuarios a las impresoras locales y de red.

Control de impresoras locales

Kaspersky Endpoint Security permite configurar el acceso a las impresoras locales en dos niveles: *conectando* e *impresión*.

Kaspersky Endpoint Security controla la conexión de la impresora local a través de los siguientes buses: USB, puerto serie (COM), puerto paralelo (LPT).

Kaspersky Endpoint Security controla la conexión de impresoras locales a los puertos COM y LPT solo a nivel del bus. Por lo tanto, para evitar conexiones de impresora mediante puertos COM y LPT, debe seleccionar el modo de acceso para impresoras locales Depende del bus de conexión y prohibir las conexiones a los buses de COM y LPT.

Para impresoras conectadas a USB, la aplicación ejerce 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 por USB:

- **Permitir** ✓. Kaspersky Endpoint Security otorga acceso total a las impresoras locales a todos los usuarios. Los usuarios pueden conectar impresoras e imprimir documentos con los medios que proporciona el sistema operativo.

- **Bloquear** ⊘. Kaspersky Endpoint Security bloquea la conexión de impresoras locales. La aplicación solo permite conectar impresoras de confianza.

- **Depende del bus de conexión**. Kaspersky Endpoint Security permite conectar impresoras locales según el estado de conexión del bus USB (**Permitir** o **Bloquear**).

- **Por reglas**. Para controlar la impresión, debe agregar *reglas de impresión*. En estas reglas, puede seleccionar usuarios o un grupo de usuarios para los que desea permitir 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 para las 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 solo permite el acceso a las impresoras de confianza.

- **Por reglas**. Kaspersky Endpoint Security otorga acceso a la impresión según las reglas de impresión. En las reglas, puede seleccionar usuarios o un grupo de usuarios a los que se les permitirá o impedirá imprimir documentos en una impresora de red.

Agregar reglas de impresión para impresoras

Cómo agregar 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 correspondiente 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 dispositivos **Impresoras locales** y **Impresoras de red**, configure el modo de acceso para 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. Si desea configurar reglas de impresión en impresoras locales y de red, haga doble clic en las listas de reglas para abrirlas.

7. Seleccione **Por reglas** como modo de acceso a la impresora.

8. Seleccione los usuarios o los grupos de usuarios a los que desea aplicar la regla de acceso al dispositivo.

   a. Haga clic en **Agregar**.

      Se abre una ventana para agregar una nueva regla de acceso al dispositivo.

   b. Asigne una prioridad a la entrada de regla. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (permitir/bloquear) y prioridad.

      Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

      La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

   c. En **Acción**, configure el acceso del usuario a las impresoras.

   d. Haga clic en **Usuarios y grupos** y seleccione los usuarios o los grupos de usuarios que podrán acceder a las impresoras. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar 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 ficha **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 vínculo **Dispositivos y redes Wi-Fi**.

   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 **Impresoras locales** o **Impresoras de red**.

   Esto abre las reglas de acceso a la impresora.

7. Configure el modo de acceso para las impresoras relevantes: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Depende del bus** (solo para impresoras locales) o **Personalizada**.

8. Si selecciona el modo **Personalizada**, debe agregar reglas de impresión para impresoras locales o de red. Para ello, haga clic en el botón **Agregar** en la tabla de reglas de impresión.

   Se abre la configuración de la nueva regla de impresión.

9. Asigne una prioridad a la entrada de regla. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (permitir/bloquear) y prioridad.

   Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

   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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

   La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

10. En **Acción**, configure el acceso del usuario a las impresoras.

11. En **Usuario o grupo**, seleccione los usuarios o los grupos de usuarios que podrán acceder a las impresoras. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

12. Guarde los cambios.

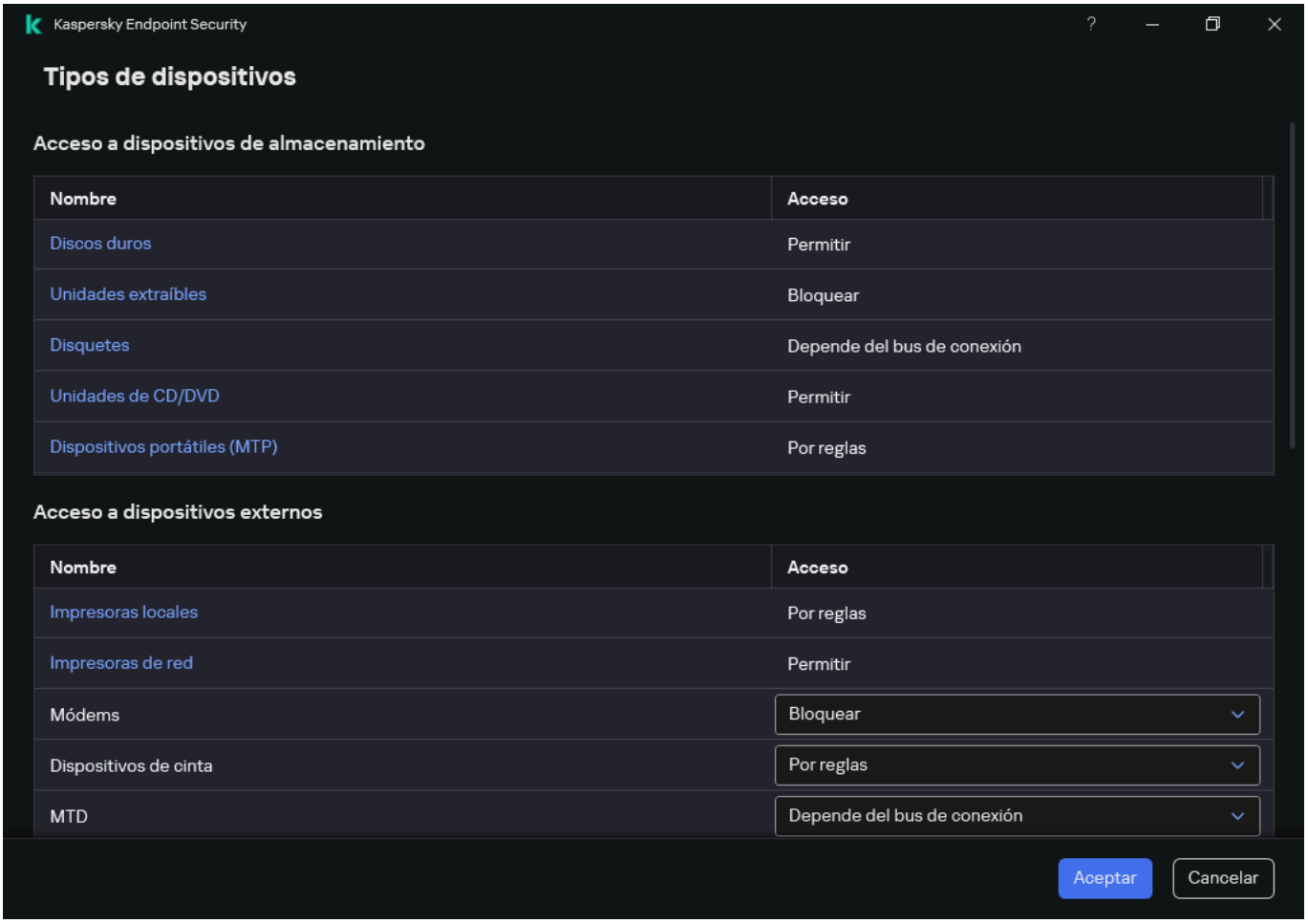
Cómo agregar reglas de impresión en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 Wi-Fi**.

La ventana que se abre 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 **Impresoras de red**.

   Se abre una ventana con las reglas de acceso a la impresora.

5. En **Acceso a las impresoras locales** o **Acceso a las impresoras de red**, configure el modo de acceso para las impresoras: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Depende del bus de conexión** (solo para impresoras locales) o **Por reglas**.

6. Si selecciona el modo **Por reglas**, debe agregar reglas de impresión para las impresoras. Seleccione los usuarios o los grupos de usuarios a los que desea aplicar la regla de acceso al dispositivo.

   a. Haga clic en **Agregar**.

      Se abre una ventana para agregar una nueva regla de acceso al dispositivo.

   b. Asigne una prioridad a la entrada de regla. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, permisos (permitir/bloquear) y prioridad.

      Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security le permite asignar prioridad con valores de 0-10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      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 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

c. En **Acción**, configure los permisos de usuario para acceder a las impresoras.

d. En **Usuarios y grupos**, seleccione los usuarios o los grupos de usuarios que podrán acceder a las impresoras. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

7. Guarde los cambios.

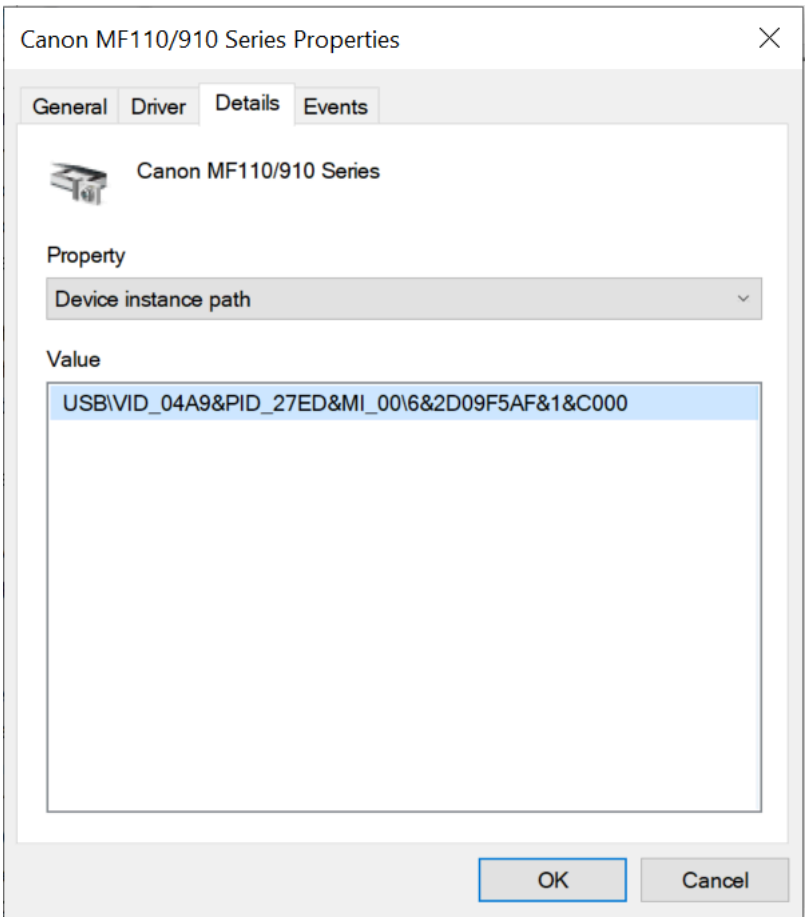
Impresoras de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

El procedimiento para agregar impresoras de confianza es exactamente igual al de otros tipos de dispositivos de confianza. Puede agregar impresoras locales por Id. o por modelo de dispositivo. Solo puede agregar impresoras de red por Id. de dispositivo.

Para agregar una impresora local de confianza por ID, necesitará un ID único (Hardware ID: HWID). Para buscar el Id. en las propiedades del dispositivo, utilice las herramientas del sistema operativo (vea la figura a continuación). Puede hacerlo con la herramienta Device Manager. El Id. de una impresora local puede verse así: `6&2D09F5AF&1&C000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id. También puede usar máscaras.

Para agregar una impresora local de confianza por modelo de dispositivo, necesitará su Vendor ID (VID) y Product ID (PID). Puede buscar los Id. en las propiedades del dispositivo utilizando las herramientas del sistema operativo (vea la figura a continuación). Los valores VID y PID deben especificarse en este formato: `VID_04A9&PID_27FD`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.



Id. de dispositivo en el Administrador de dispositivos

Para agregar una impresora de red de confianza, necesitará su Id. de dispositivo. Para las impresoras de red, el Id. de dispositivo puede ser el nombre de la red de la impresora (nombre de la impresora compartida), la dirección IP de la impresora o la dirección URL de la impresora.

Control de conexiones Wi-Fi

El Control de dispositivos permite administrar la conexión Wi-Fi del equipo (computadora portátil). Las redes Wi-Fi públicas pueden ser inseguras y su uso puede provocar la pérdida de datos. El Control de dispositivos le permite bloquear a un usuario para que no se conecte a Wi-Fi o permitir que se conecte solo a redes de confianza. Por ejemplo, puede permitir conectarse solo a la red Wi-Fi corporativa que sea lo suficientemente segura. El Control de dispositivos bloqueará el acceso a todas las redes Wi-Fi salvo por las especificadas en la lista de confianza.

En los equipos que ejecutan Windows 11, debe habilitar los servicios de ubicación para controlar las conexiones Wi-Fi. Para hacerlo, debe habilitar el interruptor **Servicios de ubicación** en la configuración del sistema operativo (**Configuración** → **Privacidad y seguridad** → **Ubicación**). Si los servicios de ubicación están deshabilitados, Kaspersky Endpoint Security no controla las conexiones a redes Wi-Fi.

Cómo restringir las conexiones Wi-Fi 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 correspondiente 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 **Wi-Fi**, seleccione la acción de Control de dispositivos que se realiza al conectarse a Wi-Fi: **Permitir** (✓), **Bloquear** (⊘) o **Bloquear con excepciones** (▤).

6. Si seleccionó la opción **Bloquear con excepciones**, cree una lista de redes Wi-Fi de confianza:

   a. Haga doble clic para abrir la lista de redes Wi-Fi de confianza.

   b. En el bloque **Redes Wi-Fi de confianza**, haga clic en el botón **Agregar**.

   c. Se abre una ventana en la que puede configurar la red Wi-Fi de confianza (vea la figura a continuación):

   - **Nombre de la red**. Nombre o SSID (Service Set Identifier) de la red Wi-Fi.

   - **Tipo de autenticación**. Tipo de autenticación utilizado cuando se conecta a la red Wi-Fi.

     > A partir de la versión 12.0 de Kaspersky Endpoint Security para Windows, se agregó la compatibilidad con el protocolo WPA3 a la aplicación. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en una computadora, el protocolo WPA2 se selecciona en computadoras con Kaspersky Endpoint Security versión 11.11.0 y anteriores. Para las versiones 12.0 a 12.1, se selecciona WPA2/WPA3; para las versiones 12.2 y posteriores, se selecciona WPA3.

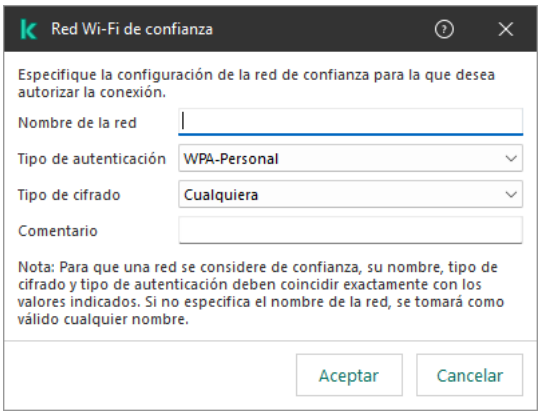
   - **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico de Wi-Fi.

   - **Comentario**. Más información sobre la red Wi-Fi agregada.

   Puede ver la configuración de la red Wi-Fi de confianza en la configuración del router.

   > Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

7. Guarde los cambios.



Configuración de la red Wi-Fi de confianza

Cómo restringir las conexiones Wi-Fi 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 ficha **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 Wi-Fi**.

   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 Wi-Fi**, haga clic en el vínculo **Wi-Fi**.

7. En la ventana que se abre, seleccione la acción de Control de dispositivos que se realizará al conectarse a una red Wi-Fi: **Permitir**, **Bloquear**, o **Bloquear con exclusiones**.

8. Si seleccionó la opción **Bloquear con exclusiones**, cree una lista de redes Wi-Fi de confianza:

   a. Haga doble clic para abrir la lista de redes Wi-Fi de confianza.

   b. En el bloque **Redes Wi-Fi de confianza**, haga clic en el botón **Agregar**.

   c. Se abre una ventana en la que puede configurar la red Wi-Fi de confianza (vea la figura a continuación):

   - **Nombre**. Nombre o SSID (Service Set Identifier) de la red Wi-Fi.

   - **Tipo de autenticación**. Tipo de autenticación utilizado cuando se conecta a la red Wi-Fi.

     A partir de la versión 12.0 de Kaspersky Endpoint Security para Windows, se agregó la compatibilidad con el protocolo WPA3 a la aplicación. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en una computadora, el protocolo WPA2 se selecciona en computadoras con Kaspersky Endpoint Security versión 11.11.0 y anteriores. Para las versiones 12.0 a 12.1, se selecciona WPA2/WPA3; para las versiones 12.2 y posteriores, se selecciona WPA3.

- **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico de Wi-Fi.
- **Comentario**. Más información sobre la red Wi-Fi agregada.

Puede ver la configuración de la red Wi-Fi de confianza en la configuración del router.

> Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

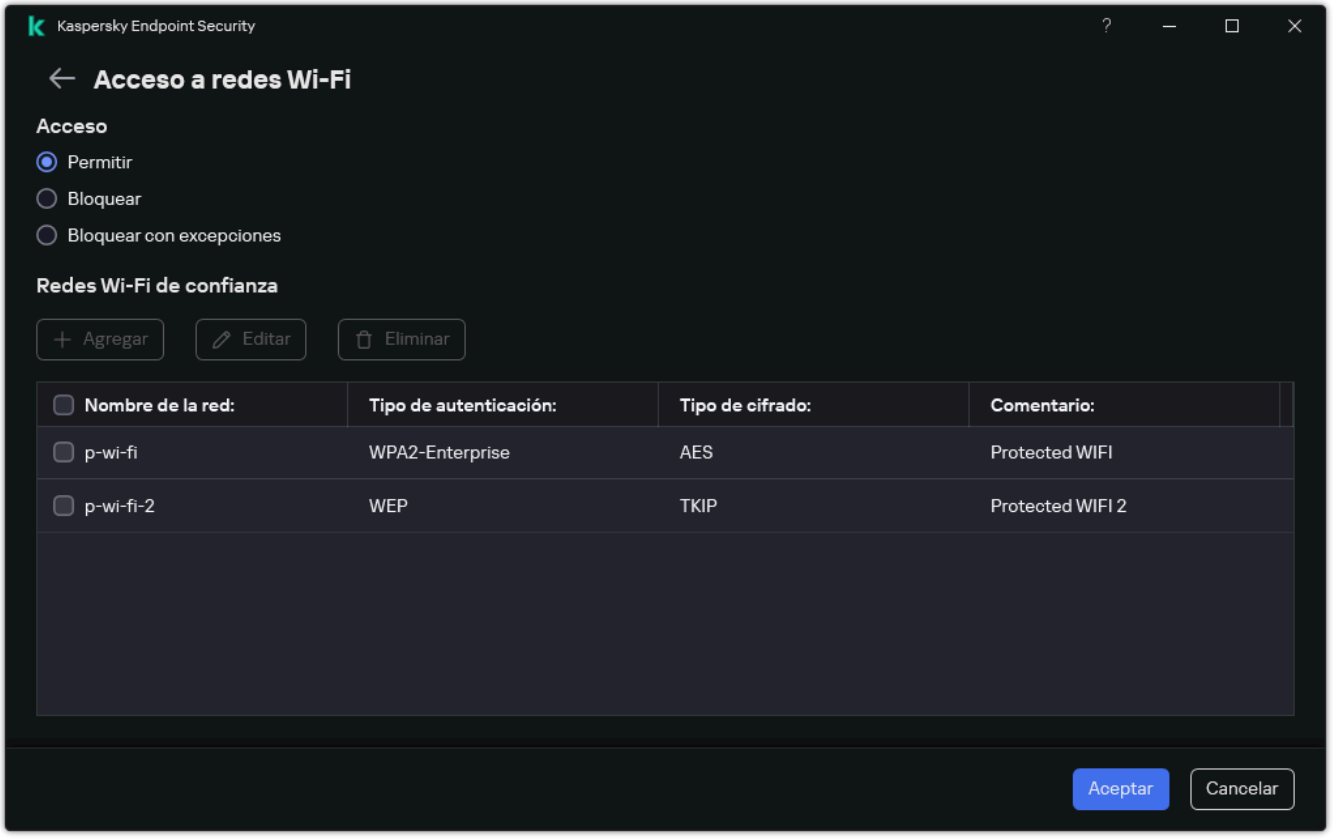
9. Guarde los cambios.

Cómo restringir las conexiones Wi-Fi en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 Wi-Fi**.

   La ventana que se abre 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 Wi-Fi**, haga clic en el vínculo **Wi-Fi**.

   La ventana que se abre muestra las reglas de acceso a la red Wi-Fi.



Configuración de acceso Wi-Fi

5. En **Acceso**, seleccione la medida de Control de dispositivos tomada cuando se conecta a la red Wi-Fi: **Permitir**, **Bloquear**, o **Bloquear con excepciones**.

6. Si seleccionó la opción **Bloquear con excepciones**, cree una lista de redes Wi-Fi de confianza:

   a. En el bloque **Redes Wi-Fi de confianza**, haga clic en el botón **Agregar**.

   b. Se abre una ventana en la que puede configurar la red Wi-Fi de confianza (vea la figura a continuación):

   - **Nombre de la red**. Nombre o SSID (Service Set Identifier) de la red Wi-Fi.
   - **Tipo de autenticación**. Tipo de autenticación utilizado cuando se conecta a la red Wi-Fi.

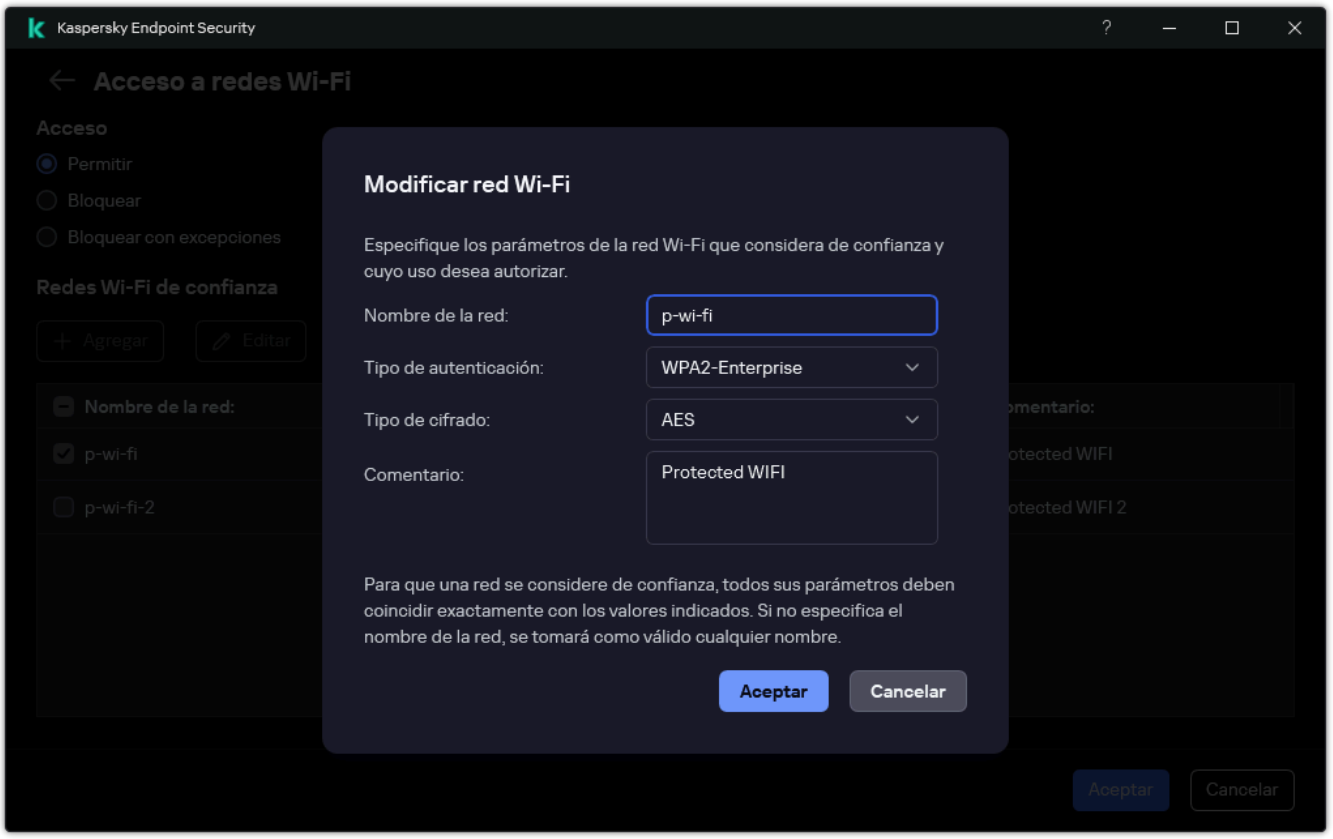
     > A partir de la versión 12.0 de Kaspersky Endpoint Security para Windows, se agregó la compatibilidad con el protocolo WPA3 a la aplicación. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en una computadora, el protocolo WPA2 se selecciona en computadoras con Kaspersky Endpoint Security versión 11.11.0 y anteriores. Para las versiones 12.0 a 12.1, se selecciona WPA2/WPA3; para las versiones 12.2 y posteriores, se selecciona WPA3.

   - **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico de Wi-Fi.
   - **Comentario**. Más información sobre la red Wi-Fi agregada.

   Puede ver la configuración de la red Wi-Fi de confianza en la configuración del router.

   > Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

7. Guarde los cambios.



Configuración de la red Wi-Fi de confianza

Como resultado, cuando un usuario intenta conectarse a una red Wi-Fi que no figura como confiable, la aplicación bloquea la conexión y muestra una notificación (ver la figura a continuación).

Notificación del Control de dispositivos

Supervisar el uso de unidades extraíbles

Supervisar el uso de unidades extraíbles incluye:

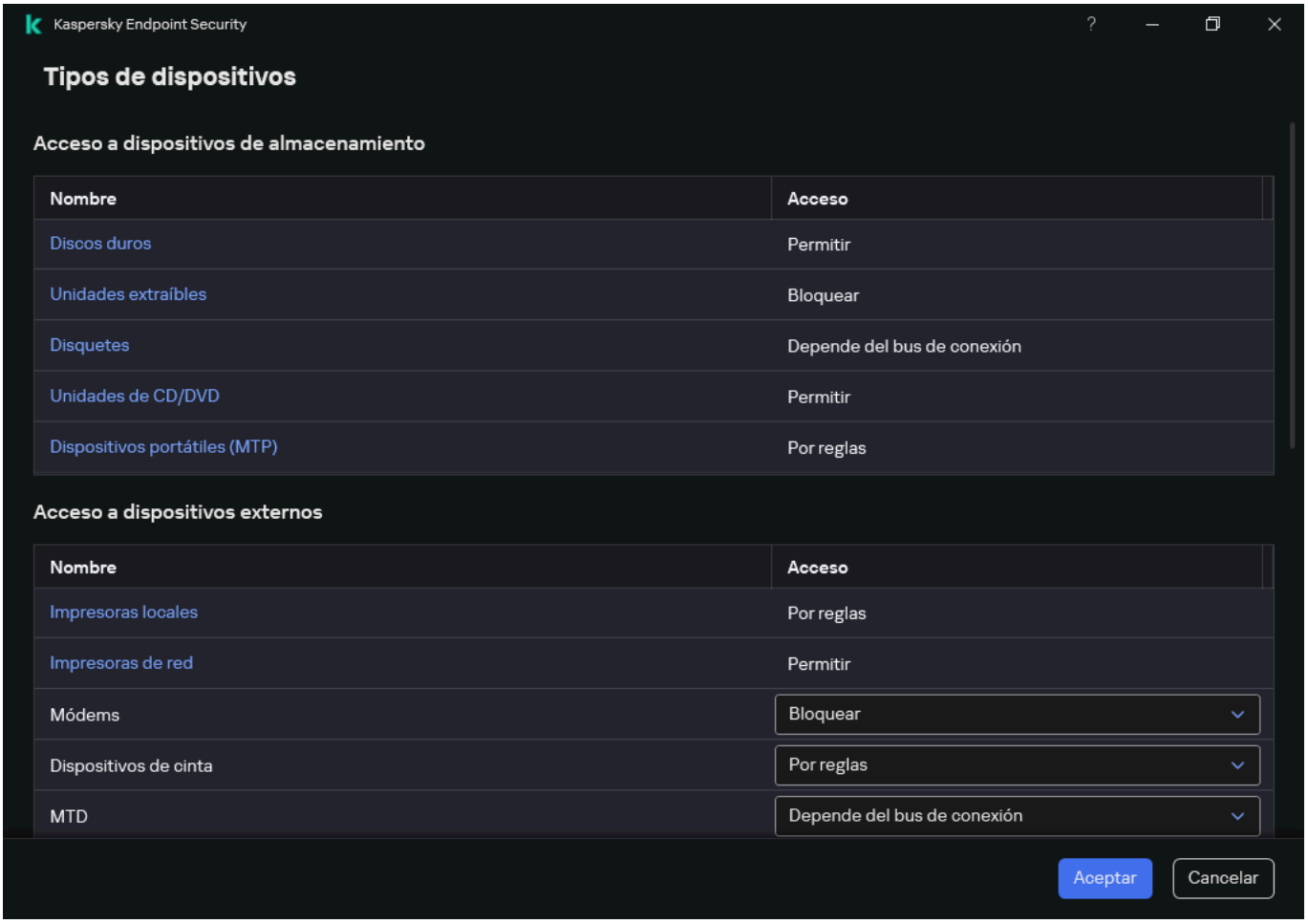
- Supervisión de operaciones en archivos en unidades extraíbles.
- Supervisión de la conexión y desconexión de unidades extraíbles de confianza.

  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 configuración de notificaciones para el componente Control de dispositivos. Los eventos tienen el nivel de gravedad *Mensaje informativo*.

Para habilitar la supervisión del uso de unidades extraíbles:

1. En la ventana principal de la aplicación 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 Wi-Fi**.

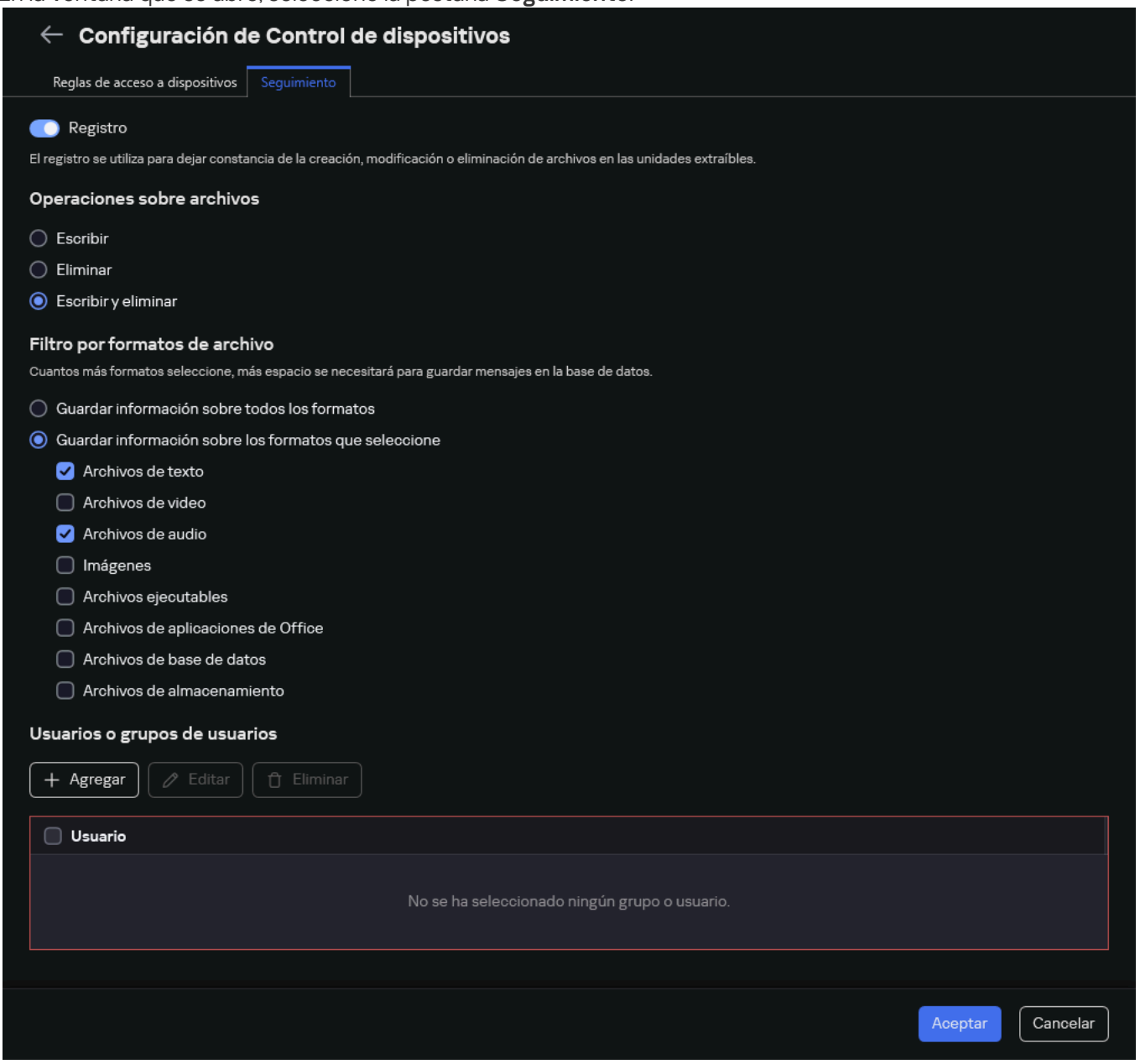
La ventana que se abre muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.



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 pestaña **Seguimiento**.



La configuración del monitoreo del uso de unidades extraíbles

6. Active el interruptor de **Registro**.

7. En el bloque **Operaciones sobre archivos**, seleccione las operaciones que desea supervisar: **Escribir**, **Eliminar**.

8. En el bloque **Filtro por formatos de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas debe seguir Control de dispositivos.

9. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.

10. Guarde los cambios.

De esta manera, cuando los usuarios escriban en archivos ubicados en unidades extraíbles o eliminen archivos de unidades extraíbles, Kaspersky Endpoint Security guardará la información sobre dichas operaciones en el registro de eventos y enviará un mensaje al Servidor de administración de 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 del **Servidor de administración** en la ficha **Eventos**. Para que se muestren los eventos en el registro de eventos local de Kaspersky Endpoint Security, debe seleccionar la casilla **Se realizó una operación en un archivo** en la notifications settings 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. A continuación, 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 de tiempo 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 todas las configuraciones de eventos siguientes coinciden con el registro en la caché:

- Id. de dispositivo
- SID de la cuenta de usuario que intenta acceder
- Categoría de dispositivo
- Acción realizada con el dispositivo
- Permiso de solicitud para esta acción: permitido o rechazado
- Ruta del proceso utilizado para realizar la acción
- Archivo al que se accede

Antes de cambiar el período de almacenamiento en caché, deshabilite la Autoprotección de Kaspersky Endpoint Security. Después de cambiar el período de almacenamiento en caché, habilite la 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\environment]`
   - Para sistemas operativos de 32 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. Abra `DeviceControlEventsCachePeriod` para editarlo.
4. Defina la cantidad de minutos durante los que Control de dispositivos debe guardar información sobre un evento antes de eliminarla.

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 completo en todo momento.

Puede conceder acceso a los dispositivos de confianza a un usuario específico, a un grupo de usuarios o a todos los usuarios de su organización.

Por ejemplo, si usar unidades extraíbles está prohibido en su organización, pero los administradores necesitan utilizarlas, puede permitir su uso solo para un grupo de administradores. Para ello, deberá agregar las unidades extraíbles a la lista de dispositivos de confianza y configurar los permisos de acceso de los usuarios.

No se recomienda agregar más de 5000 dispositivos de confianza, ya que pueden generar inestabilidad en el sistema.

Kaspersky Endpoint Security ofrece distintos métodos para agregar un dispositivo a la lista de dispositivos de confianza:

- Si no utiliza Kaspersky Security Center en su organización, puede conectar el dispositivo a un equipo y agregarlo a la lista de dispositivos de confianza a través de los ajustes de la aplicación. Para distribuir esta lista a todos los equipos de la organización, use el procedimiento de exportación e importación o permita que las listas de las directivas se combinen.

- Si utiliza Kaspersky Security Center en su organización, puede detectar todos los dispositivos conectados y crear una lista de dispositivos de confianza en la directiva. La lista de dispositivos de confianza estará disponible en todos los equipos que estén sujetos a la directiva.

Kaspersky Endpoint Security permite controlar el uso de dispositivos de confianza (conexión y desconexión). Puede activar el registro de eventos en configuración de notificaciones para el componente Control de dispositivos. Los eventos tienen el nivel de gravedad *Mensajes informativos*.

Agregar un dispositivo a la lista De confianza desde la interfaz de la aplicación

Por defecto, cuando se agrega un dispositivo a la lista de dispositivos de confianza, el acceso a ese dispositivo se otorga a todos los usuarios (el grupo de usuarios Todos).

Para agregar un dispositivo a la lista De confianza desde la interfaz de la aplicación:

1. En la ventana principal de la aplicación 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 selecciona en la lista desplegable **Mostrar dispositivos conectados**.

5. En la lista de dispositivos, seleccione el dispositivo que desea agregar a la lista de confianza.

   Kaspersky Endpoint Security no admite agregar dispositivos del tipo **Disquetes** a la lista de confianza.

6. En el campo **Comentario**, puede proporcionar toda la 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

8. Guarde los cambios.

Añadir un dispositivo a la lista De confianza desde Kaspersky Security Center

Cuando Kaspersky Endpoint Security está instalado en los equipos y el componente Control de dispositivos está habilitado, Kaspersky Security Center recibe información sobre los dispositivos. Para que un dispositivo pueda agregarse a la lista De confianza, Kaspersky Security Center debe tener información sobre el mismo.

Para agregar un dispositivo a la lista De confianza, pueden usarse los siguientes datos:

- **Dispositivos por Id**. Cada dispositivo tiene un identificador único (id. de hardware, también denominado HWID). Puede ver el Id. en las propiedades del dispositivo usando las herramientas del sistema operativo. Un Id. de dispositivo típico podría ser: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id.

- **Dispositivos por modelo**. Cada dispositivo tiene un id. de proveedor (VID) y un id. de producto (PID). Puede ver los ID. en las propiedades del dispositivo usando las herramientas del sistema operativo. Los valores VID y PID deben especificarse en este formato: `VID_1234&PID_5678`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.

- **Dispositivos por máscara de id**. Si está usando varios dispositivos con Id. similares, puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `WDC_C*`.

- **Dispositivos por máscara de modelo**. Si está usando varios dispositivos con VID o PID similares (por ejemplo, dispositivos del mismo fabricante), puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `VID_05AC&PID_*`.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de dispositivos de confianza. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Para agregar dispositivos a la lista de dispositivos de confianza:

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

2. Seleccione la directiva correspondiente 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 la parte derecha de la ventana, seleccione la ficha **Dispositivos de confianza**.

5. Active la casilla **Combinar valores al heredar** si desea crear una lista de dispositivos de confianza unificada para todos los equipos de la empresa.

   La lista de dispositivos de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Los dispositivos de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlos. No podrá modificarlos ni eliminarlos.

6. Haga clic en el botón **Agregar** y seleccione el método que desee usar para agregar los dispositivos a la lista.

7. Para filtrar los dispositivos, seleccione un tipo de dispositivo en la lista desplegable **Tipo de dispositivo** (por ejemplo, **Unidades extraíbles**).

   Kaspersky Endpoint Security no admite agregar dispositivos del tipo **Disquetes** a la lista de confianza.

8. En el campo **Nombre o modelo**, escriba un identificador, modelo (VID y PID) o máscara de dispositivo, según el método que haya elegido para agregar los dispositivos.

   La opción de agregar dispositivos por máscara de modelo (VID y PID) funciona del siguiente modo: cuando se introduce una máscara de modelo que no se corresponde con ningún modelo, Kaspersky Endpoint Security busca una correspondencia entre la máscara y el id. de dispositivo (HWID). Para ello, Kaspersky Endpoint Security verifica solo la parte del id. de dispositivo que determina cuál es el tipo de dispositivo y quién es su fabricante (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Si se encuentra una coincidencia entre la máscara de modelo y esta parte del id. de dispositivo, los dispositivos alcanzados por la máscara se agregarán a la lista de dispositivos de confianza del equipo. Paralelamente, la lista de dispositivos en Kaspersky Security Center se mantendrá vacía cuando haga clic en el botón **Actualizar**. Para que la lista de dispositivos se muestre correctamente, deberá agregar los dispositivos utilizando una máscara de id. de dispositivo.

9. Para filtrar los dispositivos, en el campo **Equipo** escriba el nombre del equipo (o la máscara del nombre del equipo) al que se encuentre conectado el dispositivo.

   El carácter `*` le permitirá representar cuantos caracteres sea necesario. El carácter `?` representa cualquier carácter individual.

10. Haga clic en el botón **Actualizar**.

    En la tabla, verá una lista con los dispositivos que cumplan con las condiciones de filtrado.

11. Active las casillas adyacentes a los dispositivos que desee agregar a la lista De confianza.

12. En el campo **Comentario**, indique por qué decidió agregar los dispositivos a la lista de dispositivos de confianza.

13. Haga clic en el botón **Seleccionar**, ubicado a la derecha del campo **Autorizar a los siguientes usuarios o grupos de usuarios**.

14. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

    De manera predeterminada, el grupo Everyone tiene acceso a los dispositivos de confianza.

15. Guarde los cambios.

Cuando se conecte un dispositivo, Kaspersky Endpoint Security revisará la lista de dispositivos de confianza en nombre del usuario autorizado. Si el dispositivo conectado es de confianza, Kaspersky Endpoint Security permitirá que se acceda al mismo sin restricciones de permisos, incluso si el acceso a ese tipo de dispositivo o a su bus de conexión se encuentra bloqueado. Si el dispositivo no es de confianza y no se permite acceder a él, existe un procedimiento para solicitar acceso a dispositivos bloqueados.

Exportar e importar la lista de dispositivos de confianza

Si desea distribuir la lista de dispositivos de confianza a todos los equipos de la organización, puede usar el procedimiento de exportación/importación.

Por ejemplo, si necesita distribuir una lista de unidades extraíbles de confianza, haga lo siguiente:

1. Conecte las unidades extraíbles a su propio equipo, una tras otra.
2. En la configuración de Kaspersky Endpoint Security, agregue las unidades extraíbles a la lista de dispositivos de confianza. Si lo considera necesario, configure los permisos de acceso para los usuarios. Por ejemplo, limite el uso de unidades extraíbles a los administradores.
3. Exporte la lista de dispositivos de confianza mediante la interfaz de Kaspersky Endpoint Security (consulte las instrucciones más abajo).
4. Distribuya el archivo con la lista de dispositivos de confianza a los demás equipos de la red. Para ello, copie el archivo a una carpeta compartida o utilice el método que considere conveniente.
5. Importe la lista de dispositivos de confianza en la configuración de Kaspersky Endpoint Security de los demás equipos de la organización (consulte las instrucciones más abajo).

Para importar o exportar la lista de dispositivos de confianza:

1. En la ventana principal de la aplicación 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 desea exportar.

   b. Haga clic en **Exportar**.

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

   Kaspersky Endpoint Security exportará la lista de dispositivos de confianza completa al archivo XML.

5. Para importar la lista de dispositivos de confianza:

   a. En la lista desplegable **Importar**, seleccione la acción correspondiente: **Importar y agregar a existente(s)** o **Importar y reemplazar existente(s)**.

   b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de dispositivos de confianza.

   c. Abra el archivo.

6. Guarde los cambios.

Cuando se conecte un dispositivo, Kaspersky Endpoint Security revisará la lista de dispositivos de confianza en nombre del usuario autorizado. Si el dispositivo conectado es de confianza, Kaspersky Endpoint Security permitirá que se acceda al mismo sin restricciones de permisos, incluso si el acceso a ese tipo de dispositivo o a su bus de conexión se encuentra bloqueado.

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 agregar el dispositivo a la lista de dispositivos de confianza o deshabilitar 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.

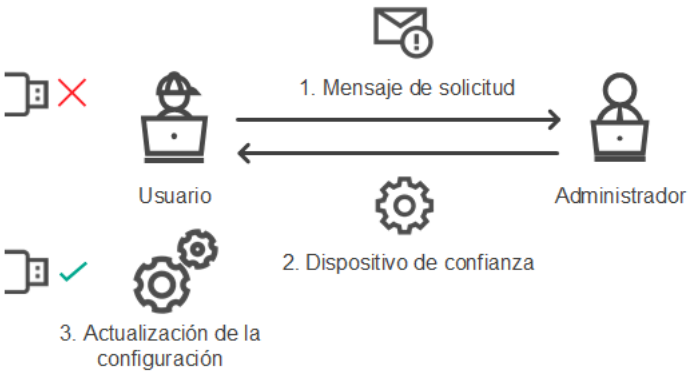
2. El administrador recibe un mensaje con la solicitud en la consola de Kaspersky Security Center.

   La consola de Kaspersky Security Center tiene la selección de eventos preestablecida *Solicitudes de usuario* para facilitar el seguimiento de los mensajes de los usuarios.

3. El administrador agrega el dispositivo a la lista de dispositivos de confianza.

   Para agregar 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.

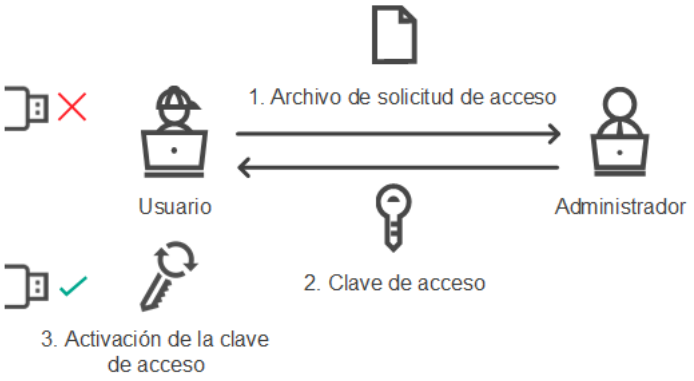
Si necesita otorgar acceso temporal a un dispositivo, pero no puede agregarlo a la lista de dispositivos de confianza, puede utilizar el modo sin conexión. Este modo permite otorgar acceso a un dispositivo bloqueado aun cuando un equipo no tiene conexión a la red o se encuentra fuera de la red corporativa.

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:

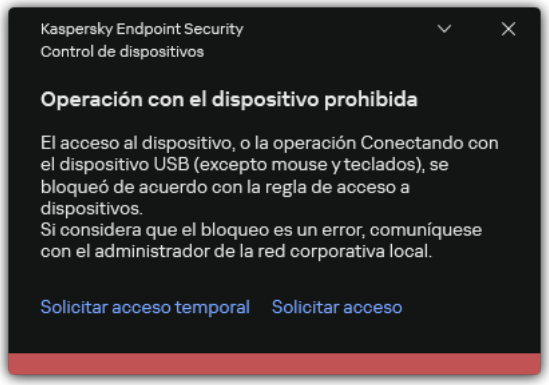
1. Conecte el dispositivo al equipo.

   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 vínculo **Solicitar acceso**.

   Esto abre una ventana que tiene un mensaje para el administrador. El mensaje contendrá información sobre el dispositivo bloqueado.

3. Haga clic en **Enviar**.



Notificación del Control de dispositivos

A continuación, el administrador de la consola de Kaspersky Security Center recibe el evento *Mensaje de bloqueo del acceso a un dispositivo para el administrador*. El evento incluye el nombre de usuario, el nombre del equipo, los detalles del dispositivo al que el usuario intenta obtener acceso y otra información. Puede configurar cómo se notifica al administrador acerca de estos eventos y, por ejemplo, seleccionar notificaciones por correo electrónico. La consola de Kaspersky Security Center tiene la selección de eventos preestablecida *Solicitudes de usuario* para facilitar el seguimiento de los mensajes de los usuarios.

Para permitir el acceso, debe agregar el dispositivo a la lista de dispositivos 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 vínculo **Solicitar acceso temporal**.

   Esto abre una ventana que contiene una lista de dispositivos conectados.

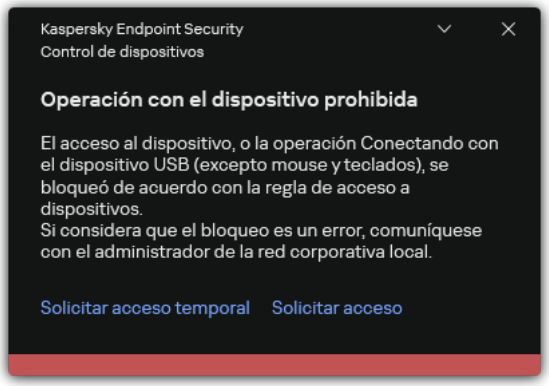
3. En la lista de dispositivos conectados, seleccione el dispositivo al que desee obtener acceso.

4. Haga clic en **Generar archivo de solicitud de acceso**.

5. En el campo **Duración del acceso**, especifique el período durante el cual quiera tener 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 del Control de dispositivos

Cómo el administrador puede 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 con el nombre del grupo de administración al cual pertenece el equipo cliente en cuestión.

3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.

4. En la lista de equipos cliente, seleccione el equipo a cuyo usuario se le debe otorgar acceso temporal al dispositivo bloqueado.

5. En el menú contextual del equipo, seleccione el elemento **Otorgar acceso en el modo sin conexión**.

6. En la ventana que se abre, 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 permiso de acceso**.

   De manera predeterminada, el valor de **Duración del permiso de acceso** es el mismo que indicó el usuario al crear el archivo de solicitud de acceso.

9. Especifique el valor de **Activar a partir de**.

   Esta configuración define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado con la clave de acceso provista.

10. Guarde el archivo de clave de acceso en el equipo.

Cómo el administrador puede 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 a cuyo usuario se le debe otorgar acceso temporal al dispositivo bloqueado.

3. Haga clic en el botón de puntos suspensivos (...) encima de la lista de equipos y luego haga clic en el botón **Otorgar acceso al dispositivo en modo sin conexión**.

4. En la ventana que se abre, seleccione la sección **Control de dispositivos**.

5. 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.

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 durante el cual se puede activar la clave de acceso en el dispositivo.

   Esta configuración define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado con la clave de acceso provista.

8. Guarde el archivo de clave de acceso en el equipo.

Como resultado, se descargará al equipo una clave de acceso para el dispositivo bloqueado. Los archivos de clave de acceso tienen la extensión *.acode. Envíe el archivo de clave de acceso al usuario utilizando cualquier método a su disposición.

Para activar una clave de acceso como usuario:

1. En la ventana principal de la aplicación 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.

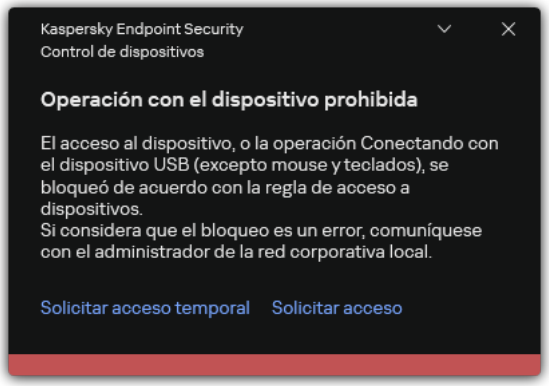
6. Haga clic en **Aceptar**.

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, agregue el dispositivo a la lista de dispositivos de confianza.

Edición de plantillas de mensajes del Control de dispositivos

Cuando el usuario intenta acceder a un dispositivo bloqueado, Kaspersky Endpoint Security muestra un mensaje en el que se indica que el acceso al dispositivo está bloqueado o que la operación con el contenido del dispositivo está prohibida. Los expertos de Kaspersky proporcionan una plantilla de mensaje al usuario en la que se describen las razones por las que se bloqueó el acceso al dispositivo (consulte la figura a continuación).

Se proporcionan variables especiales para administrar las plantillas de mensajes (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensajes para diferentes equipos. 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 que coincide con el equipo, el usuario y el evento específicos.



Notificación del Control de dispositivos

Si el usuario cree que el acceso al dispositivo se bloqueó por error o que una operación con contenido del dispositivo se prohibió por equivocación, puede enviar un mensaje al administrador de la red corporativa local haciendo clic en el vínculo presente en el mensaje en pantalla sobre la acción bloqueada. Para hacerlo, el usuario debe hacer clic en **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 y agregarle datos que pueden informar su decisión de permitir o bloquear el acceso al dispositivo. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del acceso a un dispositivo para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 las plantillas de mensajes 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 correspondiente 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, donde debe configurar las plantillas de Control de aplicaciones:

   - **Mensaje para bloqueos**. 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**. Plantilla del mensaje que se envía al administrador de la red de área local cuando el usuario considera que el acceso a un dispositivo se ha bloqueado por error o, de manera similar, que la posibilidad de realizar una operación con el contenido de un dispositivo se ha bloqueado por error.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada.

6. Guarde los cambios.

Cómo cambiar las plantillas de mensajes de Control de dispositivos 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de dispositivos**.

5. En el bloque **Plantillas de mensajes**, configure plantillas para los mensajes de Control de aplicaciones:

   - **Mensaje para el 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 para el administrador**. Plantilla del mensaje que se envía al administrador de la red de área local cuando el usuario considera que el acceso a un dispositivo se ha bloqueado por error o, de manera similar, que la posibilidad de realizar una operación con el contenido de un dispositivo se ha bloqueado por error.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada.

6. Guarde los cambios.

Cómo cambiar las plantillas de mensajes de Control de dispositivos en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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**, configure plantillas para los mensajes de Control de aplicaciones:

   - **Mensaje para bloqueos**. 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**. Plantilla del mensaje que se envía al administrador de la red de área local cuando el usuario considera que el acceso a un dispositivo se ha bloqueado por error o, de manera similar, que la posibilidad de realizar una operación con el contenido de un dispositivo se ha bloqueado por error.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada.

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 los siguientes tipos predeterminados de dispositivos:

- Adaptadores de red
- Adaptadores Wi-Fi
- Módems

Si se habilita una regla de conexión, 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 establecidas mediante la utilización de los tipos de dispositivo para los cuales se utilizan las reglas de menor prioridad.

Habilitar Anti-Bridging

Por defecto, el componente Anti-Bridging está deshabilitado.

Para habilitar Anti-Bridging:

1. En la ventana principal de la aplicación 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 **Habilitar Anti-Bridging** para habilitar o deshabilitar esta característica.

5. Guarde los cambios.

   Una vez habilitada la protección Anti-Bridging, Kaspersky Endpoint Security bloquea las conexiones ya establecidas de conformidad con las reglas de conexión.

Edición del estado de una regla de conexiones

Para cambiar el estado de una regla de conexión:

1. En la ventana principal de la aplicación 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 los dispositivos**, seleccione la regla cuyo estado desea cambiar.

5. Utilice los interruptores de la columna **Control** para habilitar o deshabilitar la regla.

6. Guarde los cambios.

Cambio de prioridad de una regla de conexión

Para cambiar la prioridad de una regla de conexión:

1. En la ventana principal de la aplicación 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 los dispositivos**, seleccione la regla cuya prioridad desea cambiar.

5. Utilice los botones **Subir**/**Abajo** para configurar la prioridad de la regla de conexión.

   Cuanto más arriba está una regla en la tabla, mayor es su prioridad. El componente Anti-Bridging bloquea todas las conexiones excepto una conexión establecida usando el tipo de dispositivo para el cual se utiliza la regla de la prioridad más alta.

6. Guarde los cambios.

Control de anomalías adaptativo

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha 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 conectados a una red corporativa. Para ello utiliza una serie de reglas, diseñadas para buscar comportamientos que no se consideran típicos (por ejemplo, la regla *Inicio de Microsoft PowerShell desde una aplicación de ofimática*). Los especialistas de Kaspersky crean estas reglas basándose en casos característicos de actividad maliciosa. La manera en que el Control de anomalías adaptativo responde ante cada regla es configurable; esto significa que, por ejemplo, es posible permitir la ejecución de scripts de PowerShell que se hayan creado para automatizar ciertos aspectos de un flujo de trabajo. Las reglas se actualizan junto con las bases de datos de Kaspersky Endpoint Security. No obstante, las actualizaciones para las reglas deben confirmarse manualmente.

Configuración del Control de anomalías adaptativo

Los pasos para configurar el Control de anomalías adaptativo son los siguientes:

1. Usar el modo de aprendizaje del Control de anomalías adaptativo.

   Una vez que el Control de anomalías adaptativo se habilita, sus reglas entran en un *modo de aprendizaje*. Mientras dicho modo está activo, el Control de anomalías adaptativo monitorea la activación de las reglas y envía los eventos de activación a Kaspersky Security Center. El tiempo de aprendizaje varía según la regla. Quienes definen la duración son los expertos de Kaspersky. Lo normal es que el modo de aprendizaje esté activo por dos semanas.

   Si una regla no se activa en lo absoluto durante el período de aprendizaje, el componente considerará que las acciones asociadas con la regla son atípicas. En consecuencia, Kaspersky Endpoint Security bloqueará cualquier acción vinculada con esa regla.

   Si una regla se activa durante el período de aprendizaje, Kaspersky Endpoint Security dejará constancia de los eventos en el informe de activación de las reglas y en el repositorio **Activación de reglas en el estado Aprendizaje inteligente**.

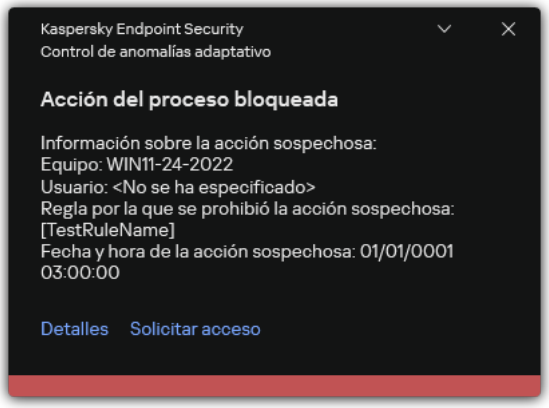
2. Analizar el informe de activación de las reglas.

   El administrador analiza el informe de activación de reglas o el contenido del repositorio **Activación de reglas en el estado Aprendizaje inteligente**. A continuación, selecciona cómo reaccionará el Control de anomalías adaptativo cuando se active una regla; las opciones posibles son permitir y bloquear. El administrador también puede optar por seguir controlando el funcionamiento de la regla y extender la duración del modo de aprendizaje. Si el administrador no realiza ninguna acción, la aplicación seguirá operando en modo de aprendizaje. El plazo de aprendizaje se reiniciará.

Control de anomalías adaptativo se configura en tiempo real mediante los siguientes canales:

- El Control de anomalías adaptativo comienza a bloquear automáticamente las acciones asociadas con las reglas que nunca se activaron en el modo de aprendizaje.
- Kaspersky Endpoint Security agrega reglas nuevas o elimina las que han quedado obsoletas.
- El administrador configura el funcionamiento de Control de anomalías adaptativo tras revisar el informe de activación de reglas y el contenido del repositorio **Activación de reglas en el estado Aprendizaje inteligente**. Recomendamos consultar el informe sobre la activación de reglas y el contenido del almacenamiento **Activación de reglas en el estado Aprendizaje inteligente**.

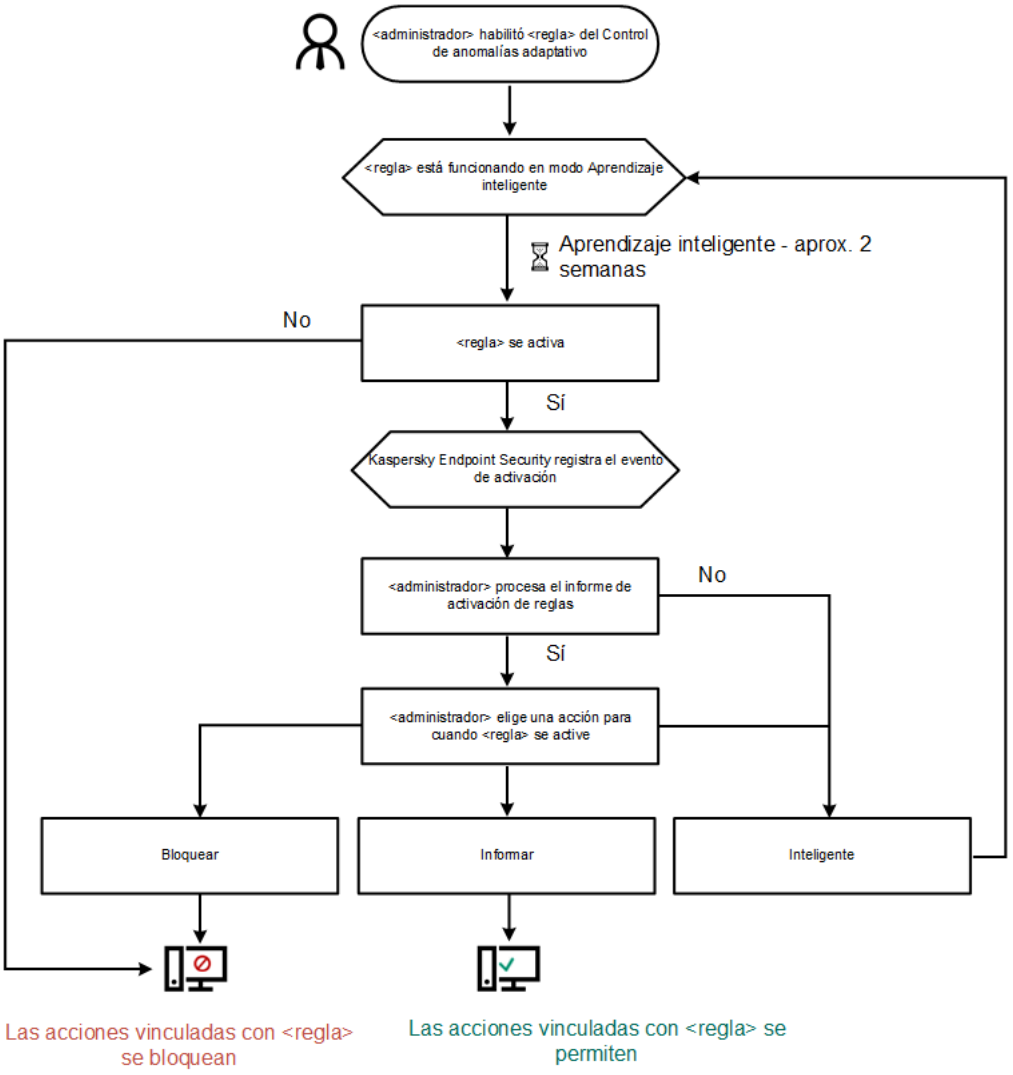
Cuando una aplicación maliciosa intente realizar una acción, Kaspersky Endpoint Security bloqueará el intento y mostrará una notificación (consulte la siguiente imagen).



Notificación del Control de anomalías adaptativo

Algoritmo de funcionamiento del Control de anomalías adaptativo

Para determinar si una acción asociada a una regla debe permitirse o bloquearse, Kaspersky Endpoint Security usa el algoritmo de la siguiente imagen.



Algoritmo de funcionamiento del Control de anomalías adaptativo

Aprendizaje del Control de anomalías adaptativo

El Control de anomalías adaptativo incluye un conjunto de reglas (patrones de comportamiento). Una vez que el Control de anomalías adaptativo se habilita, sus reglas entran en un *modo de aprendizaje*. Mientras dicho modo está activo, el Control de anomalías adaptativo monitorea la activación de las reglas y envía los eventos de activación a Kaspersky Security Center. El Control de anomalías adaptativo no bloquea la actividad de las aplicaciones en el equipo, solo informa al administrador. También puede seleccionar manualmente la acción que se realiza cuando se activa una regla de Control de anomalías adaptativo.

Cómo ver la lista de reglas del 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 correspondiente 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 de verificación **Control de anomalías adaptativo**.

6. En **Configuración de las reglas del Control de anomalías adaptativo**, consulte la lista de reglas.

   De manera predeterminada, todas las reglas funcionan en el modo **Inteligente**.

7. Si es necesario, confirme la actualización de la regla del Control de anomalías adaptativo.

8. Si es necesario, seleccione una acción cuando se active una regla del Control de anomalías adaptativo:

   - **Bloquear**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y deja registro de la actividad.

   - **Informar**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y deja registro de la actividad.

9. Si es necesario, deshabilite las reglas que no desee utilizar.

10. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo ver los informes de las reglas del 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de anomalías adaptativo**.

5. Active el interruptor de **Control de anomalías adaptativo HABILITADO**.

6. En **Reglas**, consulte la lista de reglas.

   De manera predeterminada, todas las reglas funcionan en el modo **Inteligente**.

7. Si es necesario, confirme la actualización de la regla del Control de anomalías adaptativo.

8. Si es necesario, seleccione una acción cuando se active una regla del Control de anomalías adaptativo:

   - **Bloquear**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y deja registro de la actividad.

   - **Informar**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y deja registro de la actividad.

9. Si es necesario, deshabilite las reglas que no desee utilizar.

10. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo ver la lista de reglas del Control de anomalías adaptativo en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.

3. Active el interruptor de **Control de anomalías adaptativo**.

4. En el bloque **Reglas**, haga clic en el vínculo **Modificar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo. De manera predeterminada, todas las reglas funcionan en el modo **Inteligente**.

5. Si es necesario, confirme la actualización de la regla del Control de anomalías adaptativo.

6. Si es necesario, seleccione una acción cuando se active una regla del Control de anomalías adaptativo:

   - **Bloquear**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y deja registro de la actividad.

   - **Informar**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y deja registro de la actividad.

7. Si es necesario, deshabilite las reglas que no desee utilizar.

8. Guarde los cambios.

El tiempo de aprendizaje varía según la regla. Quienes definen la duración son los expertos de Kaspersky. Lo normal es que el modo de aprendizaje esté activo por 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**. Luego, la aplicación bloquea cualquier actividad que coincida con esta regla.

Si una regla se activa durante el entrenamiento, debe configurar manualmente la acción que la aplicación aplicará a la actividad detectada que coincida con esta regla. Si no selecciona la acción cuando se activa la regla, el Control de anomalías adaptativo continúa en modo de entrenamiento.

Habilitación y deshabilitación de una regla del Control de anomalías adaptativo

Para habilitar o deshabilitar una regla del Control de anomalías adaptativo:

1. En la ventana principal de la aplicación 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 **Modificar 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 aplicaciones de ofimática*) y amplíe el conjunto.

5. Seleccione una regla (por ejemplo, *Inicio de Microsoft PowerShell desde una aplicación de ofimática*).

6. Use el conmutador del interruptor en la columna **Condición** para habilitar o deshabilitar 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 principal de la aplicación 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 **Modificar 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 del Control de anomalías adaptativo.

6. En el bloque **Acción**, seleccione una de las siguientes opciones:

   - **Inteligente**. Si esta opción está seleccionada, la regla del Control de anomalías adaptativo funcionará en el estado de aprendizaje inteligente durante un plazo definido por el grupo de especialistas de Kaspersky. En este modo, cuando una regla del Control de anomalías adaptativo se activa, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y agrega 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 estado de aprendizaje inteligente, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y agrega una entrada de registro con información sobre la actividad.

   - **Bloquear**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y deja registro de la actividad.

   - **Informar**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y deja registro de la actividad.

7. Guarde los cambios.

Crear una exclusión para 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 adaptativo 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. Por ejemplo, abre un archivo de nombre `file.xlsx`. Por lo tanto, se carga un archivo de la biblioteca con la extensión DLL en la memoria del equipo. Un navegador utiliza esta biblioteca (cuyo archivo ejecutable es `browser.exe`). En 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.

Si desea crear una exclusión para una regla del Control de anomalías adaptativo:

1. En la ventana principal de la aplicación 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 **Modificar 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 del Control de anomalías adaptativo.
6. En el bloque **Exclusiones**, haga clic en el botón **Agregar**.

   Se abre la ventana de propiedades de la exclusión.
7. Seleccione el usuario en el cual desea configurar una exclusión.

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar 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 aplica la exclusión.
8. En el campo **Descripción**, describa la exclusión.
9. Defina los parámetros del objeto de origen o del proceso de origen iniciado 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 del 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>`, reemplazando `<object>` con 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 del objeto de origen**. Hash SHA256 del archivo.

La regla del Control de anomalías adaptativo 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 del 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 del objeto de destino**. Hash SHA256 del archivo.

    La regla del Control de anomalías adaptativo 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.

Exportar e importar exclusiones para reglas del Control de anomalías adaptativo

Si desea exportar o importar la lista de exclusiones para las reglas seleccionadas:

1. En la ventana principal de la aplicación 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 **Modificar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.

4. Para exportar la lista de reglas:

   a. Seleccione la regla cuyas excepciones desea exportar.

   b. Haga clic en **Exportar**.

c. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

d. Confirme que desea exportar solo las exclusiones seleccionadas, o bien exporte 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 que se usará para importar la lista de exclusiones.

c. Abra el archivo.

Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 agregarse o eliminarse.

Hasta que se aplica una actualización, las reglas pendientes de eliminarse se siguen mostrando en la tabla de reglas, pero Kaspersky Endpoint Security les asigna el estado *Deshabilitado*. No es posible cambiar la configuración de estas reglas.

Para actualizar las reglas del Control de anomalías adaptativo:

1. En la ventana principal de la aplicación 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 **Modificar 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 del Control de anomalías adaptativo, Kaspersky Endpoint Security muestra un mensaje que indica que las acciones potencialmente dañinas están bloqueadas. Si el usuario cree que la acción está bloqueada por error, puede usar el vínculo 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 las plantillas de mensajes (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensajes para diferentes equipos. 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 que coincide con el equipo, el usuario y el evento específicos.

Para modificar una plantilla de mensaje:

1. En la ventana principal de la aplicación 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 para bloqueos**. Plantilla del mensaje que se le mostrará al usuario cuando se active una regla del Control de anomalías adaptativo para bloquear una acción atípica.

   - **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la red local corporativa si considera que una acción se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo de actividad de aplicación enviado al administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada utilizando el botón **Restablecer**.

4. Guarde los cambios.

Supervisión de las operaciones de Control de anomalías adaptativo

Control de anomalías adaptativo incluye varias herramientas de supervisión. Se supervisa el componente Control de anomalías adaptativo para configurarlo durante el aprendizaje.

Informes de Control de anomalías adaptativo

Control de anomalías adaptativo utiliza los siguientes informes:

- **Informe sobre el estado de las reglas del Control de anomalías adaptativo**. El informe contiene información sobre el estado de las reglas del Control de anomalías adaptativo (*Apagado*, *Aprendizaje inteligente*, *Bloqueo inteligente*, *Notificar*, *Bloquear*). Este informe permite analizar el nivel de aprendizaje de Control de anomalías adaptativo y evaluar la cantidad de reglas que cambiaron del modo *Aprendizaje inteligente* al modo de funcionamiento normal (por ejemplo, *Bloqueo inteligente*).

- **Informe sobre las reglas activadas del Control de anomalías adaptativo**. El informe contiene información sobre los activadores de reglas. El informe también muestra el modo de activación de reglas: *Bloquear* (incluido *Bloqueo inteligente*) o *Notificar*. Este informe permite evaluar la actividad del componente 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 correspondiente 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 el vínculo **Informe sobre el estado de las reglas del Control de anomalías adaptativo**.

   - Si desea ver el informe sobre las reglas activadas del Control de anomalías adaptativo, haga clic en el vínculo **Informe sobre las reglas activadas del Control de anomalías adaptativo**.

5. Se inicia el proceso de generación del informe.

   El informe se muestra en una ventana nueva.

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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de anomalías adaptativo**.

5. En el bloque **Reglas**, realice una de las siguientes acciones:

   - Si desea ver el informe sobre el estado de las reglas del Control de anomalías adaptativo, seleccione **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 del informe.

   El informe se muestra en una ventana nueva.

Para generar informes en la consola de Kaspersky Security Center, debe habilitar la transferencia de datos al Servidor de administración. Esta transferencia de datos está habilitada de forma predeterminada.

Cómo habilitar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y repositorios**.

4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.

5. Seleccione las siguientes casillas:

   - **Informe sobre el estado de las reglas del Control de anomalías adaptativo**.

   - **Informe sobre las reglas activadas del Control de anomalías adaptativo**.

6. Guarde los cambios.

Cómo habilitar 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 ficha **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 sobre el estado de las reglas del Control de anomalías adaptativo**.

   - **Informe sobre las reglas activadas del Control de anomalías adaptativo**.

6. Guarde los cambios.

Almacenamiento de Activación de reglas en el estado Aprendizaje inteligente

En el modo de aprendizaje, 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 aparece en el almacenamiento en formato de lista de eventos. Para configurar Control de anomalías adaptativo, puede confirmar el comportamiento atípico en el equipo o agregar una exclusión de la regla.

Eventos de Control de anomalías adaptativo

Control de anomalías adaptativo registra los eventos de activación de reglas en los modos *Bloquear* (incluido *Bloqueo inteligente*) y *Notificar*. Para esto, se proporcionan los siguientes eventos:

Acción del proceso bloqueada

Acción del proceso omitida

Los eventos contienen información sobre actividades sospechosas, 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 considera que la actividad es legítima.

Control de aplicaciones

El componente Control de aplicaciones se utiliza para gestionar la ejecución de aplicaciones en los equipos de los usuarios. Permite, con ello, implementar una directiva de seguridad corporativa que regule el uso de aplicaciones. Gracias a las restricciones de acceso, el componente también ayuda a reducir el riesgo de que los equipos se infecten.

Los pasos para configurar Control de aplicaciones son los siguientes:

1. Creación de categorías de aplicaciones.

   El administrador crea categorías con las aplicaciones que desea controlar. Las categorías de aplicaciones impactan en todos los equipos de una red corporativa, independientemente del grupo de administración al que pertenecen. Las categorías se crean sobre la base de distintos criterios: categoría KL (por ejemplo, *Navegadores* u otra categoría), hash del archivo, proveedor de la aplicación y otros.

2. Creación de reglas de Control de aplicaciones.

   El administrador crea reglas de Control de aplicaciones dentro de la directiva asignada a un grupo de administración. Las reglas contienen las distintas categorías de aplicaciones y el estado de ejecución (inicio permitido o bloqueado) asignado a las aplicaciones de esas categorías. El administrador puede crear la cantidad de reglas que desee. Una aplicación puede coincidir con los criterios de varias reglas. La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. Kaspersky Endpoint Security comprueba si una aplicación coincide con una regla cada vez que se inicia. Kaspersky Endpoint Security compara de forma secuencial la aplicación con todas las reglas de Control de aplicaciones.

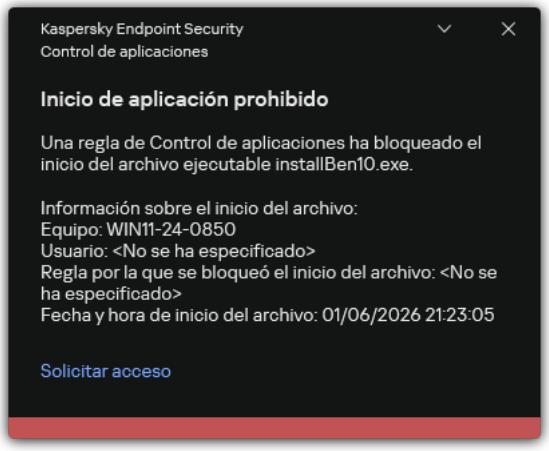
3. Selección del modo de Control de aplicaciones.

   El administrador decide el modo para trabajar con aplicaciones que no están contempladas en ninguna de las reglas (lista de autorización y de bloqueo).

Cuando un usuario intenta ejecutar una aplicación prohibida, Kaspersky Endpoint Security se lo impide y le muestra una notificación (vea la imagen de más abajo).

Existe un *modo de prueba*, diseñado para verificar la configuración de Control de aplicaciones. Cuando se utiliza este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite que se ejecute cualquier aplicación, esté o no prohibida.
- Muestra una notificación cuando se inicia una aplicación prohibida y agrega el evento al informe almacenado en el equipo del usuario.
- Transfiere información sobre la ejecución 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 permite que los usuarios inicien cualquier aplicación, excepto por las que se hayan prohibido a través de las reglas de Control de aplicaciones.

  Este modo de Control de aplicaciones está habilitado por defecto.

- **Lista de admitidos**. En este modo, Control de aplicaciones no permite que ningún usuario inicie ninguna aplicación, excepto por las que se hayan permitido (y no prohibido) a través de las reglas de Control de aplicaciones.

  Si se configuran completamente las reglas de autorización del Control de aplicaciones, el componente bloquea el inicio de todas las aplicaciones nuevas que no han sido verificadas por el administrador de la red LAN, mientras que permite el funcionamiento del sistema operativo y de las aplicaciones de confianza de las que dependen los usuarios para hacer su trabajo.

  Puede leer las recomendaciones sobre cómo configurar las reglas de control de aplicaciones en el modo de lista de autorización.

El Control de aplicaciones se puede configurar para funcionar en estos modos, tanto a través de la interfaz local de Kaspersky Endpoint Security como por medio de 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 necesarias para las siguientes tareas:

- Creación de categorías de aplicaciones.

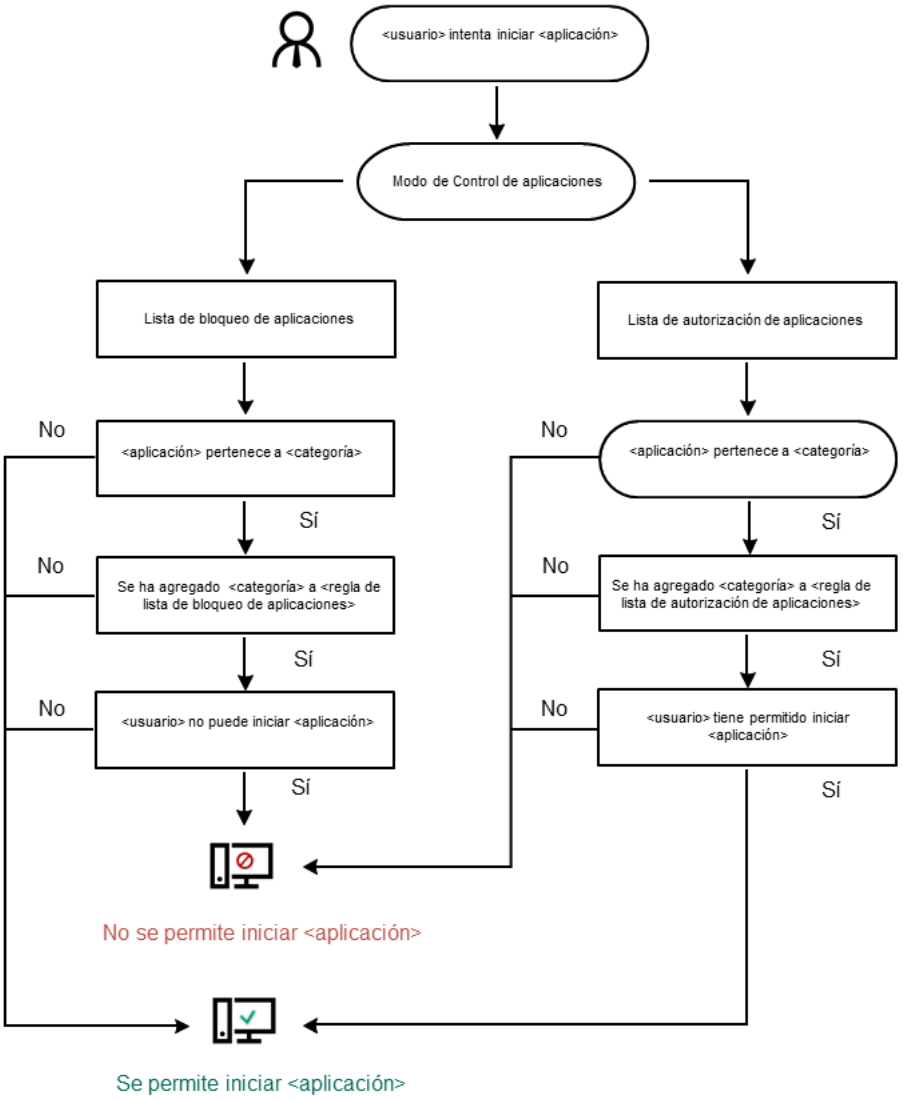
  Las reglas de Control de aplicaciones creadas en la Consola de administración de Kaspersky Security Center se basan en sus categorías de aplicaciones personalizadas, y no en condiciones de inclusión y exclusión como es el caso de la interfaz local de Kaspersky Endpoint Security.

- Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN.

Por este motivo se recomienda utilizar 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 decidir si una aplicación podrá iniciarse (vea la siguiente imagen).



Algoritmo de funcionamiento de Control de aplicaciones

Limitaciones de la funcionalidad del Control de aplicaciones

El funcionamiento del componente Control de aplicaciones está limitado en los casos siguientes:

- Cuando se actualiza la versión de la aplicación, no se admite la importación de los parámetros del componente Control de aplicaciones.

- Si no hay ninguna conexión con servidores de KSN, Kaspersky Endpoint Security recibe información sobre la reputación de las aplicaciones y sus módulos solo desde bases de datos locales.

  La lista de aplicaciones que Kaspersky Endpoint Security designa como categoría KL **Otro software\Aplicaciones, de confianza según su 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, se puede guardar información sobre 150 000 archivos procesados. Una vez que se alcance este número de registros, no se procesarán los archivos nuevos. Para reanudar operaciones del inventario, debe eliminar los archivos que se inventariaron anteriormente en la base de datos de Kaspersky Security Center desde el equipo en el cual está instalado 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 las reglas de Control de aplicaciones permiten el inicio de un intérprete, el componente no bloqueará un script iniciado desde este intérprete.

  Si al menos uno de los scripts especificados en la línea de comandos del intérprete está bloqueado desde el inicio por las reglas de control de la aplicación, el componente bloquea todos los scripts, especificados en la línea de comandos del intérprete.

- El componente no controla el inicio de scripts desde intérpretes que no son 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

Recepción de información sobre las aplicaciones que se instalan en equipos de usuarios

Para crear reglas de Control de aplicaciones óptimas, se recomienda obtener primero un panorama general de las aplicaciones que se utilizan en los equipos de la red LAN corporativa. Para hacerlo, puede obtener la siguiente información:

- Proveedores, versiones y localizaciones de aplicaciones utilizadas en la red LAN.
- Frecuencia de actualización de las aplicaciones.
- Directivas de uso de las aplicaciones adoptadas en la empresa (pueden ser directivas de seguridad o directivas administrativas).
- Ubicación de almacenamiento de los paquetes de distribución de las aplicaciones.

Visualizar información de la aplicación

El Agente de red de Kaspersky Security Center proporciona la información sobre las aplicaciones instaladas. 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 que envía el Agente de red, consulte la Ayuda de Kaspersky Security Center.

Para abrir la ventana de propiedades de una aplicación desde la carpeta Registro de aplicaciones, haga lo siguiente:

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**.

Visualización de información sobre archivos ejecutables

Puede reducir la carga en la base de datos al reunir información sobre archivos ejecutables. Para lograr esto, recomendamos ejecutar la tarea *Inventario* en varios equipos de referencia que tienen instalado su conjunto de software estándar.

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 las bases 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Inventario**.

Paso 2. Alcance del inventario

Cree una lista de carpetas en las que desea que Kaspersky Endpoint Security busque archivos ejecutables. Configure los ajustes de inventario (vea la siguiente tabla).

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Selección de la cuenta con la que se ejecutará la tarea

Seleccione la cuenta con la que se ejecutará la tarea *Inventario*. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local. Si incluyó unidades de red u objetos de acceso restringido en el alcance del inventario, asegúrese de elegir una cuenta de usuario que tenga los derechos de acceso necesarios.

Paso 5. Programación de la tarea

Configure la programación de la tarea, por ejemplo, manualmente.

Paso 6. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Inventario de referencia*.

Paso 7. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. Como resultado, se realiza una búsqueda de archivos ejecutables en los equipos de los usuarios de acuerdo con la programación configurada.

Cómo ejecutar una tarea de Inventario con 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   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 referencia*).

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del Asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Para configurar la tarea, vaya a las propiedades de la tarea (consulte la siguiente tabla).

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 buscarán archivos ejecutables en los equipos de los usuarios de acuerdo con la programación especificada.

Configuración de inventario

Parámetro	Descripción
Alcances del inventario	Lista de objetos que formarán el alcance del inventario.
Inventario de módulos DLL	Kaspersky Endpoint Security busca módulos DLL en el alcance del inventario y envía información a Kaspersky Security Center. Si habilita el inventario de módulos DLL, se aumenta significativamente el tiempo que lleva completar la tarea Inventario y el tamaño de la base de datos.
Inventario de archivos de script	Kaspersky Endpoint Security busca scripts en el alcance del inventario y envía la información a Kaspersky Security Center. Si habilita el inventario de archivos de script, se aumenta significativamente el tiempo que lleva completar la tarea Inventario y el tamaño de la base de datos.

Parámetro	Descripción
Ejecutar solo cuando el equipo esté inactivo	Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando el equipo está en uso.
Analizar solo 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 compuestos.
Omitir archivo que se analice durante más de (s) N s	Limitar el tiempo de ejecución de la tarea. Luego de un período 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 comienzo y según lo programado.
Analizar archivos de almacenamiento	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
No desempaquetar archivos compuestos grandes	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada o no.

Para abrir la ventana de propiedades de un archivo ejecutable en la carpeta Archivos ejecutables, haga lo siguiente:

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 los archivos ejecutables, y una lista de equipos donde se instaló la aplicación, abra la ventana de propiedades de una aplicación que esté seleccionada en la carpeta **Registro de aplicaciones** o en la carpeta **Archivos ejecutables**.

Actualizar la información acerca de las aplicaciones instaladas y los archivos ejecutables

A partir de Kaspersky Endpoint Security 12.3 para Windows, se optimiza el funcionamiento del componente Control de aplicaciones con la base de datos de archivos ejecutables. Kaspersky Endpoint Security 12.3 para Windows actualiza automáticamente la base de datos después de que se elimina 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 las aplicaciones instaladas actualizada, se debe habilitar el envío de información de la aplicación al Servidor de administración (está habilitado de manera predeterminada).

Cómo habilitar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y repositorios**.

4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.

5. Seleccione la casilla de verificación **Aplicaciones iniciadas**.

6. Guarde los cambios.

Cómo habilitar el envío de información 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 ficha **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, seleccione la casilla **Acerca de las aplicaciones iniciadas**.

7. Guarde los cambios.

Cómo habilitar el modo de aplicaciones bloqueadas

El modo *Aplicaciones bloqueadas* permite que los usuarios inicien cualquier aplicación, excepto por las que se hayan prohibido a través de 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 habilitado por defecto.

> Antes de habilitar el modo *Aplicaciones bloqueadas*, recomendamos probar las reglas de Control de aplicaciones. Para ello, puede habilitar el modo de prueba.

Cómo habilitar el modo 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 correspondiente 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 de verificación **Control de aplicaciones**.

6. En el bloque **Configuración de Control de aplicaciones**, utilice la lista desplegable **Modo de control** para seleccionar **Lista de rechazados**.

7. En la lista desplegable **Acción**, seleccione la acción para el Control de aplicaciones:

- **Probar reglas**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución esté prohibida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, estarían bloqueadas.

- **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:

- **Sí**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.

- **No**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.

- **Prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica la regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

Si es necesario, agregue reglas de Control de aplicaciones.

9. Establezca la configuración avanzada de Control de aplicaciones:

- **Supervisar la carga de módulos DLL (aumenta significativamente la carga del sistema)**. Si se selecciona la casilla, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. En el informe se registra información acerca del módulo de DLL y la aplicación que cargó el mismo.

  Si planea supervisar la carga de controladores y módulos DLL, asegúrese de que una de las siguientes reglas esté habilitada en la configuración de Control de aplicaciones: la **Imagen de oro** predeterminada u otra regla que contenga la categoría KL "**Imagen de oro\Certificados de confianza**" y que garantice que los módulos DLL y los controladores de confianza se carguen antes del arranque de Kaspersky Endpoint Security. Habilitar la supervisión de la carga de módulos DLL y controladores cuando la regla **Imagen de oro** está deshabilitada puede causar inestabilidad en el sistema operativo.

  Kaspersky Endpoint Security solamente supervisa los módulos DLL y los controladores cargados desde que se seleccionó la casilla. Después de seleccionar la casilla, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y los controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.

- **Usar verificación estricta de firma digital**. Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si se selecciona esta casilla, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas con certificados solo del almacén de confianza de certificados del sistema. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección, por ejemplo, la tarea *Análisis de malware*. Sin embargo, si especifica un certificado de un almacén diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla.

  Si la casilla no está seleccionada, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas por un certificado de Trusted Root Certificate Store de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección controlan la actividad de tales aplicaciones.

- **Mensaje para bloqueos**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.

- **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

10. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de aplicaciones**.

5. Active el interruptor de **Control de aplicaciones HABILITADO**.

6. En el bloque **Modo de funcionamiento**, seleccione **Bloquear todo excepto la lista de reglas**.

7. En el bloque **Acción**, seleccione la acción del Control de aplicaciones:

   - **Informar**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución esté prohibida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, estarían bloqueadas.

   - **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:

   - **Habilitado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.

   - **Deshabilitado**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.

   - **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica la regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

   Si es necesario, agregue reglas de Control de aplicaciones.

9. Establezca la configuración avanzada de Control de aplicaciones:

   - **Supervisar la carga de módulos DLL**. Si se selecciona la casilla, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. En el informe se registra información acerca del módulo de DLL y la aplicación que cargó el mismo.

Si planea supervisar la carga de controladores y módulos DLL, asegúrese de que una de las siguientes reglas esté habilitada en la configuración de Control de aplicaciones: la **Imagen de oro** predeterminada u otra regla que contenga la categoría KL "**Imagen de oro\Certificados de confianza**" y que garantice que los módulos DLL y los controladores de confianza se carguen antes del arranque de Kaspersky Endpoint Security. Habilitar la supervisión de la carga de módulos DLL y controladores cuando la regla **Imagen de oro** está deshabilitada puede causar inestabilidad en el sistema operativo.

Kaspersky Endpoint Security solamente supervisa los módulos DLL y los controladores cargados desde que se seleccionó la casilla. Después de seleccionar la casilla, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y los controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.

- **Usar verificación estricta de firma digital**. Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si se selecciona esta casilla, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas con certificados solo del almacén de confianza de certificados del sistema. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección, por ejemplo, la tarea *Análisis de malware*. Sin embargo, si especifica un certificado de un almacén diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla.

  Si la casilla no está seleccionada, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas por un certificado de Trusted Root Certificate Store de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección controlan la actividad de tales aplicaciones.

- **Mensaje para el usuario**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.

- **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

10. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo habilitar el modo de aplicaciones bloqueadas en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.

3. Active el interruptor de **Control de aplicaciones**.

4. En el bloque **Modo de Control de inicio de aplicaciones**, seleccione **Lista de rechazados: se podrá iniciar cualquier aplicación, excepto las que aparezcan en la lista de reglas**.

5. En el bloque **Acción al iniciar aplicaciones bloqueadas por las reglas**, seleccione la acción del Control de aplicaciones:

   - **Informar (modo de prueba) y registrar eventos en informe**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución esté prohibida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, estarían bloqueadas.

   - **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:

- **Habilitado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.
- **Deshabilitado**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.
- **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica la regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

Si es necesario, agregue reglas de Control de aplicaciones.

7. Establezca la configuración avanzada de Control de aplicaciones:

- **Supervisar la carga de módulos DLL**. Si se selecciona la casilla, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. En el informe se registra información acerca del módulo de DLL y la aplicación que cargó el mismo.

  Si planea supervisar la carga de controladores y módulos DLL, asegúrese de que una de las siguientes reglas esté habilitada en la configuración de Control de aplicaciones: la **Imagen de oro** predeterminada u otra regla que contenga la categoría KL "**Imagen de oro\Certificados de confianza**" y que garantice que los módulos DLL y los controladores de confianza se carguen antes del arranque de Kaspersky Endpoint Security. Habilitar la supervisión de la carga de módulos DLL y controladores cuando la regla **Imagen de oro** está deshabilitada puede causar inestabilidad en el sistema operativo.

  Kaspersky Endpoint Security solamente supervisa los módulos DLL y los controladores cargados desde que se seleccionó la casilla. Después de seleccionar la casilla, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y los controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.

- **Usar verificación estricta de firma digital**. Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si se selecciona esta casilla, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas con certificados solo del almacén de confianza de certificados del sistema. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección, por ejemplo, la tarea *Análisis de malware*. Sin embargo, si especifica un certificado de un almacén diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla.

  Si la casilla no está seleccionada, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas por un certificado de Trusted Root Certificate Store de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección controlan la actividad de tales aplicaciones.

- **Plantillas de mensajes sobre el bloqueo de la aplicación**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.
- **Plantilla del mensaje que se muestra al bloquearse el inicio de una aplicación**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

8. Guarde los cambios.

Como resultado, el Control de aplicaciones bloquea las aplicaciones bloqueadas. Kaspersky Endpoint Security también genera eventos de *Inicio de 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 referencia

Puede usar un equipo de referencia para crear una imagen con un conjunto de aplicaciones que necesite. Luego, puede usar esta imagen para implementar el sistema operativo y las aplicaciones en otros equipos. No siempre es posible mantener la imagen actualizada. Control de aplicaciones le permite mantener una lista de aplicaciones permitidas basada en un equipo de referencia. Control de aplicaciones determina automáticamente qué aplicaciones están instaladas en el equipo de referencia y actualiza la categoría. De esta manera, los equipos obtienen una lista actualizada de aplicaciones permitidas.

La configuración del Control de aplicaciones en función de un equipo de referencia implica los siguientes pasos:

1. Creación de una categoría de actualización automática. Al crear la nueva categoría, seleccione la **Categoría que incluye archivos ejecutables de una carpeta específica** y seleccione su equipo de referencia.

   Cómo crear una categoría actualizada automáticamente 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 **Nueva categoría** 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 el tipo de categoría.

   Paso 2. Introducción de un nombre de categoría de usuario

   En este paso, especifique un nombre para la categoría de aplicaciones.

   Paso 3. Configuración

   > Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados**.

En este paso, haga clic en el botón **Agregar** y especifique los equipos cuyos archivos ejecutables agregará Kaspersky Security Center a la categoría de aplicaciones. Todos los archivos ejecutables que se encuentren en la carpeta **Archivos ejecutables** serán agregados por Kaspersky Security Center en la categoría de aplicaciones.

En este paso, puede realizar los siguientes ajustes:

- Algoritmo para el cálculo de la función hash. Para seleccionar un algoritmo, debe seleccionar al menos una de las siguientes casillas:
  - **Calcular el hash SHA256 de los archivos de esta categoría (opción compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.
  - **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.
- La casilla de verificación **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 **Sincronizar datos con el repositorio del Servidor de administración** está desactivada, Kaspersky Security Center no realizará ninguna modificación en la categoría de una aplicación después de que se haya creado.

Paso 4. Filtrar

En este paso, configure un filtro para los archivos.

Puede especificar el tipo de archivo que desea utilizar para crear la categoría de la aplicación.

- **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 solo coincidirá con los archivos fuera de las categorías de la aplicación.

Puede especificar carpetas de equipos seleccionados que contienen archivos que desea usar para crear la categoría de la aplicación.

- **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 acceso a la carpeta.

Paso 5. Creación de una categoría personalizada

Salga del Asistente.

Cómo crear una categoría con contenido agregado 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 **Agregar**.

   Esto inicia el asistente de creación de categorías de aplicaciones.

3. Establezca la configuración general de la categoría de la aplicación:

   - Nombre de la categoría.
   - Método de creación de categorías. Seleccione **Categoría que incluye archivos ejecutables de dispositivos seleccionados** como el tipo de categoría.

   Vaya al siguiente paso.

4. Establezca la configuración avanzada de la categoría de la aplicación:

   - Especifique los equipos desde los cuales Kaspersky Security Center agregará archivos ejecutables a la categoría de aplicaciones. Todos los archivos ejecutables que se encuentren en la carpeta **Archivos ejecutables** serán agregados por Kaspersky Security Center en la categoría de aplicaciones.
   - 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. Salga del Asistente.

Al crear una categoría actualizada 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 la categoría y seleccionar carpetas individuales.

2. Selección del modo de Control de aplicaciones. Debe evitar la ejecución de todas las aplicaciones que no están explícitamente permitidas. Para ello, seleccione el modo *Aplicaciones bloqueadas*.

3. Creación de regla de Control de aplicaciones. En la configuración de la regla, seleccione la categoría a la que pertenecen los archivos ejecutables del equipo de referencia.

   Cómo configurar el Control de aplicaciones basado en un equipo de referencia 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 correspondiente 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 de verificación **Control de aplicaciones**.

6. En el bloque **Configuración de Control de aplicaciones**, utilice la lista desplegable **Modo de control** para seleccionar **Lista de rechazados**.

7. En la lista desplegable **Acción**, seleccione la acción para el Control de aplicaciones:

   - **Probar reglas**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución esté prohibida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, estarían bloqueadas.

   - **Aplicar reglas**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

8. En la lista de reglas de Control de aplicaciones, haga clic en el botón **Agregar**.

   Esto inicia el asistente para agregar una regla de Control de aplicaciones.

9. En la lista desplegable **Categoría**, seleccione una categoría actualizada automáticamente según el equipo de referencia.

10. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de Control de aplicaciones.

11. Establezca la configuración avanzada de la regla de Control de aplicaciones:

    - **Denegar a los demás usuarios**. La aplicación evita que se inicien 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 con permiso para crear otros archivos ejecutables que posteriormente podrán ejecutarse.

12. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar el Control de aplicaciones basado en un equipo de referencia 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de aplicaciones**.

5. Active el interruptor de **Control de aplicaciones HABILITADO**.

6. En el bloque **Modo de funcionamiento**, seleccione **Bloquear todo excepto la lista de reglas**.

7. En el bloque **Acción**, seleccione la acción del Control de aplicaciones:

   - **Informar**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución esté prohibida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, estarían bloqueadas.

   - **Aplicar reglas**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

8. En la lista de reglas de Control de aplicaciones, haga clic en el botón **Agregar**.

   Esto inicia el asistente para agregar una regla de Control de aplicaciones.

9. En **Categorías/aplicaciones**, seleccione una categoría actualizada automáticamente según el equipo de referencia.

10. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de Control de aplicaciones.

11. Establezca la configuración avanzada de la regla de Control de aplicaciones:

    - **Usuarios**. La aplicación evita que se inicien 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 con permiso para crear otros archivos ejecutables que posteriormente podrán ejecutarse.

12. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar el Control de aplicaciones basado en un equipo de referencia en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.

3. Active el interruptor de **Control de aplicaciones**.

4. En el bloque **Modo de Control de inicio de aplicaciones**, seleccione **Lista de rechazados: se podrá iniciar cualquier aplicación, excepto las que aparezcan en la lista de reglas**.

5. En el bloque **Acción al iniciar aplicaciones bloqueadas por las reglas**, seleccione la acción del Control de aplicaciones:

    - **Informar (modo de prueba) y registrar eventos en informe**. El Control de aplicaciones no bloquea las aplicaciones cuya ejecución esté prohibida por las reglas, pero genera eventos sobre la ejecución de aplicaciones que, de otro modo, estarían bloqueadas.

    - **Bloquear**. El Control de aplicaciones bloquea las aplicaciones bloqueadas y genera los eventos correspondientes.

6. En la lista de reglas de Control de aplicaciones, haga clic en el botón **Agregar**.

   Esto inicia el asistente para agregar una regla de Control de aplicaciones.

7. En **Categoría**, seleccione una categoría actualizada automáticamente según el equipo de referencia.

8. Seleccione los usuarios o grupos de usuarios a los que desea aplicar la regla de Control de aplicaciones.

9. Establezca la configuración avanzada de la regla de Control de aplicaciones:

   - **Denegar a los demás usuarios**. La aplicación evita que se inicien 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 con permiso para crear otros archivos ejecutables que posteriormente podrán ejecutarse.

10. Guarde los cambios.

Administración de las reglas de Control de aplicaciones

Kaspersky Endpoint Security controla el inicio de las aplicaciones por parte de los usuarios mediante reglas. Una regla de Control de aplicaciones está formada por una serie condiciones de activación y una serie de acciones. Cuando una regla se activa, Control de aplicaciones realiza la acción que la regla le indica (permitir o impedir que los usuarios inicien una aplicación).

Condiciones de activación de regla

Una condición que activa una regla tiene la siguiente correlación: "tipo de condición - criterio de la condición - valor de la condición". Según las condiciones de activación de la regla, Kaspersky Endpoint Security aplica (o no) una regla a la aplicación.

Los siguientes tipos de condiciones se utilizan en las reglas:

- *Condiciones de inclusión*. Kaspersky Endpoint Security aplica la regla a la aplicación si la aplicación coincide con al menos una condición de inclusión.

- *Condiciones de exclusión*. Kaspersky Endpoint Security no aplica la regla a la aplicación si la aplicación coincide con al menos una de las condiciones de exclusión y no coincide con ninguna condición de inclusión.

Las condiciones de activación de regla se crean usando criterios. Se utilizan los siguientes criterios para crear reglas en Kaspersky Endpoint Security:

- Ruta de acceso de la carpeta que contiene el archivo ejecutable de la aplicación o ruta de acceso del 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 un disco extraíble.

Se debe especificar el valor del criterio para cada criterio usado en la condición. Si los parámetros de la aplicación que se está iniciando coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, el Control de aplicaciones lleva a cabo la acción especificada en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, el Control de aplicaciones no controla el inicio de la aplicación.

Si seleccionó un certificado como condición de activación de la regla, debe asegurarse de que este certificado se agregue al almacenamiento del sistema de confianza en el equipo y comprobar la configuración de uso de almacenamiento del sistema de confianza en la aplicación.

Decisiones que toma el componente Control de aplicaciones cuando se activa una regla

Cuando se activa una regla, el Control de aplicaciones permite que los usuarios (o grupos de usuarios) inicien aplicaciones o bloquea el inicio de acuerdo con la regla. Usted puede seleccionar un usuario o un grupo de usuarios a los que se les permita o no iniciar aplicaciones que activen una regla.

Si una regla no especifica los usuarios autorizados para iniciar aplicaciones que cumplan con la regla, se denomina regla de *bloqueo*.

Una regla que no especifica ningún usuario que no esté autorizado para iniciar aplicaciones que cumplan con la regla se denomina regla de *autorización*.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. Por ejemplo, si se ha especificado una regla de autorización del Control de aplicaciones para un grupo de usuarios y también se ha especificado una regla de bloqueo de este componente para un usuario de este grupo de usuarios, este usuario no podrá iniciar la aplicación.

Estado operativo de una regla

Las reglas de control de aplicaciones pueden tener uno de los siguientes estados operativos:

- **Habilitado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.
- **Deshabilitado**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.
- **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite iniciar las aplicaciones a las cuales se aplican las reglas pero registra la información sobre el inicio de dichas aplicaciones en el informe.

Adición de una condición de activación para la regla de Control de aplicaciones

Para mayor comodidad al crear Regla de control de aplicaciones, puede crear categorías de aplicaciones.

Se recomienda crear la categoría "Aplicaciones de trabajo" que cubra el conjunto de aplicaciones estándar que se utilizan en la compañía. Si diferentes grupos de usuarios usan conjuntos de aplicaciones diferentes en su trabajo, se puede crear una categoría de aplicaciones separada para cada grupo de usuario.

Para crear una categoría de aplicación en la Consola de administración, realice lo siguiente:

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 **Nueva categoría** en el espacio de trabajo.

   Se inicia el asistente de creación de categorías de usuarios.
4. Siga las instrucciones del asistente de creación de categorías de usuarios.

Paso 1. Selección del tipo de categoría

En este paso, seleccione uno de los tipos siguientes de categorías de aplicaciones:

- Categoría con contenido agregado de forma manual. Los datos de los archivos ejecutables se agregan de forma manual a la categoría. Si seleccionó este tipo de categoría, en el paso *Configure las condiciones que se usarán para incluir aplicaciones en las categorías* y el paso *Configure las condiciones que se usarán para excluir aplicaciones de las categorías*, podrá definir los criterios por los cuales los archivos ejecutables se incluirán en la categoría.
- Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Estos archivos ejecutables se procesan de forma automática y sus métricas se agregan a la categoría. Si seleccionó este tipo de categoría, en el paso *Configuración*, podrá seleccionar un equipo. Los archivos ejecutables del equipo que elija se incluirán automáticamente en la categoría.
- Categoría con los archivos ejecutables de una carpeta específica. Los archivos ejecutables de aplicaciones presentes en la carpeta especificada se procesan automáticamente y sus métricas se agregan a la categoría. Si seleccionó este tipo de categoría, en el paso *Carpeta de repositorio*, podrá seleccionar una carpeta. Los archivos ejecutables de la carpeta que elija se incluirán automáticamente en la categoría.

Para crear una categoría con contenido agregado automáticamente, Kaspersky Security Center genera un inventario de los archivos que tienen 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 aplicaciones.

Paso 3. Configuración de las condiciones para la inclusión de aplicaciones en una categoría

Al agregar un gran número de condiciones a las reglas de Control de aplicaciones (por ejemplo, hash de archivos), aumenta el consumo de recursos del equipo. Cuando el número total de condiciones alcanza las 50 000, pueden producirse problemas de rendimiento. Para optimizar el rendimiento, se recomienda revisar y reducir el número de condiciones.

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría con contenido agregado de forma manual**.

En este paso, en la lista desplegable **Agregar**, seleccione las condiciones que determinarán qué aplicaciones se incluirán en la categoría:

- **De la lista de archivos ejecutables**. Agrega aplicaciones desde la lista de archivos ejecutables en el dispositivo cliente a la categoría personalizada.
- **De las propiedades de archivo**. Especifica los datos detallados de archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.
- **Metadatos de los archivos de la carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.
- **Sumas de comprobación de los archivos de la carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los hashes de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.
- **Certificados de los archivos de la carpeta**. Seleccione una carpeta en el dispositivo cliente que contiene archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

  No se recomienda utilizar condiciones cuyas propiedades no tengan especificado el parámetro **Huella digital del certificado**.

- **Metadatos de los archivos del instalador MSI**. Seleccione un paquete MSI. Kaspersky Security Center tomará los metadatos de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.
- **Sumas de comprobación de los archivos incluidos en el instalador MSI de la aplicación**. Seleccione un paquete MSI. Kaspersky Security Center tomará los hashes de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.
- **De la categoría KL**. Especifique una categoría KL como una condición para agregar aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que comparten atributos de temas. Los expertos de Kaspersky son los encargados de mantener la lista. Por ejemplo, la categoría KL conocida como *Aplicaciones de ofimática* incluye aplicaciones del conjunto de programas de Microsoft Office, Adobe Acrobat y otras.

  Puede seleccionar todas las categorías KL para generar una lista extendida de aplicaciones de confianza.

- **Especificar la ruta a la aplicación (se pueden usar máscaras)**. Selecciona una carpeta en el dispositivo cliente. Kaspersky Security Center agregará archivos ejecutables desde esta carpeta a la categoría personalizada.

- **Seleccionar certificado del repositorio**. Seleccione certificados que se hayan utilizado para firmar archivos ejecutables. Se los usará como condición para agregar aplicaciones a la categoría personalizada.

  No se recomienda utilizar condiciones cuyas propiedades no tengan especificado el parámetro **Huella digital del certificado**.

  Puede elegir el almacén de certificados. De manera predeterminada, Control de aplicaciones aplica reglas solo para las aplicaciones firmadas con un certificado del almacén de confianza de certificados del sistema. Esta opción se habilita en la casilla de verificación **Usar verificación estricta de firma digital**.

- **Tipo de unidad**. Seleccione el tipo de dispositivo de almacenamiento (todos los discos duros y unidades extraíbles o solo unidades extraíbles) como una condición para agregar aplicaciones a la categoría personalizada.

Paso 4. Configuración de las condiciones para la exclusión de aplicaciones desde una categoría

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría con contenido agregado de forma manual**.

Las aplicaciones especificadas en este paso se excluyen de la categoría incluso si estas aplicaciones se especificaron en el paso "Configuración de las condiciones para las aplicaciones incluidas en una categoría".

En este paso, en la lista desplegable **Agregar**, seleccione las condiciones que determinarán qué aplicaciones quedarán excluidas de la categoría:

- **De la lista de archivos ejecutables**. Agrega aplicaciones desde la lista de archivos ejecutables en el dispositivo cliente a la categoría personalizada.

- **De las propiedades de archivo**. Especifica los datos detallados de archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Metadatos de los archivos de la carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Sumas de comprobación de los archivos de la carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los hashes de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Certificados de los archivos de la carpeta**. Seleccione una carpeta en el dispositivo cliente que contiene archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Metadatos de los archivos del instalador MSI**. Seleccione un paquete MSI. Kaspersky Security Center tomará los metadatos de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.

- **Sumas de comprobación de los archivos incluidos en el instalador MSI de la aplicación**. Seleccione un paquete MSI. Kaspersky Security Center tomará los hashes de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.

- **De la categoría KL**. Especifique una categoría KL como una condición para agregar aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que comparten atributos de temas. Los expertos de Kaspersky son los encargados de mantener la lista. Por ejemplo, la categoría KL conocida como *Aplicaciones de ofimática* incluye aplicaciones del conjunto de programas de Microsoft Office, Adobe Acrobat y otras.

  Puede seleccionar todas las categorías KL para generar una lista extendida de aplicaciones de confianza.

- **Especificar la ruta a la aplicación (se pueden usar máscaras)**. Selecciona una carpeta en el dispositivo cliente. Kaspersky Security Center agregará archivos ejecutables desde esta carpeta a la categoría personalizada.

- **Seleccionar certificado del repositorio**. Seleccione certificados que se hayan utilizado para firmar archivos ejecutables. Se los usará como condición para agregar aplicaciones a la categoría personalizada.

- **Tipo de unidad**. Seleccione el tipo de dispositivo de almacenamiento (todos los discos duros y unidades extraíbles o solo unidades extraíbles) como una condición para agregar aplicaciones a la categoría personalizada.

Paso 5. Configuración

> Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados**.

En este paso, haga clic en el botón **Agregar** y especifique los equipos cuyos archivos ejecutables agregará Kaspersky Security Center a la categoría de aplicaciones. Todos los archivos ejecutables que se encuentren en la carpeta **Archivos ejecutables** serán agregados por Kaspersky Security Center en la categoría de aplicaciones.

En este paso, puede realizar los siguientes ajustes:

- Algoritmo para el cálculo de la función hash. Para seleccionar un algoritmo, debe seleccionar al menos una de las siguientes casillas:

  - **Calcular el hash SHA256 de los archivos de esta categoría (opción compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.

  - **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.

- La casilla de verificación **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 **Sincronizar datos con el repositorio del Servidor de administración** está desactivada, Kaspersky Security Center no realizará ninguna modificación en la categoría de una aplicación después de que se haya creado.

Paso 6. Carpeta de repositorio

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría con los archivos ejecutables de una carpeta específica**.

En este paso, especifique la carpeta en la cual Kaspersky Security Center buscará archivos ejecutables para agregar automáticamente aplicaciones a la categoría de aplicación.

En este paso, puede realizar los siguientes ajustes:

- La casilla de verificación **Incluir DLL en esta categoría**. Seleccione esta casilla si desea que la categoría de aplicaciones incluya bibliotecas de vínculos dinámicos (archivos DLL).

  La categoría de aplicación Incluir archivos DLL puede reducir el rendimiento de Kaspersky Security Center.

- La casilla de verificación **Incluir datos de scripts en esta categoría**. Seleccione esta casilla si desea que la categoría de aplicaciones incluya también scripts.

  Incluir scripts en la categoría de aplicaciones puede afectar el rendimiento de Kaspersky Security Center.

- Algoritmo para el cálculo de la función hash. Para seleccionar un algoritmo, debe seleccionar al menos una de las siguientes casillas:

  - **Calcular el hash SHA256 de los archivos de esta categoría (opción compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.

  - **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.

- La casilla de verificación **Forzar análisis de cambios en carpeta**. 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 análisis de cambios en carpeta**, Kaspersky Security Center busca los archivos ejecutables en la carpeta usada para agregar automáticamente a la categoría de aplicación solamente si se realizaron cambios en la carpeta, agregando o borrando un archivo de allí.

- 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 utilizada para agregarlos automáticamente a la categoría de la aplicación.

  El campo está disponible si la casilla de verificación **Forzar análisis de cambios en carpeta** está seleccionada.

Paso 7. Creación de una categoría personalizada

Salga del Asistente.

Para agregar una nueva condición de activación para una regla de Control de aplicaciones en la interfaz de la aplicación, realice lo siguiente:

1. En la ventana principal de la aplicación 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 los botones **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Esto abre la lista de reglas de control de aplicaciones.

4. Seleccione la regla para la cual desea configurar una condición de activación.

   Se abren las propiedades de Regla de Control de aplicaciones.

5. Seleccione la pestaña **Condiciones: N** o la pestaña **Exclusiones: N** y haga clic en el botón **Agregar**.

6. Seleccione las condiciones de activación para la Regla de Control de aplicaciones:

   - **Condiciones con las 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 seleccionar el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a archivo o carpeta**.

   - **Condiciones "Categoría KL"**. Una *categoría KL* es una lista de aplicaciones que comparten atributos de temas. Los expertos de Kaspersky son los encargados de mantener la lista. Por ejemplo: la categoría KL "Aplicaciones de ofimática" incluye todas las aplicaciones del conjunto de programas de Microsoft Office y Adobe® Acrobat®, entre otros.

   - **Condición personalizada**. Puede seleccionar el archivo de la aplicación y seleccionar una de las condiciones de activación de la regla: **Hash del archivo**, **Certificado**, **Metadatos** o **Ruta de acceso a archivo o carpeta**.

   - **Condición por unidad de archivo (unidad extraíble)**. La regla de Control de aplicaciones se aplica solo a los archivos que se ejecutan en una unidad extraíble.

   - **Condiciones con las propiedades de los archivos de la carpeta especificada**. La regla de Control de aplicaciones se aplica solo a los archivos dentro de la carpeta especificada. También puede incluir o excluir archivos de subcarpetas. Debe seleccionar el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a archivo o carpeta**.

7. Guarde los cambios.

Al agregar condiciones, tenga en cuenta las siguientes consideraciones especiales para Control de aplicaciones:

- Kaspersky Endpoint Security admite los caracteres `*` y `?` para ingresar una máscara en los metadatos: **Nombre de archivo**, **Nombre de la aplicación**, **Proveedor**.

- Kaspersky Endpoint Security no admite un hash de archivo MD5 y no controla el inicio de aplicaciones basadas en un hash MD5. Se utiliza un hash SHA256 como condición de activación de la regla.

- No se recomienda usar solo los criterios de **Emisor** y **Sujeto del certificado** como condiciones de activación de la regla. Utilizar estos criterios no es confiable.

- Si está usando vínculos simbólicos en el campo **Ruta de acceso a archivo o carpeta**, le aconsejamos resolver el vínculo simbólico para que la regla de Control de aplicaciones funcione correctamente. Para ello, haga clic en el botón **Resolver vínculo simbólico**.

Agregar archivos ejecutables de la carpeta Archivos ejecutables a la categoría de la 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 como resultado de la tarea Inventario.

Para agregar archivos ejecutables de la carpeta Archivos ejecutables a la categoría de la aplicación, haga lo siguiente:

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 área de trabajo, seleccione los archivos ejecutables que desea agregar a la categoría de la aplicación.

4. Haga clic 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 siguientes acciones:

     - **Agregar a una nueva categoría de aplicación**. Seleccione esta opción si desea crear una nueva categoría de aplicación y agregar archivos ejecutables.

     - **Agregar a una categoría de aplicación existente**. Seleccione esta opción si desea seleccionar una categoría de aplicación existente y agregar archivos ejecutables.

   - En el bloque **Tipo de regla**, seleccione una de las siguientes opciones:

     - **Reglas para añadir a las inclusiones**. Seleccione esta opción si desea crear una condición que agregue archivos ejecutables a la categoría de la aplicación.

     - **Reglas para añadir a las exclusiones**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de la aplicación.

   - En el bloque **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:

     - **Detalles del certificado (o hashes SHA256 para archivos sin certificado)**.

     - **Detalles del certificado (los archivos sin certificado se omitirán)**.

- **Solo SHA256 (los archivos sin hash se omitirán)**.
- **Solo MD5 (modo suspendido, solo para Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Guarde los cambios.

Adición de archivos ejecutables relacionados con eventos a la categoría de la aplicación

Para agregar 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 del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.
3. Elija una selección de eventos relacionados con el funcionamiento del componente Control de aplicaciones (Visualización de eventos resultantes del funcionamiento del componente Control de aplicaciones, Visualización de eventos resultantes del funcionamiento de prueba 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 desea añadir a la categoría de la aplicación.
6. Haga clic derecho para abrir el menú contextual de los eventos seleccionados y seleccione **Agregar a categoría**.
7. En la ventana que se abre, defina la configuración de la categoría de la aplicación:
   - En la parte superior de la ventana, elija una de las siguientes acciones:
     - **Agregar a una nueva categoría de aplicación**. Seleccione esta opción si desea crear una nueva categoría de aplicación y agregar archivos ejecutables.
     - **Agregar a una categoría de aplicación existente**. Seleccione esta opción si desea seleccionar una categoría de aplicación existente y agregar archivos ejecutables.
   - En el bloque **Tipo de regla**, seleccione una de las siguientes opciones:
     - **Reglas para agregar a inclusiones**. Seleccione esta opción si desea crear una condición que agregue archivos ejecutables a la categoría de la aplicación.
     - **Reglas para agregar a exclusiones**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de la aplicación.
   - En el bloque **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:
     - **Detalles del certificado (o hashes SHA-256 para archivos sin certificado)**.
     - **Detalles del certificado (los archivos sin certificado se omitirán)**.

- **Solo SHA-256 (los archivos sin hash se omitirán)**.
- **Solo MD5 (modo suspendido, solo para Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Guarde los cambios.

Agregar una regla de control de aplicaciones

Para crear una regla de Control de aplicaciones utilizando Kaspersky Security Center:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 **Agregar**.
   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 inicia el asistente de creación de categorías de usuarios.
     b. Siga las instrucciones del asistente de creación de categorías de usuarios.
     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 aplicaciones creada en función de la cual quiera crear una regla.
6. En la tabla **Usuarios y sus derechos**, haga clic en el botón **Agregar**.
   Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

7. En la tabla **Usuarios y sus derechos**, haga lo siguiente:

   - Si quiere permitir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione la casilla **Permitir** en las filas correspondientes.

   - 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 aplicaciones seleccionada como actualizadores de confianza que permiten crear otros archivos ejecutables que posteriormente podrán ejecutarse, seleccione 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 agregar una regla de control de aplicaciones:

1. En la ventana principal de la aplicación 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 los botones **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Esto abre la lista de reglas de control de aplicaciones.

4. Haga clic en **Agregar**.

   Se abre la ventana de configuración Regla 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**, escriba el nombre de la regla.

   b. En el campo **Descripción**, escriba la descripción de la regla.

   c. En la tabla **Usuarios y sus derechos**, haga clic en el botón **Agregar**.

      Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

      La regla se aplica a todos los usuarios de manera 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 desea que la aplicación impida la ejecución de aplicaciones que cumplan con las condiciones de activación de reglas para todos los usuarios que no figuren en la tabla **Usuarios y sus derechos** y que no sean 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 **Actualizadores de confianza** si desea que Kaspersky Endpoint Security considere las aplicaciones que cumplen las condiciones de activación de la regla 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 marcador de *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 **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.

Cambio del estado de una regla de Control de aplicaciones mediante Kaspersky Security Center

Para cambiar el estado de una regla de Control de aplicaciones, realice lo siguiente en la Consola de administración:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 para mostrar el menú contextual y seleccionar una de las siguientes opciones:

   - **Sí**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.

   - **No**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.

   - **Prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica la regla, pero registra la información sobre el inicio de dichas 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, realice lo siguiente:

1. En la ventana principal de la aplicación 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 los botones **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Esto abre la lista de reglas de control de aplicaciones.

4. En la columna **Estado**, abra el menú contextual y seleccione una de estas opciones:

   - **Habilitado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.

   - **Deshabilitado**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.

   - **Modo de prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica esta regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

5. Guarde los cambios.

Exportar e importar 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 otro servidor.

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 con el modo de Control de aplicaciones activo. Esto quiere decir que, si el Control de aplicaciones funciona en modo de lista de rechazados, Kaspersky Endpoint Security solo exporta las reglas con este modo. Para exportar la lista de reglas con el modo de lista de admitidos, necesita cambiar el modo y volver a ejecutar la operación de exportación.

- Para operar, Kaspersky Endpoint Security utiliza categorías de aplicaciones para las reglas de Control de aplicaciones. Al migrar la lista de las reglas de Control de aplicaciones a un servidor diferente, también necesita migrar la lista de categorías de aplicaciones. Para obtener más información sobre las categorías de aplicaciones de exportación e importación, consulte la Ayuda de Kaspersky Security Center.

Cómo exportar e importar una lista de reglas de Control de aplicaciones a la Consola de administración (MMC)

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

2. Seleccione la directiva correspondiente 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 la regla de acceso que desea 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 vínculo **Exportar**.

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

   Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.

5. Para importar una lista de reglas de control de aplicaciones:

   a. Haga clic en el vínculo **Importar**.

   En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

   b. Abra el archivo.

   Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

6. Guarde los cambios.

Cómo exportar e importar una lista de reglas de control de aplicaciones a 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 ficha **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 rechazados o lista de admitidos de aplicaciones.

6. Para exportar la lista de reglas:

   a. Seleccione la regla de acceso que desea 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 que se usará para importar la lista de reglas.

   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

8. Guarde los cambios.

Visualización de eventos resultantes de la operación del componente Control de aplicaciones

Para ver los eventos resultantes de la operación del componente Control de aplicaciones recibidos por Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.

3. Haga clic en el botón **Crear selección**.

4. En la ventana que se abre, vaya a la sección **Eventos**.

5. Haga clic en el botón **Quitar selección a todo**.

6. En la tabla **Eventos**, seleccione la casilla **Inicio de 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**.

Acceso al informe sobre las aplicaciones bloqueadas

Para ver el informe sobre aplicaciones bloqueadas:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **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 las instrucciones del Asistente de plantilla de informe. En el paso **Selección del tipo de plantilla de informe** seleccione **Otro** → **Informe sobre aplicaciones prohibidas**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la pestaña **Informes**.

5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

Prueba de las reglas de Control de aplicaciones

Para garantizar que las reglas de control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas. Cuando se habilita la prueba de las Reglas de control de aplicaciones, Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio está prohibido por el Control de aplicaciones, sino que enviará notificaciones sobre su inicio al Servidor de administración.

El análisis del funcionamiento de las reglas de Control de aplicaciones en el modo de prueba incluye revisar los eventos de Control de aplicaciones resultantes comunicados a Kaspersky Security Center. Si el modo de prueba no bloquea los eventos de inicio de todas las aplicaciones necesarias para el trabajo del usuario del equipo, significa que se han creado las reglas correctas. De lo contrario, es aconsejable actualizar las parametrizaciones de las reglas creadas, crear reglas adicionales o borrar las reglas existentes.

De manera predeterminada, Kaspersky Endpoint Security permite ejecutar cualquier aplicación, excepto las que se han prohibido a través de una regla.

Habilitación y deshabilitación de la prueba de reglas de Control de aplicaciones

Para habilitar o deshabilitar el modo de prueba para las reglas de Control de aplicaciones a través de Kaspersky Security Center:

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

2. Seleccione la directiva correspondiente 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, el Control de aplicaciones permite que todos los usuarios inicien cualquier aplicación, excepto en casos en que las aplicaciones cumplan con las condiciones de las reglas de bloqueo de Control de aplicaciones.

   - **Lista de admitidos**. Si se selecciona esta opción, el Control de aplicaciones bloquea a todos los usuarios de iniciar alguna aplicación, excepto en casos en que las aplicaciones cumplen con las condiciones de reglas de habilitación del Control de aplicaciones.

5. Realice una de las siguientes acciones:

   - Si desea habilitar el modo de prueba para las reglas de Control de aplicaciones, seleccione la opción **Probar reglas** en la lista desplegable **Acción**.

   - Si desea habilitar Control de aplicaciones para administrar el inicio de las aplicaciones en los equipos de los usuarios, en la lista desplegable, seleccione **Aplicar reglas**.

6. Guarde los cambios.

Para habilitar la prueba de las Reglas de control de aplicaciones o para seleccionar una acción de bloqueo para el Control de aplicaciones:

1. En la ventana principal de la aplicación 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 los botones **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

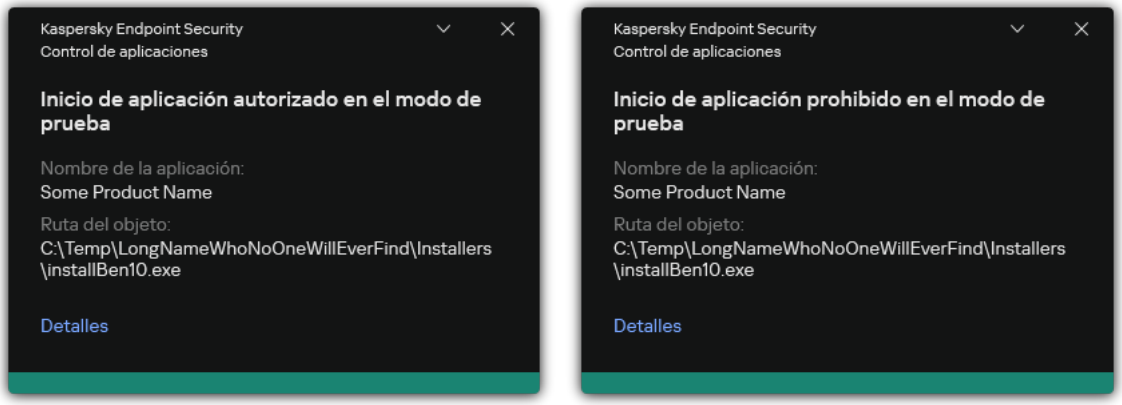
   Esto abre la lista de reglas de control de aplicaciones.

4. En la columna **Estado**, seleccione **Modo de prueba**.

   Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica esta regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

5. Guarde los cambios.

Kaspersky Endpoint Security no bloqueará aplicaciones cuyo inicio no esté permitido 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 (consulte la figura a continuación).



Notificaciones de Control de aplicaciones en modo de prueba

Acceso al 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 del **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 las instrucciones del Asistente de plantilla de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione **Otro** → **Informe sobre aplicaciones prohibidas en modo de prueba**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la pestaña **Informes**.
5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

Visualización de eventos resultantes de la operación de prueba del componente Control de aplicaciones

Para ver los eventos que Kaspersky Security Center recibió mientras Control de aplicaciones funcionaba en modo de prueba:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.
3. Haga clic en el botón **Crear selección**.
4. En la ventana que se abre, vaya a la sección **Eventos**.
5. Haga clic en el botón **Quitar selección a todo**.

6. En la tabla **Eventos**, seleccione las casillas **Inicio de aplicación prohibido en el modo de prueba** y **Inicio de aplicación autorizado en el 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**.

Monitor de actividades de aplicaciones

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El *Monitor de actividades de aplicaciones* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de las aplicaciones en el equipo de un usuario.

El uso de Monitor de actividades 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 Monitor de actividades de aplicaciones en la ventana principal de la aplicación está oculto.

Para iniciar el Monitor de actividades de aplicaciones, realice lo siguiente:

En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Monitor de actividades de aplicaciones**.

En esta ventana, se brinda información acerca de la actividad de las aplicaciones en el equipo del usuario en tres pestañas:

- En la pestaña **Todas las aplicaciones**, se muestra información acerca de todas las aplicaciones instaladas en el equipo.
- En la pestaña **En ejecución**, se muestra información en tiempo real acerca del consumo de los recursos del equipo que cada aplicación realiza. Desde esta pestaña, puede continuar para configurar los permisos de una sola aplicación.
- En la pestaña **Ejecutadas al inicio**, se 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 Monitor de actividades de aplicaciones.

Cómo ocultar Monitor de actividades de aplicaciones en la interfaz de la aplicación con la Consola de administración (MMC)

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

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

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

4. Use la casilla **Ocultar la sección Monitor de actividades de aplicaciones** para otorgar o revocar el acceso a la herramienta.

5. Guarde los cambios.

Cómo ocultar Monitor de actividades de aplicaciones en la interfaz de la aplicación con 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 ficha **Configuración de la aplicación**.

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

5. Use la casilla **Ocultar la sección Monitor de actividades de aplicaciones** para otorgar o revocar el acceso a la herramienta.

6. Guarde los cambios.

Reglas para crear máscaras de nombres para archivos o carpetas

La *máscara del nombre de un archivo o carpeta* es una representación del nombre y la extensión de un archivo o del nombre de una carpeta. Las máscaras se forman utilizando caracteres comunes.

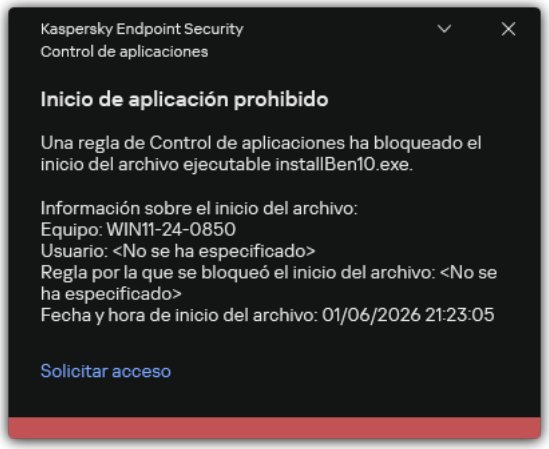
Para crear la máscara del nombre de un archivo o de una carpeta, puede usar los siguientes caracteres comunes:

- 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` ubicados en las carpetas y subcarpetas del disco C:.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 las plantillas de mensajes de Control de aplicaciones

Cuando un usuario intenta iniciar una aplicación bloqueada por una regla de Control de aplicaciones, Kaspersky Endpoint Security muestra un mensaje en el que se indica que el inicio de la aplicación está bloqueado. Los expertos de Kaspersky proporcionan una plantilla de mensaje al usuario en la que se describen las razones por las que se bloqueó la aplicación (consulte la figura a continuación). Se proporcionan variables especiales para administrar las plantillas de mensajes (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensajes para diferentes equipos. 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 que coincide con el equipo, el usuario y el evento específicos.



Notificación de Control de aplicaciones

Si el usuario cree que el inicio de la aplicación está bloqueado por error, puede usar el vínculo incluido en el texto del mensaje para enviar un mensaje al administrador de la red corporativa 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 y agregarle datos que pueden informar su decisión de permitir o bloquear el acceso a la aplicación. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del inicio de una aplicación para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 mensajes 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 correspondiente 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, donde debe configurar las plantillas de Control de aplicaciones:

   - **Mensaje para bloqueos**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.

     No puede configurar plantillas de mensajes para Control de aplicaciones en modo de prueba. Control de aplicaciones en modo de prueba muestra notificaciones predefinidas.

   - **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada utilizando el botón **Predeterminado**.

6. Guarde los cambios.

Cómo editar la plantilla de mensajes de Control de aplicaciones 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de aplicaciones**.

5. En el bloque **Plantillas de mensajes**, haga clic en el vínculo **Mensajes sobre el bloqueo del inicio de la aplicación** y configure las plantillas de los mensajes de Control de aplicaciones:

   - **Mensaje para el usuario**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.

     No puede configurar plantillas de mensajes para Control de aplicaciones en modo de prueba. Control de aplicaciones en modo de prueba muestra notificaciones predefinidas.

   - **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada utilizando el botón **Restaurar configuración predeterminada**.

6. Guarde los cambios.

Cómo editar la plantilla de mensajes de Control de aplicaciones en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 bloqueo de la aplicación**, configure plantillas para los mensajes de Control de aplicaciones:

   - **Mensaje para bloqueos**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.

     No puede configurar plantillas de mensajes para Control de aplicaciones en modo de prueba. Control de aplicaciones en modo de prueba muestra notificaciones predefinidas.

   - **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Agregar variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada 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 del usuario o del administrador:

- **Nombre de la regla que se activó**: `%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 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, con el formato `<device name>\<user alias>` (por ejemplo, `DESKTOP-123\John.Smith`).

- **Nombre de equipo**: `%COMPUTER_NAME%`.

  Nombre del equipo donde 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 de acceso del 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 está especificado en las propiedades del archivo ejecutable de la aplicación.

- **Proveedor**: `%FILE_PUBLISHER%`.

  Proveedor de la aplicación bloqueada.

- **Nombre de la aplicación**: `%FILE_PRODUCT_NAME%`.

  Nombre de la aplicación 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 se firmó el archivo ejecutable.

- **Sujeto del certificado**: `%CERT_SUBJECT%`.

  Asunto del certificado con el que se firmó el archivo ejecutable.

- **Huella digital del certificado**: `%CERT_THUMBPRINT%`.

  Huella digital del certificado con el que se firmó el archivo ejecutable.

Prácticas recomendadas para implementar una lista de aplicaciones permitidas

Al planificar la implementación de una lista de aplicaciones permitidas, se recomienda realizar las siguientes acciones:

1. Forme los siguientes tipos de grupos:

   - Grupos de usuario. Grupos de usuarios para quienes necesita permitir el uso de varios conjuntos de aplicaciones.

   - Grupos de administración. Uno o varios grupos de equipos a los cuales Kaspersky Security Center aplicará el modo de lista de aplicaciones permitidas. Es necesario crear varios grupos de equipos si se utilizan diferentes configuraciones de lista de admitidos para esos grupos.

2. Crea una lista de aplicaciones cuyo inicio esté permitido.

   Antes de crear una lista, se le aconseja que haga lo siguiente:

   a. Ejecute la tarea de inventario.

      Encontrará información para crear, reconfigurar e iniciar una tarea de inventario en la sección Administración de tareas.

   b. Ver la lista de archivos ejecutables.

Configuración del modo de lista de autorización para aplicaciones

Al configurar el modo de lista de admitidos, se recomienda realizar las siguientes acciones:

1. Crear categorías de aplicaciones que incluyan las aplicaciones cuyo inicio estará permitido.

   Puede seleccionar uno de los métodos siguientes para crear categorías de aplicaciones:

   - **Categoría con contenido agregado de forma manual**. Puede agregar manualmente a esta categoría usando las condiciones siguientes:

     - Metadatos de archivo. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables que tengan los metadatos especificados.

     - Código hash de archivo. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables que tengan el hash especificado.

       El uso de esta condición excluye la capacidad de instalar automáticamente actualizaciones porque las versiones diferentes de archivos tendrán un hash diferente.

     - Certificado de archivo. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables que tengan el certificado especificado.

     - Categoría KL Kaspersky Security Center agregará a la categoría de aplicaciones todas las aplicaciones que pertenezcan a la KL category especificada.

     - Carpeta de la aplicación. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables almacenados en la carpeta seleccionada.

       El uso de la condición **Carpeta de aplicación** puede no ser seguro porque se permitirá el inicio de cualquier aplicación desde la carpeta especificada. Se recomienda aplicar reglas que utilicen las categorías de aplicaciones con la condición **Carpeta de aplicación** solo a aquellos usuarios para los que se debe permitir la instalación automática de actualizaciones.

   - **Categoría con los archivos ejecutables de una carpeta específica**. Puede especificar una carpeta desde la cual los archivos ejecutables se asignen automáticamente a la categoría de aplicación creada.

   - **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados**. Puede especificar un equipo para el cual todos los archivos ejecutables se asignarán automáticamente a la categoría de aplicación creada.

     Si elige este método para crear las categorías de aplicaciones, Kaspersky Security Center recurrirá a la carpeta **Archivos ejecutables** para obtener información sobre las aplicaciones que estén instaladas en el equipo.

2. Seleccione el modo lista de admitidos para el componente Control de aplicaciones.

3. Cree Regla de control de aplicaciones usando las categorías de aplicaciones creadas.

> La regla **Imagen de oro** y la regla **Actualizadores de confianza** se definen inicialmente para el modo Lista de admitidos. Estas reglas de Control de aplicaciones corresponden a las KL categories. La categoría KL *Imagen de oro* incluye programas que aseguran el funcionamiento normal del sistema operativo. La categoría KL *Actualizadores de confianza* incluye actualizadores de los proveedores del software más respetables. No puede eliminar estas reglas. No se puede modificar la configuración de estas reglas. De forma predeterminada, la regla **Imagen de oro** está habilitada, y la regla **Actualizadores de confianza** está deshabilitada. A todos los usuarios se les permite iniciar aplicaciones que coincidan con las condiciones de activación de estas reglas.

4. Determine las aplicaciones para las que se debe permitir la instalación automática de actualizaciones.

   Puede permitir la instalación automática de actualizaciones utilizando uno de los métodos siguientes:

   - Especifique una lista ampliada de aplicaciones permitidas permitiendo el inicio de todas las aplicaciones que pertenezcan a cualquier categoría KL.

   - Especifique una lista ampliada de aplicaciones permitidas permitiendo el inicio de todas las aplicaciones firmadas con certificados.

     Para habilitar el inicio de todas las aplicaciones firmadas con certificados, puede crear una categoría con una condición basada en certificado que utilice solamente 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 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 aplicación** puede no ser seguro porque se permitirá el inicio de cualquier aplicación desde la carpeta especificada. Se recomienda aplicar reglas que utilicen las categorías de aplicaciones con la condición **Carpeta de aplicación** solo a aquellos usuarios para los que se debe permitir la instalación automática de actualizaciones.

Prueba del modo de lista de admitidos

Para garantizar que las reglas de control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas. Cuando está habilitado el modo de prueba, Kaspersky Endpoint Security no bloqueará aplicaciones cuyo inicio no esté permitido por las reglas de Control de aplicaciones, sino que enviará notificaciones sobre su inicio al Servidor de administración.

Al probar el modo de lista de admitidos, se recomienda realizar las siguientes acciones:

1. Determinar el período de pruebas (pudiendo elegir entre varios días a dos meses).
2. Habilitar el modo de prueba para 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. Realice cambios en la configuración del modo de lista de admitidos en función de los resultados de análisis.

   En particular, los resultados le permitirán agregar los archivos ejecutables vinculados a los eventos a una categoría de aplicaciones.

Compatibilidad del modo de lista de admitidos

Después de seleccionar una acción de bloqueo para Control de aplicaciones, se recomienda continuar con el modo de lista de admitidos mediante las siguientes acciones:

- Examine los eventos resultantes de la operación del Control de aplicaciones y los informes sobre ejecuciones bloqueadas para analizar la eficacia del Control de aplicaciones.
- Analice las solicitudes que los usuarios le envíen cuando necesiten obtener acceso a alguna aplicación.
- Para analizar archivos ejecutables desconocidos, compruebe 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 comprobar 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 contra amenazas de correo, Protección contra amenazas web, Detección de comportamiento y Prevención de exploits supervisan flujos de datos que se transmiten mediante protocolos específicos y que pasan por un TCP abierto específico y puertos de UDP en el equipo del usuario. Por ejemplo, el componente Protección contra amenazas de correo analiza la información que se transmite mediante SMTP, mientras que el componente Protección contra amenazas web analiza la información que se transmite mediante HTTP y FTP.

Kaspersky Endpoint Security divide los puertos TCP y UDP del equipo en distintos grupos, tomando como criterio la probabilidad de que se vean vulnerados. 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 utiliza servicios que no son estándar que utilizan puertos de red no estándar, estos puertos también pueden convertirse en el blanco del ataque de otros equipos. Puede especificar una lista de los puertos de red y una de las aplicaciones que requieren acceso a la red. Luego, estos puertos y aplicaciones reciben atención especial de los componentes Protección contra amenazas de correo y Protección contra amenazas web durante la supervisión del tráfico de red.

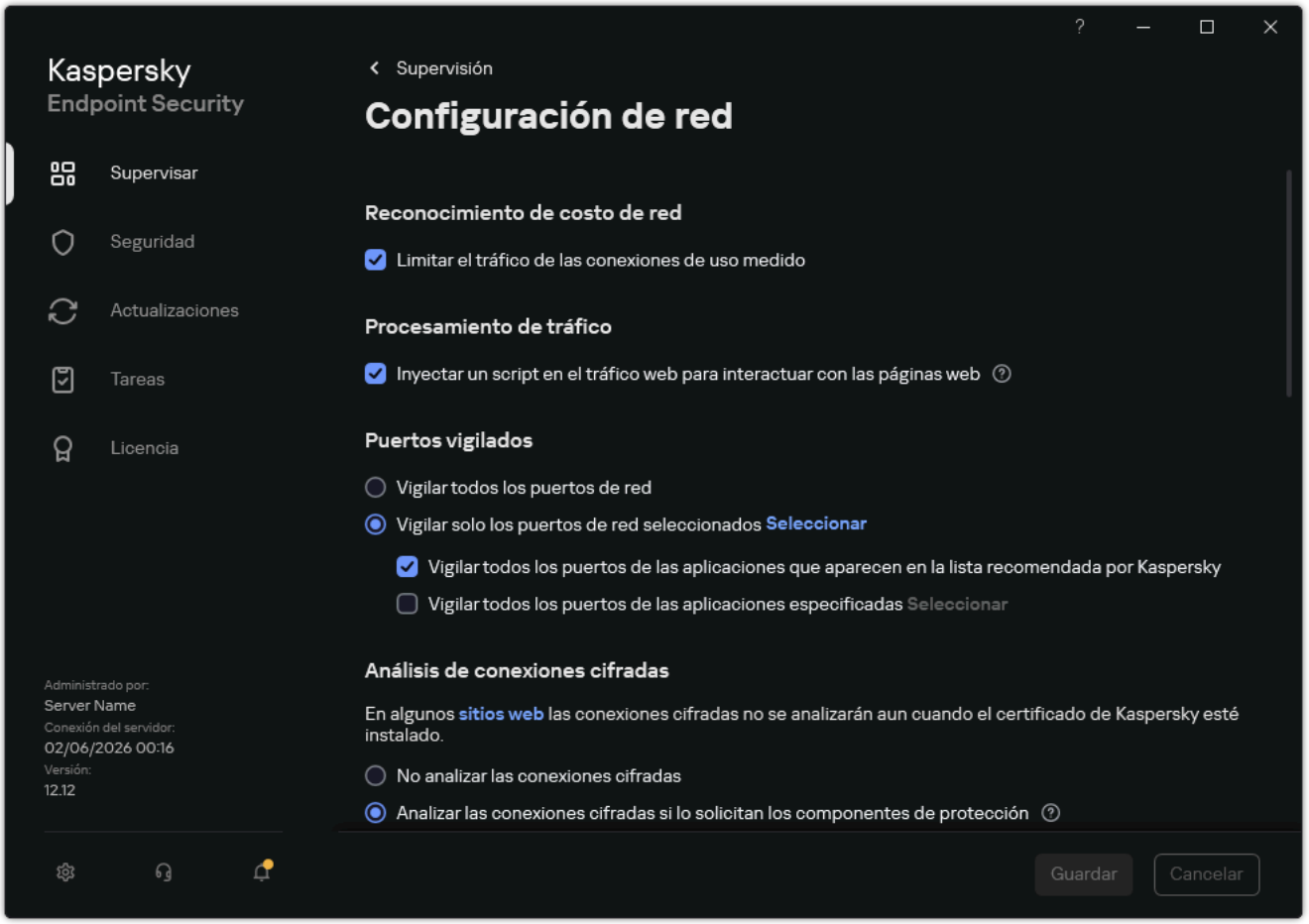
Para poder garantizar la seguridad del equipo, los componentes Detección de comportamiento y Prevención de exploits también supervisan los flujos de datos que pasan a través de los puertos de red. Estos componentes supervisan el tráfico de red de forma continua en busca de procesos independientes que puedan ser peligrosos.

Habilitación de la supervisión de todos los puertos de red

Para habilitar la supervisión de todos los puertos de red:

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

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



Configuración de 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

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de puertos de red supervisados. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Para crear una lista de puertos de red supervisados:

1. En la ventana principal de la aplicación 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 abre una lista de puertos de red que se usan normalmente para la transmisión de mensajes de correo electrónico y tráfico de red. Esta lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
5. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la supervisión del puerto de red.
6. Si no se muestra un puerto de red en la lista de puertos de red, agréguelo haciendo lo siguiente:

   a. Haga clic en **Agregar**.

   b. En la ventana que se abre, ingrese 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 se ejecuta el protocolo FTP en el modo pasivo, se puede establecer la conexión mediante un puerto de red aleatorio que no esté agregado a la lista de puertos de red supervisados. Para proteger tales conexiones, habilite el monitoreo 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 supervisarán todos los puertos de red

Puede crear una lista de las aplicaciones para las que Kaspersky Endpoint Security deba supervisar todos los puertos de red.

> Recomendamos que se incluyan las aplicaciones que envían o transmiten datos mediante el protocolo FTP en la lista de las aplicaciones para las que Kaspersky Endpoint Security deba supervisar todos los puertos de red.

Para crear una lista de aplicaciones para las que se supervisarán todos los puertos de red, realice lo siguiente:

1. En la ventana principal de la aplicación 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 de verificación **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 de 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 de verificación **Vigilar todos los puertos de las aplicaciones especificadas**.

6. Haga clic en **Seleccionar**.

   Esto abre una lista de las aplicaciones para las que Kaspersky Endpoint Security debe supervisar los puertos de red.

7. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la supervisión del puerto de red.

8. Si una aplicación no está incluida en la lista de aplicaciones, agréguela del siguiente modo:

   a. Haga clic en **Agregar**.

   b. En la ventana que se abre, ingrese la ruta al archivo ejecutable de la aplicación y una breve descripción.

   c. Configure el estado **Activo** o **Inactivo** para la supervisión de puertos de red.

9. Guarde los cambios.

Exportar e importar listas de puertos supervisados

Kaspersky Endpoint Security utiliza las siguientes listas para supervisar los puertos de red: lista de puertos de red y lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security. Puede exportar listas de puertos supervisados a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 supervisados o para migrar las listas a otro servidor.

Cómo exportar e importar listas de puertos supervisados a 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 ficha **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 vínculo de las **seleccionados N puertos**.

      Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos de red que se usan normalmente para la transmisión de mensajes de correo y tráfico de red. Esta 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 en el que se guardará la lista de puertos de red. Seleccione también la carpeta en la que se guardará este archivo.

f. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de puertos de red completa al archivo XML.

6. Para exportar la lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security:

a. En el bloque **Puertos vigilados**, seleccione la casilla **Vigilar todos los puertos de las aplicaciones especificadas**.

b. Haga clic en el vínculo de las **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, escriba el nombre del archivo XML en el que se guardará la lista de aplicaciones exportada. Seleccione también la carpeta en la que se guardará este archivo.

f. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de aplicaciones completa 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 que se usará para importar la lista de puertos de red.

b. Abra el archivo.

Cuando ya exista una lista de puertos de red en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

8. Para importar una lista de aplicaciones cuyos puertos supervisa 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 que se usará para importar la lista de aplicaciones.

b. Abra el archivo.

Cuando ya exista una lista de aplicaciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 correspondiente 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 de red que se usan normalmente para la transmisión de mensajes de correo y tráfico de red. Esta 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 en el que se guardará la lista de puertos de red. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de puertos de red completa al archivo XML.

7. Para exportar la lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security:

   a. Seleccione la casilla de verificación **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, escriba el nombre del archivo XML en el que se guardará la lista de aplicaciones exportada. Seleccione también la carpeta en la que se guardará este archivo.

   e. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de aplicaciones completa 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 que se usará para importar la lista de puertos de red.

   b. Abra el archivo.

      Cuando ya exista una lista de puertos de red en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

9. Para importar una lista de aplicaciones cuyos puertos supervisa 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 que se usará para importar la lista de aplicaciones.

   b. Abra el archivo.

      Cuando ya exista una lista de aplicaciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

10. Guarde los cambios.

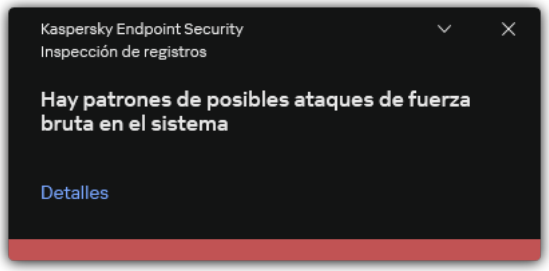
Inspección de registros

Para que pueda usar este componente, Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores. El componente no estará disponible si Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo.

A partir de la versión 11.11.0, Kaspersky Endpoint Security para Windows incluye el componente de Inspección de registros. Inspección de registro monitorea la integridad del entorno protegido en función del análisis del registro de eventos de Windows. Cuando la aplicación detecta indicios de un comportamiento atípico en el sistema, informa al administrador, ya que este comportamiento puede indicar un intento de ciberataque.

Kaspersky Endpoint Security analiza los registros de eventos de Windows y detecta las infracciones de acuerdo con las reglas. El componente incluye reglas predefinidas. Las reglas predefinidas funcionan con análisis heurístico. También puede agregar sus propias reglas (reglas personalizadas). Cuando se activa una regla, la aplicación crea un evento con el estado *Crítico* (consulte la imagen a continuación).

Si desea utilizar Inspección de registros, asegúrese de que la seguridad de la directiva de auditoría esté configurada y que el sistema registre los eventos relevantes (para obtener información, consulte el sitio web de Soporte técnico de Microsoft).



Notificación de Inspección de registro

Configuración de reglas predefinidas

Las reglas predefinidas incluyen plantillas de actividad anormal en el equipo protegido. La actividad anormal puede implicar un intento de ataque. Las reglas predefinidas funcionan con análisis heurístico. Inspección de registro tiene siete reglas predefinidas disponibles. Puede habilitarlas o deshabilitarlas. Las reglas predefinidas no se pueden eliminar.

Puede configurar los criterios de activación de las reglas que monitorean eventos para las siguientes operaciones:

- Detección de ataques de fuerza bruta a contraseñas
- Detección de inicios de sesión en la 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 correspondiente 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. Para configurar reglas predefinidas, seleccione o anule la selección de las casillas de verificación:
   - **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
   - **Se detectó una actividad inusual durante un inicio de sesión en la red**.
   - **Hay patrones de un posible abuso del Registro de eventos de Windows**.
   - **Se detectaron acciones atípicas de parte de un nuevo servicio instalado**.
   - **Se detectó un inicio de sesión atípico que usa credenciales explícitas**.
   - **Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema**.
   - **Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios**.
7. Si es necesario, configure la regla **Hay patrones de posibles ataques 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 período en el cual se deben realizar los intentos para ingresar una contraseña a fin de que se active la regla.
   c. Haga clic en **Aceptar**.
8. Si seleccionó la regla **Se detectó una actividad inusual durante un inicio de sesión en la red**, deberá configurarla:
   a. Haga clic en el botón **Configuración** debajo de la regla.
   b. En el bloque **Detección de inicios de sesión en la red**, especifique el inicio y el final del intervalo de tiempo.

      Kaspersky Endpoint Security considera los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

      De manera predeterminada, el intervalo no se establece, y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise continuamente los intentos de inicio de sesión, establezca el intervalo entre las 12:00 a. m. y las 11:59 p. m. El inicio y el final del intervalo no deben coincidir. Si coinciden, 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 en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.
Kaspersky Endpoint Security no monitorea los intentos de inicio de sesión de estos usuarios y equipos.

d. Haga clic en **Aceptar**.

9. Guarde los cambios.

Cómo configurar reglas predefinidas con 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Inspección de registros**.

5. Asegúrese de que el interruptor **Inspección de registros HABILITADA** esté activado.

6. En el bloque **Reglas predefinidas**, habilite o deshabilite las reglas predefinidas usando los interruptores:

- **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
- **Se detectó una actividad inusual durante un inicio de sesión en la red**.
- **Hay patrones de un posible abuso del Registro de eventos de Windows**.
- **Se detectaron acciones atípicas de parte de un nuevo servicio instalado**.
- **Se detectó un inicio de sesión atípico que usa credenciales explícitas**.
- **Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema**.

a. **Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios**.

7. Si es necesario, configure la regla **Hay patrones de posibles ataques 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 período en el cual se deben realizar los intentos para ingresar una contraseña a fin de que se active la regla.

c. Haga clic en **Aceptar**.

8. Si seleccionó la regla **Se detectó una actividad inusual durante un inicio de sesión en la red**, deberá configurarla:

a. Haga clic en **Configuración** debajo de la regla.

b. En el bloque **Detección de inicios de sesión en la red**, especifique el inicio y el final del intervalo de tiempo.

Kaspersky Endpoint Security considera los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

De manera predeterminada, el intervalo no se establece, y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise continuamente los intentos de inicio de sesión, establezca el intervalo entre las 12:00 a. m. y las 11:59 p. m. El inicio y el final del intervalo no deben coincidir. Si coinciden, la aplicación no supervisa los intentos de inicio de sesión.

c. En el bloque **Exclusiones**, agregue los usuarios de confianza y las direcciones IP de confianza (IPv4 e IPv6).

Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.
Kaspersky Endpoint Security no monitorea los intentos de inicio de sesión de 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 principal de la aplicación 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. Para configurar reglas predefinidas, seleccione o anule la selección de las casillas de verificación:

- **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
- **Se detectó una actividad inusual durante un inicio de sesión en la red**.
- **Hay patrones de un posible abuso del Registro de eventos de Windows**.
- **Se detectaron acciones atípicas de parte de un nuevo servicio instalado**.
- **Se detectó un inicio de sesión atípico que usa credenciales explícitas**.
- **Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema**.

a. **Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios**.

6. Si es necesario, configure la regla **Hay patrones de posibles ataques 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 período en el cual se deben realizar los intentos para ingresar una contraseña a fin de que se active la regla.

7. Si seleccionó la regla **Se detectó una actividad inusual durante un inicio de sesión en la red**, deberá configurarla:

   a. Haga clic en **Configuración** debajo de la regla.

   b. En el bloque **Detección de inicio de sesión en la red**, especifique el inicio y el final del intervalo de tiempo.

      Kaspersky Endpoint Security considera los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

      De manera predeterminada, el intervalo no se establece, y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise continuamente los intentos de inicio de sesión, establezca el intervalo entre las 12:00 a. m. y las 11:59 p. m. El inicio y el final del intervalo no deben coincidir. Si coinciden, la aplicación no supervisa los intentos de inicio de sesión.

   c. En el bloque **Exclusiones**, agregue los usuarios de confianza y las direcciones IP de confianza (IPv4 e IPv6).

      Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.
      Kaspersky Endpoint Security no monitorea los intentos de inicio de sesión de estos usuarios y equipos.

8. Guarde los cambios.

Como consecuencia, cuando se activa la regla, Kaspersky Endpoint Security crea un evento *Evento crítico*.

Agregar reglas personalizadas

Puede establecer sus propios criterios de activación de las reglas de Inspección de registro. Para hacerlo, debe ingresar un ID de evento y seleccionar una fuente de evento. Puede buscar el ID del evento en el sitio web de soporte técnico de Microsoft. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*. También puede especificar el registro de una aplicación de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de *Windows PowerShell*).

> La aplicación no comprueba si el registro especificado está realmente presente en el Registro de eventos de Windows. Si hay un error en el nombre del registro, la aplicación no monitorea los eventos de ese registro.

La lista de reglas personalizadas ya incluye tres reglas que crearon expertos de Kaspersky.

Cómo agregar una regla personalizada 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 correspondiente 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 de verificación junto a las reglas personalizadas que desea habilitar.

7. Si es necesario, haga clic en **Agregar** para crear sus reglas personalizadas.

8. Esto abre una ventana, donde debe configurar la regla personalizada:

   - **Nombre de la regla**.
   - **Nombre del registro**. Registros de eventos de Windows. Estos son los registros disponibles: *Application*, *Security*, *System*.
   - **Fuente**. Registros de aplicaciones de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de *Windows PowerShell*).
   - **Identificadores de eventos**. ID de eventos en el Registro de eventos de Windows. Puede buscar el ID del evento en la documentación técnica de Microsoft.

9. Guarde los cambios.

Cómo agregar una regla personalizada 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Inspección de registros**.

5. Asegúrese de que el interruptor **Inspección de registros HABILITADA** esté activado.

6. En el bloque **Reglas personalizadas**, seleccione las reglas personalizadas que desea habilitar.

7. Si es necesario, haga clic en **Agregar** para crear sus reglas personalizadas.

8. Esto abre una ventana, donde debe configurar la regla personalizada:

   - **Nombre de la regla**.
   - **Nombre de registro personalizado**. Registros de eventos de Windows. Estos son los registros disponibles: *Application*, *Security*, *System*.
   - **Origen**. Registros de aplicaciones de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de *Windows PowerShell*).
   - **Identificadores de eventos**. ID de eventos en el Registro de eventos de Windows. Puede buscar el ID del evento en la documentación técnica de Microsoft.

9. Guarde los cambios.

Cómo agregar una regla personalizada mediante la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 de verificación junto a las reglas personalizadas que desea habilitar.

6. Si es necesario, haga clic en **Agregar** para crear sus reglas personalizadas.

7. Esto abre una ventana, donde debe configurar la regla personalizada:

   - **Nombre de la regla**.

   - **Nombre del registro**. Registros de eventos de Windows. Estos son los registros disponibles: *Application*, *Security*, *System*.

   - **Fuente**. Registros de aplicaciones de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de *Windows PowerShell*).

   - **Identificador de eventos**. ID de eventos en el Registro de eventos de Windows. Puede buscar el ID 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

Para que pueda usar este componente, Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores. El componente no estará disponible si Kaspersky Endpoint Security debe estar instalado 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 del registro y la conexión de los dispositivos externos.

El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que podrían indicar filtraciones de seguridad en el equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos y las alertas correspondientes, y las envía al administrador. Control de integridad del sistema puede operar en tiempo real y también puede realizar controles de integridad del sistema a pedido.

Control de integridad del sistema en tiempo real

En el modo de tiempo real, Control de integridad del sistema realiza un seguimiento de los cambios en los objetos que incluyó en el alcance del componente (el *alcance del monitoreo*). Además, Control de integridad del sistema permite bloquear el acceso no autorizado a dichos objetos en tiempo real.

Comprobación de integridad del sistema a pedido

Comprobación de integridad del sistema a pedido es una tarea que se puede ejecutar manualmente o según una programación. Para ejecutar la tarea *Comprobación de integridad del sistema*, debe configurar el alcance del componente (el *alcance del monitoreo*) y crear una línea de base. Una *línea de base* es un estado registrado de los objetos en el sistema que la aplicación usa como referencia cuando se compara con el estado actual.

Migración de la configuración de Monitor de integridad de archivos

Cuando se actualiza Kaspersky Endpoint Security a la versión 12.6, la configuración de Monitor de integridad de archivos se migra automáticamente. Como parte de la migración, la aplicación mueve las reglas de monitoreo a Control de integridad del sistema. Las reglas de Monitor de integridad de archivos también se migran a Control de integridad del sistema cuando migra de KSWS a KES.

Para garantizar el correcto funcionamiento de 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 Control de integridad del sistema porque el complemento de administración no cuenta con la sección **Control de integridad del sistema**.

Acerca de las reglas de Control de integridad del sistema

Para que funcione Control de integridad del sistema, debe agregar 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. Control de integridad del sistema detecta cambios en los archivos y el registro dentro del *alcance del monitoreo* especificado. El alcance del monitoreo es uno de los criterios de una regla de Control de integridad del sistema.

Control de integridad del sistema permite supervisar los siguientes objetos:

- Archivos
- Registro
- Dispositivos externos

Consideraciones especiales involucradas en la supervisión de archivos

Control de integridad del sistema supervisa los cambios en los archivos y las carpetas, así como los archivos que se agregan al alcance del monitoreo o se eliminan de él. Estos cambios pueden indicar una filtración de seguridad informática. Recomendamos agregar objetos que rara vez se modifican u objetos a los que solo tiene acceso el administrador. Esto ayuda a reducir la cantidad de eventos de 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 usar localmente.

Kaspersky Endpoint Security supervisa los cambios de archivos y carpetas solo en aquellos discos que estaban conectados cuando comenzó a funcionar Control de integridad del sistema en tiempo real. Si un disco no estaba conectado cuando comenzó a funcionar Control de integridad del sistema en tiempo real, la aplicación no supervisa los cambios de archivos y carpetas en ese disco, incluso si los archivos y las carpetas se agregan al alcance del monitoreo.

Consideraciones especiales involucradas en la supervisión del registro

Control de integridad del sistema supervisa el registro. Estos cambios pueden indicar una filtración de seguridad informática.

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` (solo disponible en el Control de integridad del sistema en tiempo real)
- `HKEY_CURRENT_USER` (solo disponible en el Control de integridad del sistema en tiempo real)

> La tarea *Comprobación de integridad del sistema* no admite la clave `HKEY_CURRENT_USER`. Puede especificar una clave en `HKEY_USERS` como `HKEY_USERS\<user profile ID>\<key>`.

Consideraciones especiales involucradas en la supervisión de dispositivos externos

Control de integridad del sistema supervisa la conexión y desconexión de dispositivos externos. Esto es necesario para proteger el equipo de las amenazas de seguridad que pueden resultar del intercambio de archivos con dichos dispositivos. 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 utilizando un componente diferente de la aplicación, Control de dispositivos.

> Al ejecutar la tarea *Monitor comparativo de integridad del sistema*, la aplicación ignora la reconexión de dispositivos externos si los dispositivos tienen la misma letra de unidad en el sistema operativo. Para que se registren, los dispositivos reconectados deben tener distintas letras de unidad.

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 o cámara

Control de integridad del sistema en tiempo real

Control de integridad del sistema permite realizar un seguimiento de los cambios del sistema operativo en tiempo real. Puede realizar un seguimiento de cambios que pueden indicar filtraciones de seguridad en el equipo. El componente permite bloquear estos cambios o simplemente registrar eventos de cambio.

Para que funcione Control de integridad del sistema, debe agregar 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. Control de integridad del sistema detecta cambios en los archivos y el registro dentro del *alcance del monitoreo* especificado. El alcance del monitoreo es uno de los criterios de una regla de 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 acciones con recursos que sean críticos para el funcionamiento del sistema operativo u otros servicios, recomendamos habilitar el modo de prueba y analizar cómo afecta el componente al sistema. 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 de *Advertencia* ⚠.

El componente de Control de integridad del sistema en tiempo real tiene dos modos:

- Bloquear

  En este modo, Control de integridad del sistema rastrea los cambios del sistema y realiza una acción de acuerdo con las reglas: **Permitir** o **Bloquear**. 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, Control de integridad del sistema permite las acciones con archivos y claves del registro del alcance del monitoreo. Si la acción con los archivos o el registro está prohibida, la aplicación genera un evento: *Se permitió la operación prohibida en modo de prueba*. Para analizar cómo afectan las reglas al sistema, puede consultar los informes.

Habilitación de Control de integridad del sistema en tiempo real

Cómo habilitar 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 correspondiente 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 de verificación **Control de integridad del sistema**.
5. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para Control de integridad del sistema en tiempo real:
   - **Bloquear**. En este modo, Control de integridad del sistema bloquea las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.
   - **Informar**. En este modo, Control de integridad del sistema permite las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.
6. En el bloque **Control de integridad del sistema en tiempo real**, seleccione la casilla **Control de integridad del sistema en tiempo real**.

7. Configure la supervisión de dispositivos externos:

   a. Seleccione la casilla de verificación **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativos* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

   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 habilita en la configuración de la aplicación. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente.

8. Configure la supervisión de los archivos y el registro de la siguiente manera:

   a. Seleccione la casilla de verificación **Supervisar archivos y el registro**.

   b. Haga clic en **Configuración**.

   Se abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Agregar**.

   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 íconos de candado y guarde los cambios.

Cómo habilitar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de integridad del sistema**.

5. Active el interruptor de **Control de integridad del sistema HABILITADO**.

6. Seleccione la ficha **Windows**.

7. En **Control de integridad del sistema en tiempo real**, seleccione un modo para Control de integridad del sistema en tiempo real:

   - **Aplicar reglas**. En este modo, Control de integridad del sistema bloquea las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.

   - **Reglas de prueba (informar)**. En este modo, Control de integridad del sistema permite las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.

8. Configure la supervisión de los archivos y el registro de la siguiente manera:

   a. Seleccione la casilla de verificación **Supervisar archivos y el registro**.

   b. Haga clic en **Reglas**.

      Se abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Agregar**.

      También puede importar reglas de otra fuente.

   d. Configure la regla de Control de integridad del sistema (consulte la tabla a continuación).

9. Configure la supervisión de dispositivos externos:

   a. Seleccione la casilla de verificación **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia*, *Crítico*.

   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 habilita 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 íconos de candado y guarde los cambios.

Cómo habilitar Control de integridad del sistema en tiempo real en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 de **Control de integridad del sistema**.

4. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para Control de integridad del sistema en tiempo real:

   - **Bloquear**. En este modo, Control de integridad del sistema bloquea las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.

   - **Informar**. En este modo, Control de integridad del sistema permite las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.

5. En el bloque **Control de integridad del sistema en tiempo real**, seleccione la casilla **Control de integridad del sistema en tiempo real**.

6. Configure la supervisión de dispositivos externos:

   a. Seleccione la casilla de verificación **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia*, *Crítico*.

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 habilita en la configuración de la aplicación. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente.

7. Configure la supervisión de los archivos y el registro de la siguiente manera:

   a. Seleccione la casilla de verificación **Supervisar archivos y el registro**.

   b. Haga clic en **Configurar**.

      Se abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Agregar**.

      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 la regla 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 registros	• **Permitir**. Control de integridad del sistema permite realizar acciones con archivos y claves del registro del alcance de la supervisión. • **Bloquear**. El comportamiento de Control de integridad del sistema depende del modo seleccionado. Si seleccionó el *Modo de protección del sistema*, Control de integridad del sistema bloquea las acciones con archivos y claves del registro del alcance del monitoreo, genera un evento correspondiente y cambia el estado del dispositivo en la consola de Kaspersky Security Center. Si seleccionó el *Modo de prueba*, Control de integridad del sistema permite las acciones con archivos y claves del registro del alcance del monitoreo.

Parámetro	Descripción
Nivel de gravedad del evento	Kaspersky Endpoint Security registra eventos de modificación de archivos cada vez que se cambia un archivo o una clave del registro del alcance del monitoreo. Los siguientes niveles de gravedad de eventos están disponibles: *Informativo*, *Advertencia* o *Crítico*.

Alcance del monitoreo	• **Archivo**. Lista de archivos y carpetas supervisados por el componente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
	Usar máscaras:
	  • El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 del registro y valores supervisados por el componente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara.

Exclusiones	• **Archivo**. Lista de exclusiones del alcance del monitoreo. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara. Por ejemplo, `C:\Folder\Application\*.log`. Las entradas de exclusión tienen una prioridad más alta que las entradas del alcance del monitoreo.
	Usar máscaras:
	  • El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 del alcance del monitoreo. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara. Las entradas de exclusión tienen una prioridad más alta que las entradas del alcance del monitoreo.

Grupos de usuarios o usuarios de confianza	Un *usuario de confianza* es un usuario al que se le permite realizar acciones con los archivos y las claves del registro en el alcance del monitoreo. Si Kaspersky Endpoint Security detecta una acción realizada por un usuario de confianza, Control de integridad del sistema genera un evento *Informativo*. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.
Marcadores de las operaciones sobre archivos/Operaciones supervisadas	Marcadores que describen la acción con los archivos o las claves del registro que supervisará la aplicación.
Ejecución de hash	Cálculo de un hash de archivo ante operaciones de modificación. Kaspersky Endpoint Security agrega información sobre el hash del archivo cuando se genera un evento.

Comprobación de integridad del sistema a pedido

Comprobación de integridad del sistema a pedido es una tarea que se puede ejecutar manualmente o según una programación. Cuando se ejecuta la tarea *Comprobación de integridad del sistema*, la aplicación compara el estado actual de los objetos incluidos en el alcance del monitoreo con el estado de su *línea de base*. A diferencia de Control de integridad del sistema en tiempo real, la tarea *Comprobación de integridad del sistema* ayuda a limitar la cantidad de eventos y le permite generar un informe general de los cambios en el sistema operativo.

Para que funcione Control de integridad del sistema, debe agregar 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. Control de integridad del sistema detecta cambios en los archivos y el registro dentro del *alcance del monitoreo* especificado. El alcance del monitoreo es uno de los criterios de una regla de Control de integridad del sistema. Puede configurar reglas para que Control de integridad del sistema en tiempo real y la tarea *Comprobación de integridad del sistema* las compartan o puede crear reglas separadas para la tarea. Para crear una línea de base, Kaspersky Endpoint Security aplica el alcance del monitoreo de la tarea *Comprobación de integridad del sistema* a la tarea *Actualización básica*.

Creación y actualización de una línea de base

La tarea *Comprobación de 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 usa como referencia cuando se compara 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 con la tarea *Actualización básica*.

Puede actualizar la línea de base de los siguientes modos:

- Actualización completa.

  La aplicación actualiza todos los objetos que se encuentran en el alcance del monitoreo.

- Actualización gradual.

  La aplicación detecta y actualiza solo los 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Actualización básica**.

Paso 2. Selección del modo de actualización básica

Seleccione un modo de actualización básica:

- **Actualización completa**. La aplicación actualiza todos los objetos que se encuentran en el alcance del monitoreo.
- **Actualización gradual**. La aplicación detecta y actualiza solo los objetos nuevos o modificados.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Nombre de la tarea

Ingrese el nombre de la tarea, por ejemplo *Línea de base 2024*.

Paso 5. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo crear o actualizar una línea de base en Web Console

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Actualización básica**.

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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del Asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. Seleccione un modo de actualización básica:

   - **Actualización completa**. La aplicación actualiza todos los objetos que se encuentran en el alcance del monitoreo.

   - **Actualización gradual**. La aplicación detecta y actualiza solo los objetos nuevos o modificados.

10. Guarde los cambios.

11. Active la casilla ubicada junto a la tarea.

12. Haga clic en **Iniciar**.

Configuración del alcance del monitoreo para la tarea Comprobación de integridad del sistema

De manera predeterminada, el alcance de supervisión de la tarea *Comprobación de integridad del sistema* es el mismo que el alcance de supervisión de Control de integridad del sistema en tiempo real. Puede configurar un alcance del monitoreo diferente para la tarea.

> Control de integridad del sistema no admite la importación de las claves `HKEY_CURRENT_USER` ni `HKEY_CURRENT_CONFIG` para la tarea *Comprobación de integridad del sistema*. Si el alcance del control de la tarea contiene estas claves, la aplicación genera el evento *El alcance del monitoreo incluye objetos incorrectos*.

Cómo configurar un alcance del monitoreo diferente para la tarea Comprobación 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 correspondiente 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 de verificación **Control de integridad del sistema**.

5. En **Comprobación de integridad del sistema**, seleccione el modo de configuración de la tarea: **Preferencias de configuración**.

6. Configure la supervisión de dispositivos externos:

   a. Seleccione la casilla de verificación **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativos* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

   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. Cuando se ejecuta la tarea *Comprobación de integridad del sistema*, la aplicación no supervisa la desconexión de los dispositivos externos.

7. Configure la supervisión de los archivos y el registro de la siguiente manera:

   a. Seleccione la casilla de verificación **Supervisar archivos y el registro**.

   b. Haga clic en **Configuración**.

      Se abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Agregar**.

      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 alcance del monitoreo diferente para la tarea Comprobación 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de integridad del sistema**.

5. Seleccione la ficha **Windows**.

6. Active el interruptor de **Control de integridad del sistema HABILITADO**.

7. En **Comprobación de integridad del sistema**, seleccione el modo de configuración de la tarea: **Preferencias de configuración**.

8. Configure la supervisión de dispositivos externos:

   a. Seleccione la casilla de verificación **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

   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. Cuando se ejecuta la tarea *Comprobación de integridad del sistema*, la aplicación no supervisa la desconexión de los dispositivos externos.

9. Configure la supervisión de los archivos y el registro de la siguiente manera:

   a. Seleccione la casilla de verificación **Supervisar archivos y el registro**.

   b. Haga clic en **Reglas**.

      Se abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Agregar**.

      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 alcance del monitoreo diferente para la tarea Comprobación de integridad del sistema en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 de **Control de integridad del sistema**.

4. En **Comprobación de integridad del sistema**, seleccione el modo de configuración de la tarea: **Configuración personalizada**.

5. Configure la supervisión de dispositivos externos:

   a. Seleccione la casilla de verificación **Supervisar dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo* ⓘ, *Advertencia* ⚠, *Crítico* ⓘ.

   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. Cuando se ejecuta la tarea *Comprobación de integridad del sistema*, la aplicación no supervisa la desconexión de los dispositivos externos.

6. Configure la supervisión de los archivos y el registro de la siguiente manera:

   a. Seleccione la casilla de verificación **Supervisar archivos y el registro**.

   b. Haga clic en **Configurar**.

      Se abre la lista de reglas de Control de integridad del sistema.

   c. Haga clic en **Agregar**.

      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 integridad del sistema

Parámetro	Descripción
Nombre de la regla	Nombre de la regla de la tarea *Comprobación de integridad del sistema*.
Nivel de gravedad del evento	Kaspersky Endpoint Security registra eventos de modificación de archivos cada vez que se cambia un archivo o una clave del registro del alcance del monitoreo. Los siguientes niveles de gravedad de eventos están disponibles: *Informativo*, *Advertencia* o *Crítico*.

Alcance del monitoreo	• **Archivo**. Lista de archivos y carpetas supervisados por el componente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
	Usar máscaras:
	  • El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 del registro y valores supervisados por el componente. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara.

Exclusiones	• **Archivo**. Lista de exclusiones del alcance del monitoreo. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara. Por ejemplo, `C:\Folder\Application\*.log`. Las entradas de exclusión tienen una prioridad más alta que las entradas del alcance del monitoreo.
	Usar máscaras:
	  • El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
	  • `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 del alcance del monitoreo. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara. Las entradas de exclusión tienen una prioridad más alta que las entradas del alcance del monitoreo.

Ejecución de la tarea Comprobación de integridad del sistema

La tarea *Comprobación de integridad del sistema* permite verificar los archivos o las claves del registro para detectar cambios y también verifica la conexión de los dispositivos externos. Para buscar cambios en los archivos, puede ejecutar la tarea *Comprobación de integridad del sistema* en los siguientes modos:

- Análisis rápido.

  Durante la comprobación de los archivos en busca de cambios, la aplicación solo verifica los atributos de los archivos. La aplicación no verifica el contenido de los archivos.

- Análisis completo.

  Durante la comprobación de los archivos en busca de cambios, la aplicación verifica todos los atributos y el contenido de los archivos.

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 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**.

   Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

4. Seleccione **Kaspersky Endpoint Security** → **Monitor comparativo de integridad del sistema**. Seleccione un modo de Control de integridad del sistema:

   - **Análisis completo**. En este modo, la aplicación verifica todos los atributos y hash de los archivos.

   - **Análisis rápido**. En este modo, la aplicación verifica solo los atributos de los archivos.

5. Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

   - Seleccione los equipos detectados por el Servidor de Administración en la red: dispositivos no asignados. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.

   - Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las 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 manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

7. Programe la ejecución de la tarea. Puede hacer que la tarea se inicie manualmente o en un día específico de la semana.

8. Ingrese un nombre para la tarea.

9. Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo ejecutar una tarea de Comprobación 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Comprobación de integridad del sistema**.

   c. En el campo **Nombre de la tarea**, escriba una breve descripción (por ejemplo, *Comprobación de integridad del sistema semanal*).

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del Asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. Seleccione un modo de Comprobación de integridad del sistema:

   - **Análisis rápido**. La aplicación verifica solo los atributos del archivo. La aplicación no verifica el contenido de los archivos.

   - **Análisis completo**. La aplicación verifica 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 integridad del sistema* se complete correctamente, el alcance del monitoreo de la tarea *Comprobación de integridad del sistema* debe coincidir por completo con la línea de base. Si el alcance del monitoreo es diferente, la tarea finaliza con un error. Para sincronizar los alcances del monitoreo, ejecute la tarea *Actualización básica* con un nuevo alcance del monitoreo.

Exportación e importación de las reglas de Control de integridad del sistema

Puede exportar la lista de reglas de Control de integridad del sistema a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de registros del mismo tipo. Puede utilizar la función de exportación/importación para crear una copia de seguridad de la lista de reglas de Control de integridad del sistema o para migrar la lista a otro servidor.

> Control de integridad del sistema no admite la importación de las claves `HKEY_CURRENT_USER` ni `HKEY_CURRENT_CONFIG` para la tarea *Comprobación de integridad del sistema*. Si el alcance del control de la tarea contiene estas claves, la aplicación genera el evento *El alcance del monitoreo incluye objetos incorrectos*.

Cómo exportar e importar una lista de reglas de Control de integridad del sistema a la Consola de administración (MMC)

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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, haga lo siguiente*:
   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, haga lo siguiente:
      1. Seleccione la regla de acceso que desea 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 vínculo **Exportar**.
      3. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
      4. Guarde el archivo.

         Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.
   c. Para importar una lista de reglas de Control de integridad del sistema en tiempo real, haga lo siguiente:
      1. Haga clic en el vínculo **Importar**.

         En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
      2. Abra el archivo.

         Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

5. Para exportar o importar reglas de *Comprobación de integridad del sistema, haga lo siguiente*:

   a. En el bloque **Comprobación de integridad del sistema**, seleccione **Preferencias de configuración**.

   b. Haga clic en **Configuración**.

   c. Para exportar la lista de reglas de Comprobación de integridad del sistema, haga lo siguiente:

      1. Seleccione la regla de acceso que desea 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 vínculo **Exportar**.

      3. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.

      4. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.

   d. Para importar una lista de reglas de Comprobación de integridad del sistema, haga lo siguiente:

      1. Haga clic en el vínculo **Importar**.

         En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

      2. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 ficha **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** → **Control de integridad del sistema**.

5. Seleccione la ficha **Windows**.

6. Para exportar o importar reglas de *Control de integridad del sistema en tiempo real, haga lo siguiente*:

   a. En el bloque **Control de integridad del sistema en tiempo real**, haga clic en el vínculo **Reglas**.

   b. Para exportar una lista de reglas de Control de integridad del sistema en tiempo real, haga lo siguiente:

      1. Seleccione la regla de acceso que desea 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, haga lo siguiente:

      1. Haga clic en el botón → **Importar**.

         En la ventana que se abre, seleccione el archivo JSON que se usará para importar la lista de direcciones web de confianza.

      2. Abra el archivo.

         Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

7. Para exportar o importar reglas de *Comprobación de integridad del sistema, haga lo siguiente*:

   a. En el bloque **Comprobación de integridad del sistema a pedido**, seleccione **Preferencias de configuración**.

   b. Haga clic en el vínculo **Reglas**.

   c. Para exportar la lista de reglas de Comprobación de integridad del sistema, haga lo siguiente:

      1. Seleccione la regla de acceso que desea 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, haga lo siguiente:

      1. Haga clic en el botón → **Importar**.

         En la ventana que se abre, seleccione el archivo JSON que se usará para importar la lista de direcciones web de confianza.

      2. Abra el archivo.

         Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

8. Guarde los cambios.

Visualización de los 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 básica

  Los informes contienen los eventos de Control de integridad del sistema.
- En la Consola de Kaspersky Security Center:
  - El informe sobre los equipos en los que se activaron las reglas de monitoreo la mayor cantidad de veces
  - El informe sobre las reglas de monitoreo activadas con mayor frecuencia

  De manera predeterminada, se crea un informe para los 30 días anteriores, incluida la fecha en 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 del **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 las instrucciones del Asistente de plantilla de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione el informe Control de integridad del sistema (la sección **Otro**):
     - **Los 10 dispositivos cuyas reglas de Monitor de integridad de archivos / Control de integridad del sistema se desencadenan con mayor frecuencia**.
     - **Las 10 reglas Monitor de integridad de archivos / Control de integridad del sistema que se activaron con mayor frecuencia en los dispositivos**.

     Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la pestaña **Informes**.
  5. Abra el informe haciendo doble clic en él.

  Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

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 **Agregar**.

   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 dispositivos cuyas reglas de Monitor de integridad de archivos / Control de integridad del sistema se desencadenan con mayor frecuencia**.
   - **Las 10 reglas Monitor de integridad de archivos / Control de integridad del sistema que se activaron con mayor frecuencia en los dispositivos**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla.
4. Seleccione y ejecute el informe.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

Para ver los eventos generados por la aplicación, también puede usar las selecciones de eventos de 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*, or *Crítico*. Si Control de integridad del sistema detecta una modificación de los archivos o las claves del registro en el alcance del monitoreo, el estado del equipo cambia a *Advertencia* o *Crítico*. El estado asignado por 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 lo convenció de que la modificación detectada de objetos 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Programación de la tarea

Configure la programación de la tarea, por ejemplo, manualmente.

Paso 4. Nombre de la tarea

Escriba el nombre de la tarea, por ejemplo, *Restablecimiento del estado después de modificar el alcance del monitoreo*.

Paso 5. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Restablecimiento del estado de integridad del sistema**.

c. En el campo **Nombre de la tarea**, ingrese una breve descripción, por ejemplo, *Restablecimiento del estado después de modificar el alcance del monitoreo*.

d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Endpoint Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Salga del 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 *OK*. 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, Microsoft Office 365. Los servicios en la nube se agrupan en categorías, por ejemplo, *Uso compartido de archivos*, *Mensajería*, *Correo electrónico*. Los expertos de Kaspersky actualizan con regularidad 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 utiliza Kaspersky Security Network para categorizar los servicios en la nube.

Cloud Discovery proporciona las siguientes características:

- 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 se instala en un equipo que ejecuta 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. **Inyectar un script en el tráfico web para interactuar con las páginas web**. El script permite registrar eventos de Cloud Discovery. El script también brinda un bloqueo completo del acceso a los servicios en la nube. Sin el script, la aplicación solo bloquea el acceso según los dominios de servicios en la nube. Puede administrar esta funcionalidad en la sección **Configuración de red**.

También puede habilitar 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. Así, cuando un usuario usa un servicio en la nube, Cloud Discovery registra solo un evento, en lugar de varios eventos para 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 ese evento y crea una entrada en el informe. Cloud Discovery controla el uso de los servicios en la nube en el navegador, así como en las aplicaciones correspondientes. Cloud Discovery controla el uso de los servicios en la nube a través de HTTP y HTTPS.

Cómo habilitar el análisis 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 ficha **Configuración de la aplicación**.

4. Vaya a **Comunicación y Protección web** → **Cloud Discovery**.

5. Active el interruptor de **Cloud Discovery HABILITADO**.

6. Guarde los cambios.

Como resultado, la aplicación reenvía la información acerca de los servicios en la nube utilizados a Kaspersky Security Center. Puede ver la información acerca del uso de los servicios en la nube en informes. Si es necesario, puede bloquear el acceso a servicios en la nube.

Bloquear el acceso a los servicios en la nube

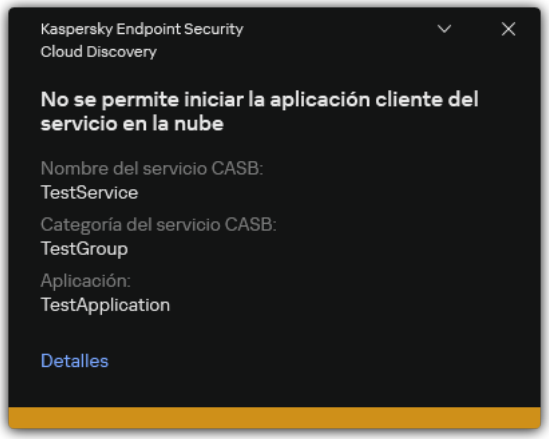
El bloqueo de acceso a servicios en la nube está disponible únicamente para la licencia de Kaspersky Next EDR Optimum y XDR Expert. Esta funcionalidad no está disponible para la licencia de Kaspersky Next EDR Foundations. Para ver una comparación de las funcionalidades de la aplicación según el tipo de licencia de Kaspersky Next, consulte Ayuda de Kaspersky Next.

El administrador puede restringir el acceso de los usuarios a las categorías de Cloud Discovery o a servicios en la nube individuales. De esta manera, el administrador puede permitir solo servicios en la nube seguros y evitar filtraciones de datos. Se muestra *información acerca del nivel de riesgo* para cada servicio en la nube de Cloud Discovery. El nivel de riesgo permite detectar servicios que no satisfacen los requisitos de seguridad de la organización.

El nivel de riesgo es un cálculo y no implica afirmaciones acerca de la calidad del servicio en la nube o de su proveedor. El nivel de riesgo es meramente una recomendación de los expertos de Kaspersky.

Los niveles de riesgo de los servicios en la nube se muestran en la sección **Cloud Discovery** de la directiva en la lista de todos los servicios en la nube controlados.

Otros componentes de Kaspersky Endpoint Security brindan protección contra amenazas y seguimiento de actividades sospechosas de los usuarios cuando utilizan los servicios en la nube.



Notificación de Cloud Discovery

Cloud Discovery no bloquea las aplicaciones en la nube que se iniciaron antes de 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 ficha **Configuración de la aplicación**.
4. Vaya a **Comunicación y Protección web** → **Cloud Discovery**.
5. Active el interruptor de **Cloud Discovery HABILITADO**.

   Se muestra una lista de todos los servicios en la nube. Los servicios en la nube se agrupan en categorías, por ejemplo, *Uso compartido de archivos*, *Servicios de mensajería instantánea* y *Correo electrónico*. Los expertos de Kaspersky actualizan con regularidad 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. Utilice el conmutador del interruptor en la columna **Acceso** para configurar el acceso a los servicios en la nube.

7. Guarde los cambios.

Como resultado, la aplicación controla el uso de los servicios 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 configurados por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza independientemente, teniendo en cuenta las características de los objetos manejados y las aplicaciones instaladas en el equipo. Puede ser necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a un objeto o una aplicación determinados, si está seguro de que dicho objeto o aplicación no suponen peligro alguno. 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 agregar telemetría EDR a la zona de confianza. Esto permite optimizar los datos que la aplicación envía al servidor de recopilación de 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 aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 el modo de Light Agent para proteger entornos virtuales. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de Citrix y VMware.

Cómo crear una exclusión de análisis

Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas. A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre el software legal que los intrusos pueden utilizar para dañar su equipo o datos personales están disponibles en el sitio web de la Enciclopedia TI de Kaspersky.

Kaspersky Endpoint Security puede bloquear estas aplicaciones. Para prevenir que se bloqueen, puede configurar la exclusión del análisis para las aplicaciones en uso. Busque para ello el nombre (o la máscara de nombre) pertinente en la Enciclopedia de Kaspersky y agréguelo a la zona de confianza. Por ejemplo, a menudo utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security considera esta actividad como sospechosa y puede bloquearla. Para evitar que la aplicación se bloquee, cree una exclusión de análisis con el nombre o la máscara de nombre que se indiquen en la Enciclopedia de Kaspersky.

Si una aplicación que recopila información y la envía para su proceso se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis si configura Kaspersky Endpoint Security tal como se describe en este documento.

Las exclusiones de análisis pueden ser utilizadas por los siguientes componentes de las aplicaciones y tareas que configuró el administrador del sistema:

- Detección de comportamiento
- Prevención de exploits
- Prevención de intrusiones en el host
- Protección contra amenazas de archivo
- Protección contra amenazas web
- Protección contra amenazas de correo
- Tarea de *Análisis de malware*

Kaspersky Endpoint Security no analiza un objeto si la unidad o la carpeta que lo contiene está incluida en el alcance del análisis al inicio de una de las tareas de análisis. Sin embargo, la exclusión de análisis no se aplica cuando se inicia una tarea de análisis personalizado para este objeto en particular.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de exclusiones de análisis. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Cómo crear una exclusión de análisis 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 correspondiente 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 objetos**.
4. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Exclusiones de análisis**, haga clic en el botón **Configuración**.

   Esto abre una ventana que contiene una lista de exclusiones.
5. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.

6. Seleccione la casilla **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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Endpoint Security oculta la lista consolidada de exclusiones de análisis en la interfaz de usuario de la aplicación.

7. Haga clic en **Agregar** y seleccione una acción:

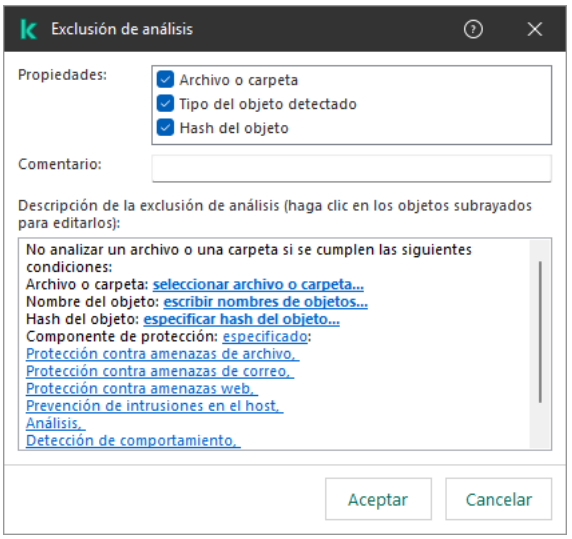
   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega 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 agregaron exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las exclusiones de análisis predefinidas según el propósito del servidor protegido.

   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva exclusión de análisis a una categoría específica, seleccione una categoría.

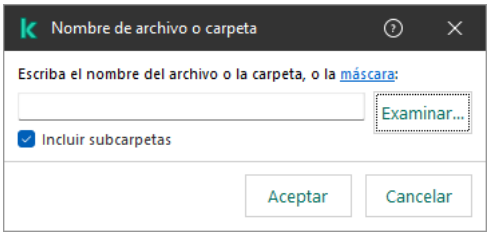
8. Para excluir un archivo o una carpeta del análisis:



Opciones de exclusión

a. En el bloque **Propiedades**, seleccione la casilla **Archivo o carpeta**.

b. Haga clic en el vínculo del siguiente bloque 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) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

   - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

Kaspersky Endpoint Security admite variables de entorno

Puede excluir carpetas de la red. Para hacer esto, ingrese la ruta a la carpeta de la red manualmente (por ejemplo, `\\Network Share\*`).

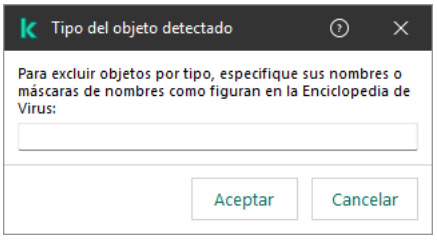
> Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de exclusiones en la consola de Kaspersky Security Center. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

b. Guarde los cambios.

9. Para excluir objetos con un nombre específico del análisis:

a. En el bloque **Propiedades**, seleccione la casilla **Tipo del objeto detectado**.

b. Haga clic en el vínculo del siguiente bloque para abrir la ventana **Tipo del objeto detectado**.



Seleccionar objeto

a. Escriba el nombre que se le da al tipo de objeto en la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza 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.

10. Si desea excluir un archivo individual de los análisis:

    a. En el bloque **Propiedades**, seleccione la casilla **Hash del objeto**.

    b. Haga clic en el vínculo del siguiente bloque para abrir la ventana **Hash del objeto**.

Seleccionar archivo

    a. Ingrese el hash del archivo o seleccione el archivo haciendo clic en el botón **Examinar**.

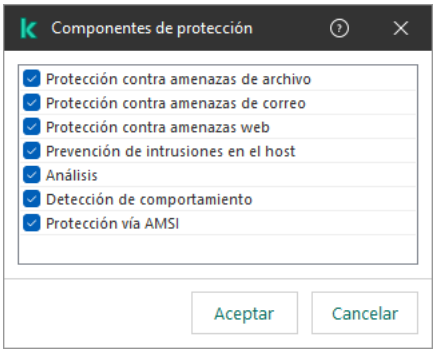
    Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se agregará a las exclusiones.

    b. Guarde los cambios.

11. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

12. Especifique los componentes de Kaspersky Endpoint Security que deben utilizar la exclusión de análisis:

    a. Haga clic en el vínculo del siguiente bloque para abrir la ventana **Componentes de protección**.



Seleccionar componentes de protección

    a. Seleccione las casillas que se encuentran frente a los componentes a los cuales se debe aplicar la exclusión de análisis.

    Si especifica componentes en la configuración de la exclusión de análisis, 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.

13. Haga clic en **Aceptar**.

    La nueva exclusión se agregará a la lista. Puede deshabilitar la exclusión en cualquier momento utilizando la casilla de verificación que se encuentra junto al objeto.

14. Guarde los cambios.

Cómo crear una exclusión de análisis con 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 ficha **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 de malware**.

6. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.

7. Seleccione la casilla **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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Endpoint Security oculta la lista consolidada de exclusiones de análisis en la interfaz de usuario de la aplicación.

8. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega 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 agregaron exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las exclusiones de análisis predefinidas según el propósito del servidor protegido.

   Para agregar una nueva exclusión de análisis a una categoría específica, seleccione la casilla de verificación junto a esa categoría y seleccione la opción **Nueva exclusión**.

9. Seleccione cómo desea agregar la exclusión: **Ruta al archivo o carpeta**, **Tipo de objeto** o **Hash del objeto**.

10. Para excluir un archivo o una carpeta del análisis, ingrese la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

    - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

      Puede excluir carpetas de la red. Para hacer esto, ingrese la ruta a la carpeta de la red manualmente (por ejemplo, `\\Network Share\*`).

11. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Tipo de objeto** debe ingresar el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza 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, ingrese 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 agregará a las exclusiones.

13. En el bloque **Aplicar exclusión a**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

14. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

15. Haga clic en **Aceptar**.

    La nueva exclusión se agregará a la lista. Puede usar el interruptor para detener una exclusión en cualquier momento.

16. Guarde los cambios.

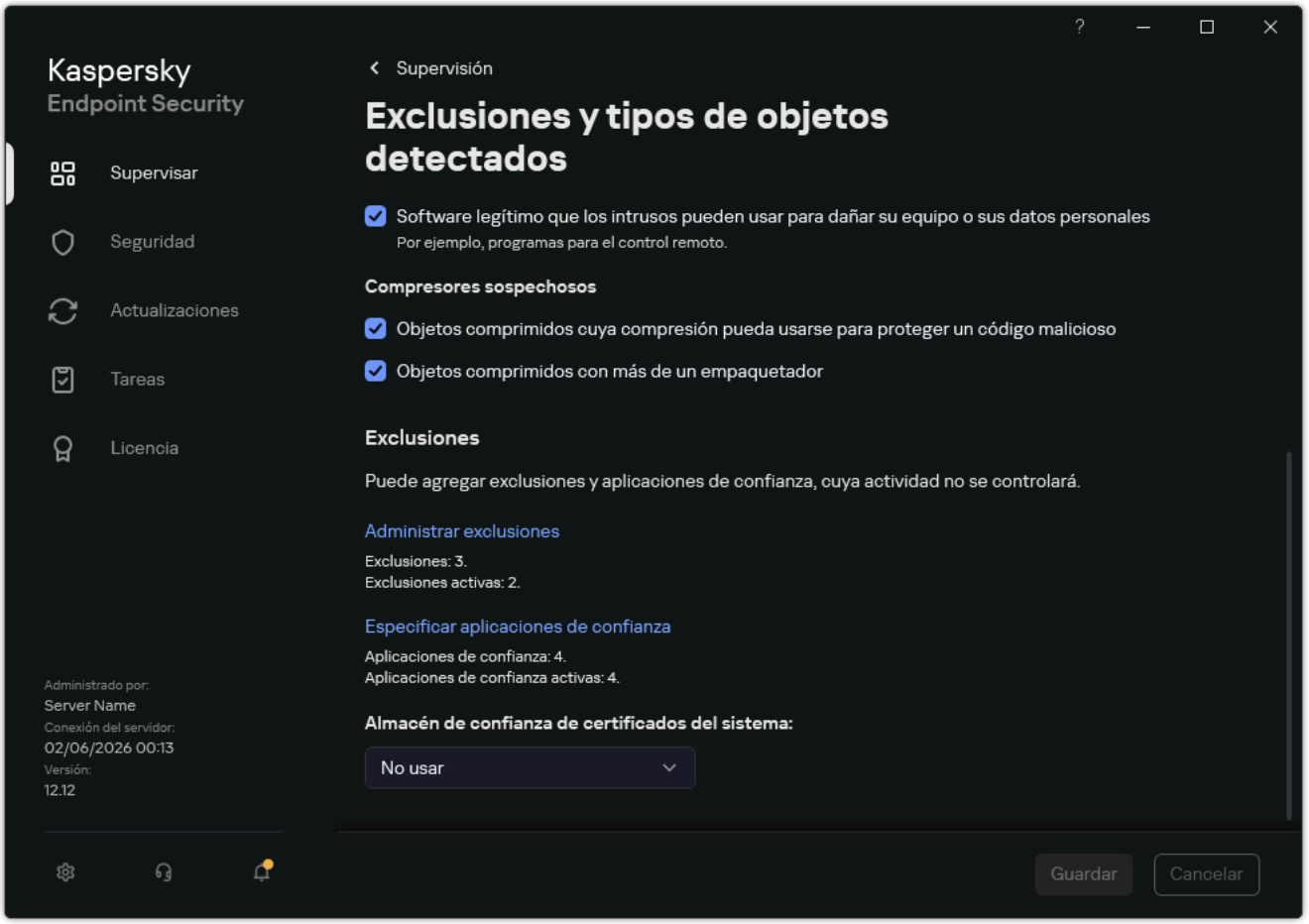
Cómo crear una exclusión de análisis en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **Administrar exclusiones**.

> Kaspersky Endpoint Security oculta la lista de exclusiones de análisis locales en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las exclusiones de análisis en la consola (símbolo de "candado cerrado") y las exclusiones de análisis locales están prohibidas (la casilla **Permitir el uso de exclusiones locales** está desactivada).



Configuración de exclusiones

4. Haga clic en **Agregar** y seleccione una acción:

- **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.
- **Nueva exclusión**. Kaspersky Endpoint Security agrega 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 agregaron exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las exclusiones de análisis predefinidas según el propósito del servidor protegido.

Para agregar una nueva exclusión de análisis a una categoría específica, seleccione la casilla de verificación junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Si desea excluir un archivo o una carpeta de los análisis, para seleccionar el archivo o la carpeta haga clic en el botón **Examinar**.

También puede escribir la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

  Puede excluir carpetas de la red. Para hacer esto, ingrese la ruta a la carpeta de la red manualmente (por ejemplo, `\\Network Share\*`).

6. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Tipo del objeto detectado** debe ingresar el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza 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, ingrese 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 agregará a las exclusiones.

8. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

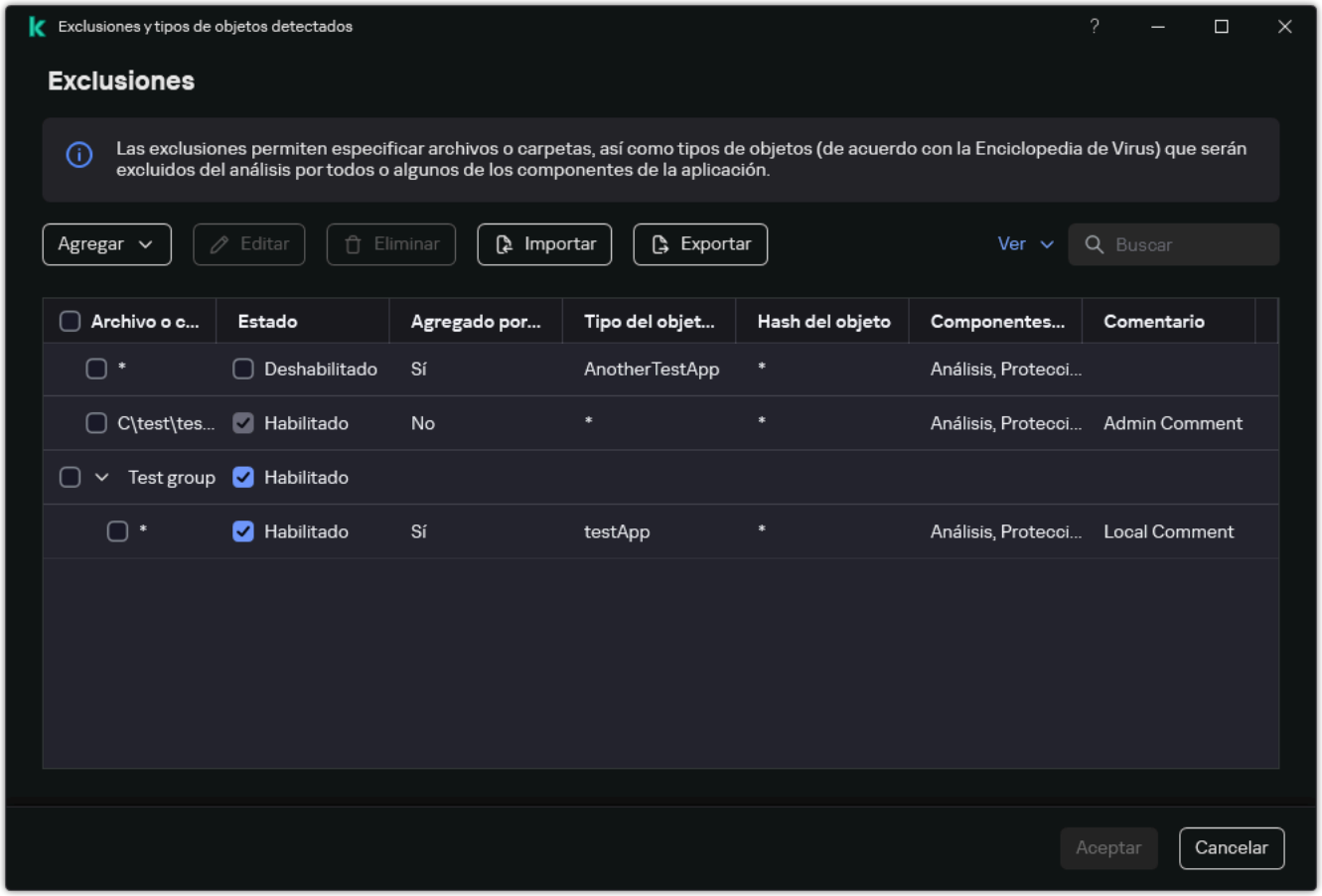
9. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

10. Seleccione el estado **Activo** para la exclusión.

11. Haga clic en **Agregar**.

    La nueva exclusión se agregará a la lista. Puede deshabilitar 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 archivo. Por ejemplo, `*\Program Files (x86)\Folder\Subfolder`.

Rutas a los archivos de cualquier carpeta:

- Si utiliza la máscara `*.exe`, se excluirán del análisis 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 almacenados en la carpeta `C:\dir\`, pero no a los almacenados en las subcarpetas de `C:\dir\`.
- La máscara `C:\dir\*` comprende las rutas a todos los archivos de la carpeta `C:\dir\` incluidas las subcarpetas.
- La máscara `C:\dir\` comprende las rutas a todos 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 la carpeta `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 la carpeta `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 la carpeta `C:\dir\` y en las subcarpetas de `C:\dir\`.
- La máscara `C:\dir1\*\dir3\` comprende las rutas a todos los archivos en las subcarpetas de dir3, un nivel menos en la carpeta `C:\dir1\`.
- La máscara `C:\dir1\**\dirN\` comprende las rutas a todos los archivos en las subcarpetas de dirN, en cualquier nivel en la carpeta `C:\dir1\`.

Rutas a los archivos de cualquier carpeta que tenga un nombre específico:

- La máscara `dir\*.*` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\` comprende las rutas a todos los 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 objeto detectado

Kaspersky Endpoint Security clasifica los objetos detectados de la siguiente forma:

- **Virus y gusanos**

  Subcategoría: Virus y gusanos (Viruses_and_Worms)

  Nivel de peligrosidad: Alto

Los virus y gusanos tradicionales realizan acciones no autorizadas por el usuario. Pueden crear copias de sí mismos capaces de replicarse.

Virus habitual

Cuando un virus tradicional ingresa a un equipo, lo que hace es infectar un archivo, activarse, realizar acciones malintencionadas y agregar copias de sí mismo a otros archivos.

Los virus tradicionales solo se multiplican en los recursos locales del equipo; no pueden penetrar otros equipos por sí mismos. Solo pueden pasar a otro equipo si agregan una copia de sí mismos a un archivo almacenado en una carpeta compartida o en un CD dentro del equipo, o si el usuario reenvía un mensaje de correo con un archivo adjunto infectado.

El código de los virus tradicionales puede penetrar diversas áreas 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 scripts* y *virus de macros*.

Los virus pueden infectar archivos mediante una variedad de técnicas. Los virus de tipo *Overwriting* escriben su código sobre el código del archivo infectado y borran el contenido de este último. El archivo infectado deja de funcionar y no se puede restaurar. Los virus de tipo *Parasitic* modifican archivos y los dejan total o parcialmente funcionales. Los virus de tipo *Companion* no modifican archivos, sino que crean duplicados. Cuando se abre un archivo infectado, se inicia un duplicado de este (que, en realidad, es un virus). También es posible encontrarse con los siguientes tipos de virus: Virus de tipo *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. Los gusanos reciben este nombre debido a su capacidad para "arrastrarse" de un equipo a otro y propagar copias de sí mismos sin el permiso del usuario mediante numerosos canales de datos.

La principal función que permite diferenciar los distintos tipos de gusanos es la forma de propagarse. La siguiente tabla proporciona un resumen de distintos tipos de gusanos, clasificados según la forma en que se propagan.

Formas de propagación

Tipo	Name	Descripción
Email-Worm	Email-Worm	Se propagan mediante el correo electrónico. Un mensaje de correo infectado contiene un documento adjunto con una copia de un gusano o un vínculo a un archivo cargado en un sitio web que puede haber sufrido un ataque o haber sido creado exclusivamente con ese fin. Cuando se abre el documento adjunto, se activa el gusano. Cuando se hace clic en el vínculo, se descarga y se abre el archivo, y el gusano empieza a realizar acciones malintencionadas. Después de esto, empieza a distribuir copias de sí mismo. Para ello, busca otras direcciones de correo y les envía mensajes infectados.
IM-Worm	Gusanos de cliente de MI	Se propagan a través de clientes de MI. Por lo general, estos gusanos envían mensajes que incluyen un vínculo a un archivo con una copia del gusano ubicado en un sitio web y utilizan las listas de contactos del usuario. Cuando el usuario descarga el archivo y lo abre, se activa el gusano.
IRC-Worm	Gusanos de chat de Internet	Se propagan mediante Internet Relay Chats, sistemas de servicio que permiten comunicarse con otras personas a través de Internet en tiempo real. Estos gusanos publican un archivo con una copia de sí mismos o un vínculo al archivo en un chat de Internet. Cuando el usuario descarga el archivo y lo abre, se activa el gusano.

Tipo	Name	Descripción
Net-Worm	Gusanos de red	Estos gusanos se propagan a través de redes de equipos. A diferencia de otros tipos de gusanos, un gusano de red típico se propaga sin la participación del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red (punto vulnerable) especialmente formado que contiene el código del gusano o una parte de él. Si en la red hay algún equipo "vulnerable", recibe este paquete de red. El gusano se activa una vez que penetra completamente en el equipo.
P2P-Worm	Gusanos de redes de uso compartido de archivos	Se propagan mediante redes punto a punto de uso compartido de archivos. Para infiltrar una red P2P, el gusano se copia en una carpeta de uso compartido de archivos que, por lo general, está situada en el equipo del usuario. La red P2P muestra información sobre este archivo, de modo que el usuario pueda "encontrar" el archivo infectado en la red como a cualquier otro archivo, descargarlo y abrirlo. Gusanos más sofisticados emulan el protocolo de red de una red P2P específica: devuelven respuestas positivas a solicitudes de búsqueda y ofrecen copias de sí mismo para su descarga.
Gusano	Otros tipos de gusanos	Otros tipos de gusanos incluyen los siguientes: • Gusanos que distribuyen copias de sí mismos por los recursos de red. Al utilizar las funciones del sistema operativo, buscan carpetas disponibles de red, se conectan a equipos conectados a Internet e intentan obtener acceso total a sus unidades de disco. A diferencia de los tipos de gusanos descritos anteriormente, otras clases 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 celular a otro).

- **Troyanos y ransomware**

  Subcategoría: Troyanos

  Nivel de peligrosidad: Alto

  A diferencia de los gusanos y los virus, los troyanos no se autorreplican. Por ejemplo, penetran un equipo a través del correo o un navegador cuando el usuario visita una página web infectada. Los troyanos requieren la participación del usuario para iniciarse. Comienzan a realizar acciones malintencionadas inmediatamente después de iniciarse.

  Los distintos troyanos se comportan de manera diferente en los equipos infectados. Las principales funciones de los troyanos consisten en bloquear, modificar o destruir información y en deshabilitar equipos o redes. Los troyanos también reciben o envían archivos, los ejecutan, muestran mensajes en pantalla, solicitan páginas web, descargan e instalan programas y reinician equipos.

  Con frecuencia, los piratas usan "conjuntos" de varios troyanos.

  Los tipos de comportamiento de los caballos de troya se describen en la siguiente tabla.

Tipos de comportamiento de caballos de troya en equipos infectados

Tipo	Name	Descripción
Trojan-ArcBomb	Troyanos: "bombas en archivos de almacenamiento"	Cuando se descomprimen, estos archivos de almacenamiento aumentan de tamaño en una medida tal que afecta el funcionamiento del equipo. Cuando el usuario intenta descomprimir un archivo de almacenamiento de esta clase, es posible que el equipo se ralentice o se bloquee, y el disco duro puede llenarse de datos "vacíos". Las "bombas en archivo de almacenamiento" son especialmente peligrosas para los servidores de correo y de archivos. Si el servidor utiliza un sistema automático para procesar la información entrante, una "bomba en archivo de almacenamiento" puede detener el servidor.
Puerta trasera	Troyanos de administración remota	Se considera que son los troyanos más peligrosos. Funcionan de manera bastante similar a las aplicaciones de administración remota instaladas en los equipos. Estos programas se instalan en el equipo sin que el usuario los detecte, lo que permite al intruso administrarlo de forma remota.

Tipo	Name	Descripción
Troyano	Troyanos	En esta categoría se incluyen las siguientes aplicaciones maliciosas: • **Troyanos tradicionales**. Estos programas solo realizan las funciones principales de los troyanos: bloquear, modificar o destruir información y deshabilitar equipos o redes. A diferencia de los otros tipos de troyano descritos en la tabla, estos no tienen funciones avanzadas. • **Troyanos versátiles**. Estos programas tienen funciones avanzadas típicas de diversos tipos de troyanos.
Trojan-Ransom	Ransom troyanos	Toman la información del usuario como "rehén", modificándola o bloqueándola, o afectan el funcionamiento del equipo, de modo que el usuario pierde la capacidad de utilizar la información. El intruso le exige al usuario un rescate a cambio de una aplicación que permita restaurar la información y la operatividad del equipo.
Trojan-Clicker	Trojan-Clicker	Acceden a páginas web desde el equipo del usuario, ya sea mediante el envío de comandos a un navegador por su cuenta o por medio de la modificación de las direcciones web especificadas en los archivos del sistema operativo. Al utilizar estos programas, los intrusos realizan ataques de red e incrementan las visitas a sitios web, lo que aumenta la cantidad de anuncios publicitarios que se muestran.
Trojan-Downloader	Descargadores troyanos	Acceden a la página web del intruso para descargar de allí otra aplicación malintencionada e instalarla en el equipo del usuario. El nombre del archivo que se debe descargar puede venir establecido de antemano dentro del troyano o puede determinarse al acceder a la página del atacante.
Trojan-Dropper	Caballos de troya instaladores de software malintencionado	Contienen otros troyanos que descargan en el disco duro y luego instalan. Los intrusos pueden utilizar programas de este tipo para cumplir los siguientes objetivos: • Instalar una aplicación malintencionada sin que el usuario lo advierta: Los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (por ejemplo, pueden advertir sobre la existencia de un archivo dañado o sobre incompatibilidades en el sistema operativo). • Impedir la detección de una aplicación malintencionada conocida. No todos los antivirus son capaces de detectar aplicaciones malintencionadas cuando vienen ocultas en troyanos de este tipo.
Trojan-Notifier	Caballos de troya notificadores	Le informan al atacante que puede introducirse en el sistema infectado y le envían información sobre el equipo: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso por medio del correo electrónico, FTP, ingreso a la página web del intruso o de otra manera. Los troyanos notificadores suelen utilizarse en conjuntos conformados por varios troyanos. Informan al intruso que se han instalado correctamente otros troyanos en el equipo del usuario.
Trojan-Proxy	Caballos de troya proxy	Permiten al intruso acceder de forma anónima a páginas web mediante el equipo del usuario. Con frecuencia, se utilizan para enviar correo no deseado.
Trojan-PSW	Programas que roban contraseñas	Los programas que roban contraseñas son una clase de caballo de troya que roba cuentas de usuarios, tales como datos de registro de software. Estos troyanos encuentran datos confidenciales en archivos del sistema y en el registro y se los envían al "atacante" mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo. Algunos de estos troyanos se categorizan en los distintos tipos descritos en esta 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 por Internet (Trojan-GameThief).
Trojan-Spy	Caballos de troya espías	Espían al usuario y reúnen información acerca de las acciones que este realiza cuando trabaja en el equipo. Pueden interceptar los datos introducidos por el usuario mediante el teclado, realizar capturas de pantalla o compilar listas de aplicaciones activas. Después de recibir la información, se la transfieren al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.
Trojan-DDoS	Caballos de troya atacantes de red	Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). Los piratas suelen infectar muchos equipos con estos programas de manera de utilizar los equipos para atacar a un único servidor simultáneamente. Los programas DoS llevan a cabo un ataque desde un único equipo con el conocimiento del usuario. Los programas DDoS (DoS distribuida) llevan a cabo ataques distribuidos desde distintos equipos sin que lo advierta el usuario del equipo infectado.
Trojan-IM	Troyanos que roban información de usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de quienes usan clientes de mensajería instantánea. Transfieren los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.

Tipo	Name	Descripción
Rootkit	RootKits	Enmascaran la existencia y las acciones de otras aplicaciones malintencionadas para ayudarlas a perdurar en el sistema operativo. También pueden ocultar archivos, claves del registro que se utilicen para ejecutar aplicaciones malintencionadas o procesos que se encuentren cargados en la memoria del equipo infectado. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones en el equipo del usuario y en otros equipos de la red.
Trojan-SMS	Troyanos en la forma de mensajes SMS	Infectan teléfonos móviles y envían mensajes SMS a números de teléfono con tarifas elevadas.
Trojan-GameThief	Troyanos que roban información de usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, tras lo cual envían los datos al intruso mediante correo, 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 luego envían la información al hacker por correo electrónico, por FTP, a través de una página creada por el atacante o usando otros medios.
Trojan-Mailfinder	Troyanos que reúnen direcciones de correo	Recopilan direcciones de correo almacenadas en un equipo y se las envían al intruso mediante correo, FTP, acceso a la página web del intruso o de 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 malware, las herramientas maliciosas no realizan acciones inmediatamente después de iniciarse. Pueden almacenarse de manera segura e iniciarse en el equipo del usuario. A menudo, los intrusos utilizan las funciones de estos programas para crear virus, gusanos y troyanos, perpetrar ataques de red en servidores remotos, atacar equipos o llevar a cabo otras acciones malintencionadas.

  Varias funciones de las herramientas maliciosas se agrupan en los tipos descritos en la siguiente tabla.

Funciones de herramientas maliciosas

Tipo	Name	Descripción
Constructor	Constructores	Permiten crear nuevos virus, gusanos y troyanos. Algunos constructores ofrecen una interfaz estándar, con ventanas para elegir el tipo de aplicación malintencionada que se va a crear, los métodos que se usarán para contrarrestar los depuradores y otras características.
DoS	Ataque de red	Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS).
Exploit	Exploits	Los *puntos vulnerables* son conjuntos de datos o códigos de programas que se sirven de las vulnerabilidades de la aplicación en la que se procesa para realizar una acción maliciosa en un equipo. Por ejemplo, un punto vulnerable puede escribir o leer archivos o solicitar páginas web "infectadas". Distintos puntos vulnerables se sirven de las vulnerabilidades de diversos servicios de red o aplicaciones. Disfrazados como paquete de red, los puntos vulnerables se transfieren a través de la red a numerosos equipos y buscan equipos con servicios de red vulnerables. Un punto vulnerable en un archivo DOC se sirve de las vulnerabilidades de un editor de texto. Puede comenzar a realizar las acciones preprogramadas por el pirata cuando el usuario abre el archivo infectado. Un punto vulnerable incrustado en un mensaje de correo busca vulnerabilidades en cualquier cliente de correo. Puede empezar a realizar una acción malintencionada apenas el usuario abre el mensaje infectado en dicho cliente. Los gusanos de red se propagan por las redes mediante los puntos vulnerables. Los puntos vulnerables Nuker son paquetes de red que deshabilitan equipos.
FileCryptor	Cifradores	Se utilizan para cifrar otras aplicaciones malintencionadas y evitar, con ello, que las aplicaciones antivirus las detecten.

Tipo	Name	Descripción
Flooder	Programas para "contaminar" redes	Envían numerosos mensajes a través de canales de red. Este tipo de herramienta incluye, por ejemplo, programas que contaminan Internet Relay Chats. Las herramientas de tipo "flooder" no incluyen programas que "contaminan" los canales usados por el correo, los clientes de mensajería instantánea y los sistemas de comunicaciones móviles. Estos programas se describen de manera individual en la tabla (flooder de correo, IM-Flooder y flooder de SMS).
HackTool	Herramientas de piratería	Permiten los ataques a los equipos en los que están instalados o atacan otro equipo (por ejemplo, mediante la adición de nuevas cuentas de sistema sin el permiso del usuario o la eliminación de registros del sistema para ocultar rastros de su presencia en el sistema operativo). Este tipo de herramienta incluye algunos analizadores de protocolos que ofrecen funciones malintencionadas, como la interceptación de contraseñas. Los analizadores de protocolos son programas que permiten ver el tráfico de red.
Hoax	Hoax	Alarman al usuario con mensajes similares a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario de que se dio formato a un disco, cuando esto no sucedió en realidad.
Spoofer	Herramientas de falsificación	Envían mensajes y solicitudes de red con una dirección falsa del remitente. Los intrusos utilizan herramientas de falsificación para hacerse pasar por los verdaderos remitentes de los mensajes, por ejemplo.
VirTool	Herramientas que pueden ingresar modificaciones en las aplicaciones malintencionadas	Permiten la modificación de otros programas de software malware y los ocultan de las aplicaciones antivirus.
Email-Flooder	Programas que "contaminan" las direcciones de correo	Envían numerosos mensajes a varias direcciones de correo electrónico y, de este modo, las contaminan. Un gran volumen de mensajes entrantes impide que los usuarios vean mensajes deseados en sus buzones.
IM-Flooder	Programas que "contaminan" el tráfico de los clientes de MI	"Inundan" a los usuarios de clientes de MI con mensajes. Un gran volumen de mensajes impide a los usuarios visualizar mensajes entrantes deseados.
SMS-Flooder	Programas que "contaminan" el tráfico con mensajes SMS	Envían numerosos mensajes de SMS a teléfonos móviles.

- **Adware**

  Subcategoría: software de publicidad (Adware)

  Nivel de peligrosidad: medio

  El adware muestra información publicitaria al usuario. Los programas de adware muestran anuncios publicitarios en las interfaces de otros programas y redireccionan las solicitudes de búsqueda a páginas web publicitarias. Algunos reúnen información de marketing acerca del usuario y la envían a su desarrollador. Esta información puede incluir los nombres de los sitios web visitados por el usuario o el contenido de sus solicitudes de búsqueda. A diferencia de los caballos de troya espías, el 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 conexiones telefónicas de forma encubierta mediante un módem.

- **Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales**

  Subcategoría: Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales.

Nivel de peligrosidad: medio

La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP y Telnet.

Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

Tipo	Name	Descripción
Cliente IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware.
Downloader	Programas para realizar descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas para supervisar	Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito.
RemoteAdmin	Programas de administración remota	Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo.
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores Telnet. Los intrusos los implantan 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 los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos.
NetTool	Herramientas de red	Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos.
Client-P2P	Clientes de red P2P	Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware.
Cliente SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
WebToolbar	Barras de herramientas web	Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Pseudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada.

- **Objetos comprimidos cuya compresión pueda usarse para proteger un 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 descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen con compresores especiales. Los expertos de Kaspersky identificaron los compresores más utilizados por los piratas informáticos.

- **Objetos comprimidos con más de un empaquetador**

  Subcategoría: Archivos comprimidos múltiples.

  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 los archivos comprimidos.

De forma predeterminada, Kaspersky Endpoint Security detecta objetos de todo tipo. Recomendamos habilitar la detección de todo tipo de objetos para mejorar la seguridad del equipo. Si emplea utilidades internas que la aplicación detecta como maliciosas, agréguelas a una lista de exclusión, pero no deshabilite la detección de todo 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 correspondiente 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 objetos**.
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 ubicadas junto a los tipos de objetos que desee que Kaspersky Endpoint Security detecte.
7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo seleccionar 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 ficha **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 junto a los tipos de objetos que desee que Kaspersky Endpoint Security detecte.

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

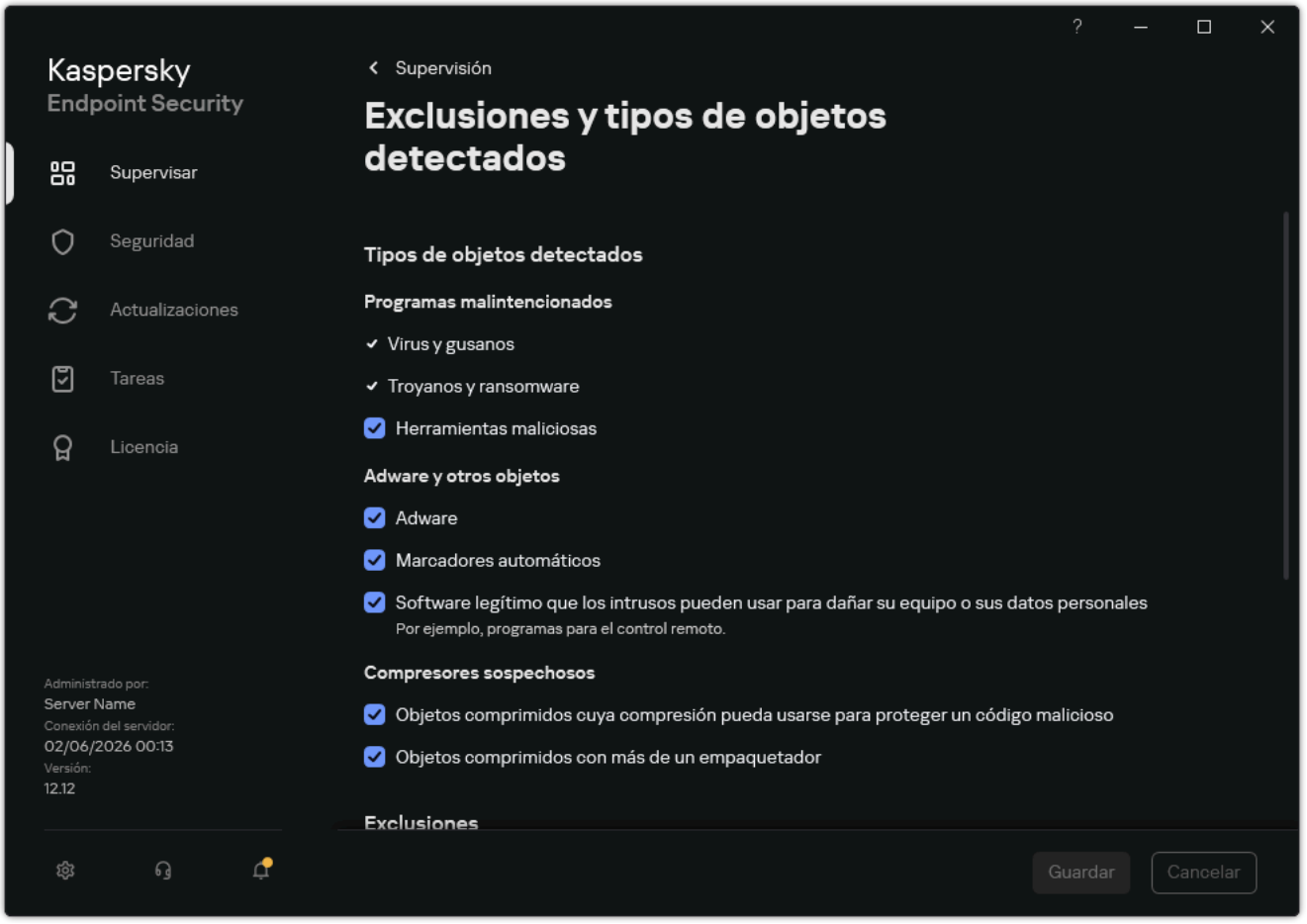
Cómo seleccionar tipos de objetos detectables en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 junto a los tipos de objetos que desee que Kaspersky Endpoint Security detecte.

4. Guarde los cambios.



Tipos de objetos detectables

Modificación de la lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de archivos y de red (incluida la actividad maliciosa) y el acceso al registro del sistema no son supervisados por Kaspersky Endpoint Security. De manera predeterminada, Kaspersky Endpoint Security supervisa las acciones y el tráfico de red de todas las aplicaciones y analiza los objetos que abren, ejecutan o guardan los procesos asociados a las mismas. 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 agrega a las exclusiones, Kaspersky Endpoint Security omitirá este archivo.

Por ejemplo, si considera que los objetos utilizados por la aplicación estándar Bloc de notas de Microsoft Windows son seguros, es decir, que confía en esta aplicación, puede agregar el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza para no supervisar los objetos utilizados por esta aplicación. Esto aumentará el rendimiento del equipo, lo cual es especialmente importante cuando se usan aplicaciones de servidor.

Además, ciertas acciones clasificadas por Kaspersky Endpoint Security como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de una cantidad de aplicaciones. Por ejemplo, la intercepción del texto escrito con el teclado es un proceso de rutina para los conmutadores de disposición del teclado automática (como Punto Switcher). Para tener en cuenta las características de estas aplicaciones y no supervisarlas, se recomienda agregarlas 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 otra aplicación antivirus).

Al mismo tiempo, el archivo ejecutable y los procesos de la aplicación de confianza seguirán siendo analizados en busca de virus y otras clases de malware. Una aplicación se puede excluir completamente del análisis de Kaspersky Endpoint Security mediante Exclusiones de análisis.

Las propiedades de la directiva principal pueden bloquear la modificación de la lista de aplicaciones de confianza. Para modificar la lista, debe permitir cambiar la configuración de la zona de confianza en Web Console (el "candado" debe estar cerrado).

Las zonas de confianza se agrupan de manera diferente en la Consola de administración (MMC) y Web Console. Asimismo, la forma en que se evitan los cambios en los parámetros de la zona de confianza es diferente (diferentes "candados"). Recomendamos usar solo Web Console para administrar la aplicación. Si configura la zona de confianza en diferentes consolas, el complemento de administración podría restablecer el "candado" a su estado predeterminado.

Cómo agregar una aplicación a la lista 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 correspondiente 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 objetos**.

4. 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 las aplicaciones de confianza.

5. Active la casilla **Combinar valores al heredar** si desea crear una lista de aplicaciones de confianza unificada para todos los equipos de la empresa. La lista de aplicaciones de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las aplicaciones de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.

6. Seleccione la casilla **Permitir el uso de aplicaciones de confianza 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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Endpoint Security oculta la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación.

7. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega la 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 agregaron aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las aplicaciones de confianza predefinidas según el propósito del servidor protegido.

   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva aplicación de confianza a una categoría específica, seleccione una categoría.

8. Seleccione los criterios de confianza:

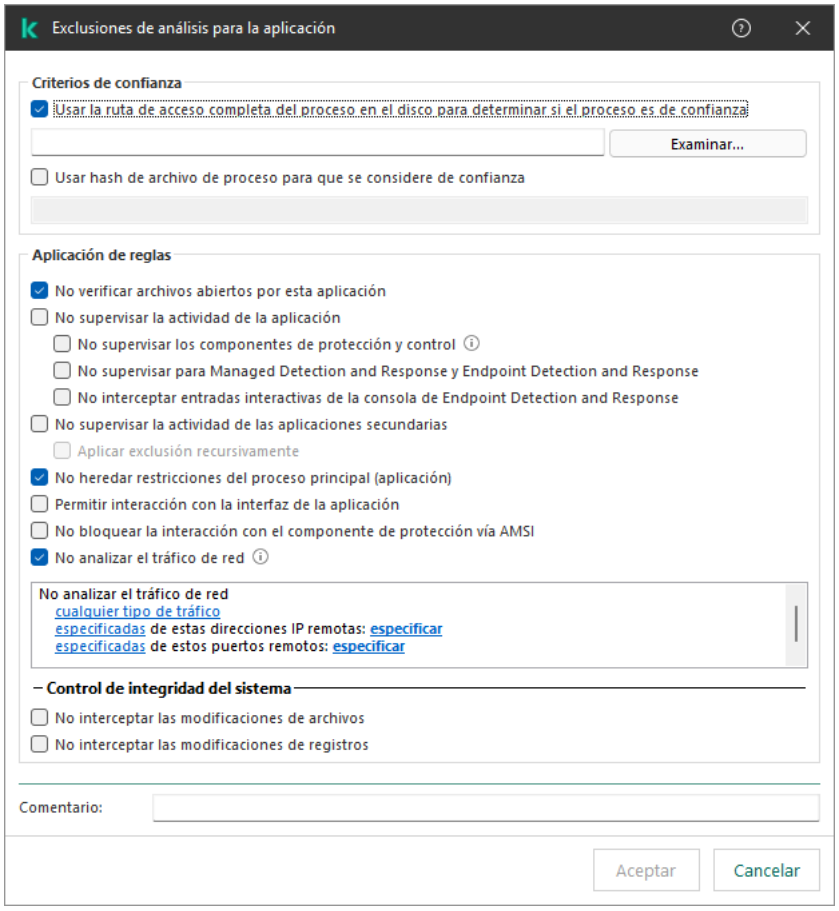
   - **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza**. Ingrese la ruta al archivo ejecutable de la aplicación de confianza.

     Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

     Kaspersky Endpoint Security distingue mayúsculas y minúsculas en el nombre de archivo de una aplicación de confianza. Si el nombre del archivo que ingresa es incorrecto, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

   - **Usar hash de archivo de proceso para que se considere 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 aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.



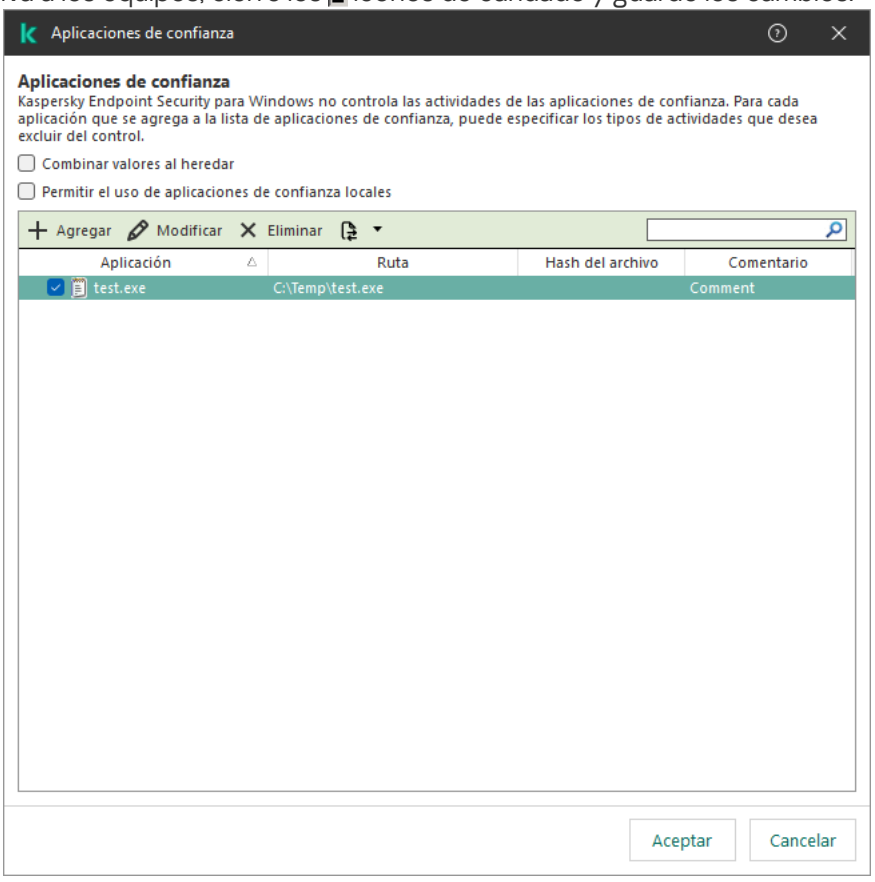
Configuración de la aplicación de confianza

9. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).

10. Haga clic en **Aceptar**.

    La nueva aplicación de confianza se agregará a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación que se encuentra junto al objeto.

11. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.



Lista de aplicaciones de confianza

Cómo agregar una aplicación a la lista 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 ficha **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 las aplicaciones de confianza.

6. Active la casilla **Combinar valores al heredar** si desea crear una lista de aplicaciones de confianza unificada para todos los equipos de la empresa. La lista de aplicaciones de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las aplicaciones de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.

7. Seleccione la casilla **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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Endpoint Security oculta la lista consolidada de aplicaciones de confianza en la interfaz de usuario de la aplicación.

8. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega la 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 agregaron aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las aplicaciones de confianza predefinidas según el propósito del servidor protegido.

   Para agregar una nueva aplicación de confianza a una categoría específica, seleccione la casilla de verificación junto a esa categoría y seleccione la opción **Nueva exclusión**.

9. Seleccione los criterios de confianza:

   - **Ruta al archivo o carpeta**. Ingrese la ruta al archivo ejecutable de la aplicación de confianza.

     Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

     Kaspersky Endpoint Security distingue mayúsculas y minúsculas en el nombre de archivo de una aplicación de confianza. Si el nombre del archivo que ingresa es incorrecto, 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 aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

10. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).

11. Haga clic en **Aceptar**.

    La nueva aplicación de confianza se agregará 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. Guarde los cambios.

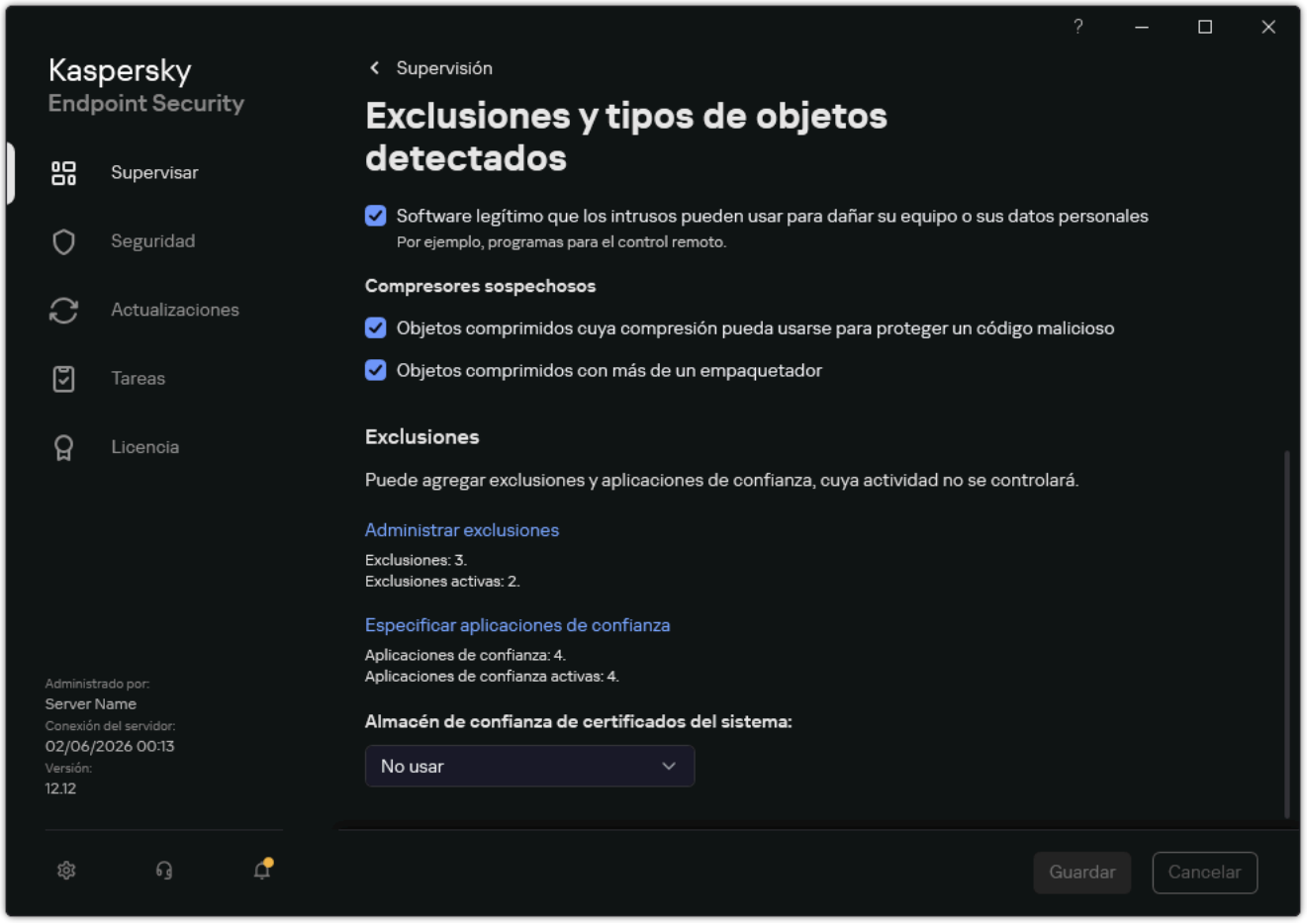
Cómo agregar una aplicación a la lista de confianza en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **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 **Permitir el uso de aplicaciones de confianza locales** está desactivada).



Configuración de exclusiones

4. Haga clic en **Agregar** y seleccione una acción:

- **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.
- **Nueva exclusión**. Kaspersky Endpoint Security agrega la 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 agregaron aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las aplicaciones de confianza predefinidas según el propósito del servidor protegido.

Para agregar una nueva aplicación de confianza a una categoría específica, seleccione la casilla de verificación junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Seleccione los criterios de confianza:

- **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza**. Ingrese la ruta al archivo ejecutable de la aplicación de confianza.

  Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

Kaspersky Endpoint Security distingue mayúsculas y minúsculas en el nombre de archivo de una aplicación de confianza. Si el nombre del archivo que ingresa es incorrecto, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

- **Usar hash de archivo de proceso para que se considere de confianza**.

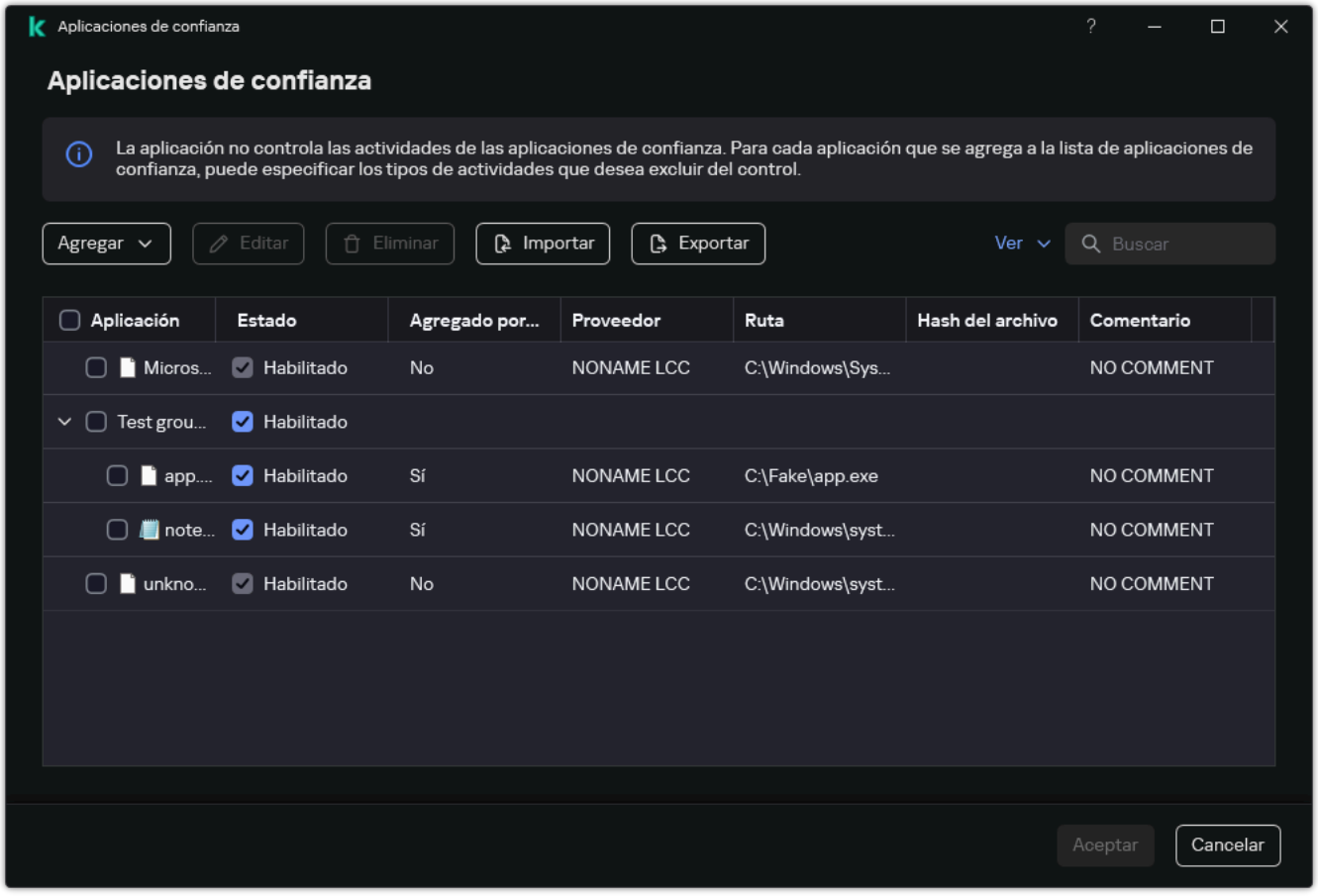
Kaspersky Endpoint Security es compatible con variables de entorno y convierte la ruta en la interfaz local de la aplicación. Es decir, si ingresa la ruta de archivo `%userprofile%\Documents\File.exe`, se agregará un registro `C:\Users\Fred123\Documents\File.exe` en la interfaz local de la aplicación para el usuario Fernando123. De forma similar, Kaspersky Endpoint Security omite el programa de confianza `File.exe` para otros usuarios. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, defina la configuración avanzada.

7. Haga clic en **Aceptar**.

   La nueva aplicación de confianza se agregará 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

Parámetro	Descripción
No verificar archivos abiertos por esta aplicación	Kaspersky Endpoint Security no analizará ningún archivo que la aplicación abra. 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 la red y los archivos de la aplicación en el sistema operativo. Puede configurar la supervisión de la actividad de las aplicaciones para diferentes componentes de Kaspersky Endpoint Security: • **No supervisar los componentes de protección y control**. La actividad de la aplicación se supervisa 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 y Endpoint Detection and Response**. La actividad de las aplicaciones se supervisa a través del agente MDR incorporado y el EDR (KATA) agent incorporado. • **No interceptar entradas interactivas de la consola de Endpoint Detection and Response**. Kaspersky Endpoint Security no envía datos de telemetría sobre la administración de la aplicación en la consola. Los datos de telemetría son utilizados por Kaspersky Anti Targeted Attack Platform (EDR).
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Endpoint Security no supervisará las actividades de red ni las operaciones de archivo que realicen las aplicaciones iniciadas por la aplicación. Puede aplicar la exclusión de manera recurrente. De esta manera, 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 lo inicia una aplicación para la que se configuran los derechos de aplicaciones (Prevención de intrusiones en el host) y las reglas de red de aplicaciones (Firewall).
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Endpoint Security no supervisará las actividades de red ni las operaciones de archivo que realicen las aplicaciones iniciadas por la aplicación. Puede aplicar la exclusión de manera recurrente. De esta manera, la aplicación no supervisa la actividad de toda la cadena de aplicaciones secundarias.
Permitir interacción con la interfaz de la aplicación	La Autoprotección de Kaspersky Endpoint Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona esta casilla, se permite que la aplicación de acceso remoto administre la configuración de Kaspersky Endpoint Security a través de la interfaz de Kaspersky Endpoint Security.
No bloquear la interacción con el componente de protección vía AMSI	Kaspersky Endpoint Security no supervisará las solicitudes de la aplicación de confianza para que el componente de protección vía AMSI analice objetos.
No analizar el tráfico de red	Kaspersky Endpoint Security no analizará el tráfico de red que tenga origen en la aplicación. Puede excluir de los análisis todo el tráfico o solo el tráfico cifrado. También puede excluir direcciones IP y números de puerto individuales 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 las modificaciones de archivos *(disponible solo en la Consola de Kaspersky Security Center)*	Kaspersky Endpoint Security no supervisa los cambios en los archivos incluidos en el alcance del monitoreo de Control de integridad del sistema. La aplicación ejecuta la exclusión en todos los modos de Control de integridad del sistema: Control de integridad del sistema en tiempo real y Comprobación de integridad del sistema a pedido.
No interceptar las modificaciones de registros *(disponible solo en la Consola de Kaspersky Security Center)*	Kaspersky Endpoint Security no supervisa los cambios en las claves del registro incluidas en el alcance del monitoreo de Control de integridad del sistema. La aplicación ejecuta la exclusión en todos los modos de Control de integridad del sistema: Control de integridad del sistema en tiempo real y Comprobación de integridad del sistema a pedido.
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: • Un estado **Activo** significa que la aplicación está en la zona de confianza. • Un estado **Inactivo** significa que la aplicación fue excluida de la zona de confianza.

Crear una zona de confianza local

El usuario ahora puede crear su propia zona de confianza local para 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 de verificación **Permitir el uso de exclusiones locales** y **Permitir el uso de aplicaciones de confianza locales** en la sección **Exclusiones** de la directiva.

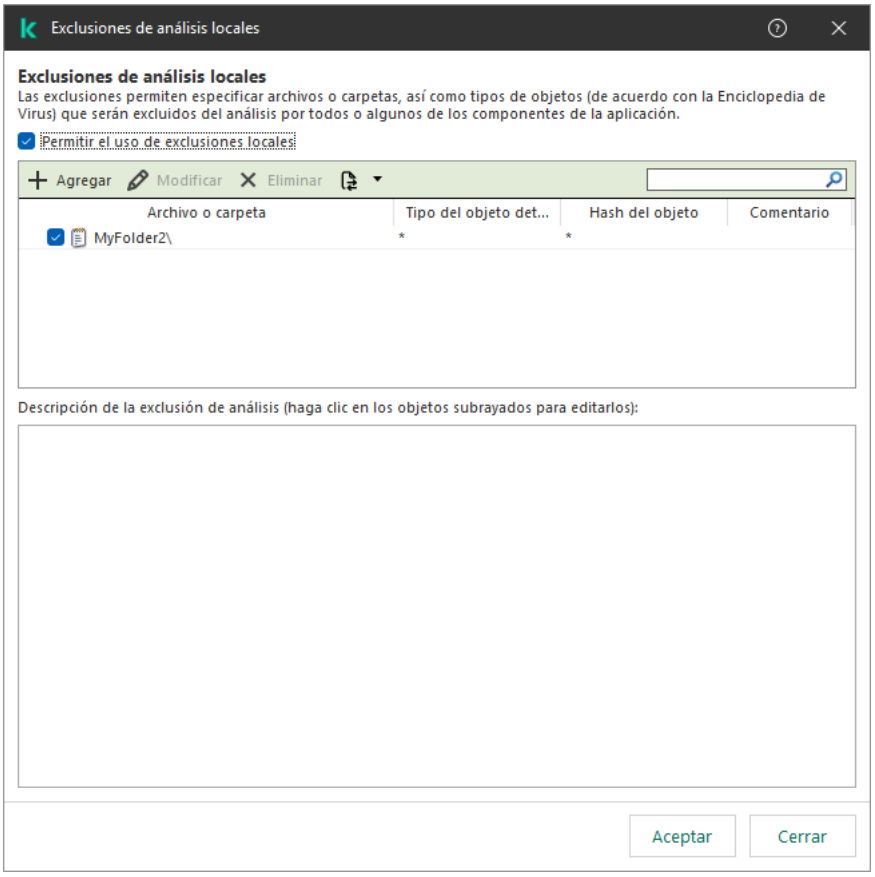
Si un administrador permite la creación de una zona de confianza local, el usuario puede agregar sus propias exclusiones de análisis y aplicaciones de confianza en la interfaz de usuario de la aplicación. Al mismo tiempo, el usuario no tiene permisos para modificar o eliminar objetos de la zona de confianza configurada en la directiva. El administrador también puede ver, agregar, modificar o eliminar elementos de la lista en la consola de Kaspersky Security Center si es necesario agregar exclusiones para un equipo individual.

Kaspersky Endpoint Security oculta las listas de exclusiones de 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 de análisis y las aplicaciones de confianza locales están prohibidas.

Cómo agregar 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Haga doble clic en un equipo para abrir su ventana de propiedades.
5. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.1)** 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 objetos**.
8. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Exclusiones de análisis locales**, haga clic en el botón **Configuración**.

Esto abre una ventana que contiene una lista de exclusiones locales.



Configuración de la zona de confianza

9. Haga una lista de exclusiones de análisis locales.

   Las reglas para crear exclusiones de análisis locales son las mismas que para las exclusiones generales. Kaspersky Endpoint Security admite variables de entorno y los caracteres * y ? al ingresar una máscara.

10. En el bloque **Exclusiones de análisis y aplicaciones de confianza** → **Aplicaciones de confianza locales**, haga clic en el botón **Configuración**.

    Esto abre una ventana que contiene una lista de las aplicaciones de confianza locales.

11. Haga una lista de las aplicaciones de confianza locales.

    Las reglas para agregar aplicaciones a la lista de aplicaciones de confianza locales son las mismas que las reglas para agregarlas a la lista general. Kaspersky Endpoint Security admite variables de entorno y los caracteres * y ? al ingresar una máscara.

12. Guarde los cambios.

Cómo agregar un objeto a la zona de confianza local en 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 donde quiere permitir que un usuario realice una acción bloqueada.

3. Seleccione la ficha **Aplicaciones**.

4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.

5. Seleccione la ficha **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 vínculo **Exclusiones de análisis locales**.

8. Haga una lista de exclusiones de análisis locales.

   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 ingresar una máscara.

9. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el vínculo **Aplicaciones de confianza locales**.

10. Haga una lista de las aplicaciones de confianza locales.

    Las reglas para agregar aplicaciones a la lista de aplicaciones de confianza locales son las mismas que las reglas para agregarlas a la lista general. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

11. Guarde los cambios.

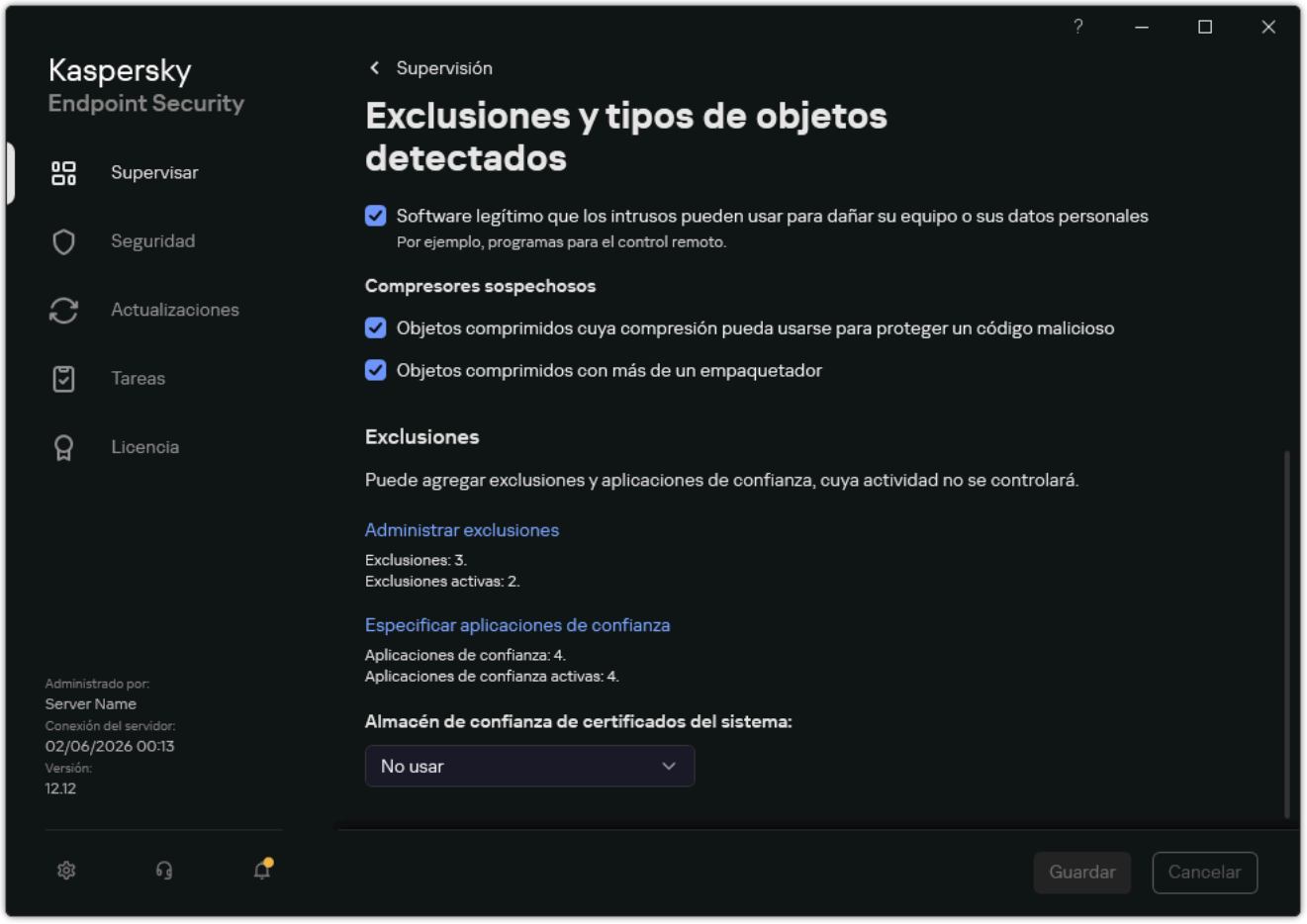
Cómo crear una exclusión de análisis local en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **Administrar exclusiones**.

Kaspersky Endpoint Security oculta la lista de exclusiones de análisis locales en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las exclusiones de análisis en la consola (símbolo de "candado cerrado") y las exclusiones de análisis locales están prohibidas (la casilla **Permitir el uso de exclusiones locales** está desactivada).



Configuración de exclusiones

4. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.

   - **Nueva exclusión**. Kaspersky Endpoint Security agrega 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 agregaron exclusiones de análisis predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las exclusiones de análisis predefinidas según el propósito del servidor protegido.

   Para agregar una nueva exclusión de análisis a una categoría específica, seleccione la casilla de verificación junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Si desea excluir un archivo o una carpeta de los análisis, para seleccionar el archivo o la carpeta haga clic en el botón **Examinar**.

También puede escribir la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

  Puede excluir carpetas de la red. Para hacer esto, ingrese la ruta a la carpeta de la red manualmente (por ejemplo, `\\Network Share\*`).

6. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Tipo del objeto detectado** debe ingresar el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza 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, ingrese 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 agregará a las exclusiones.

8. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

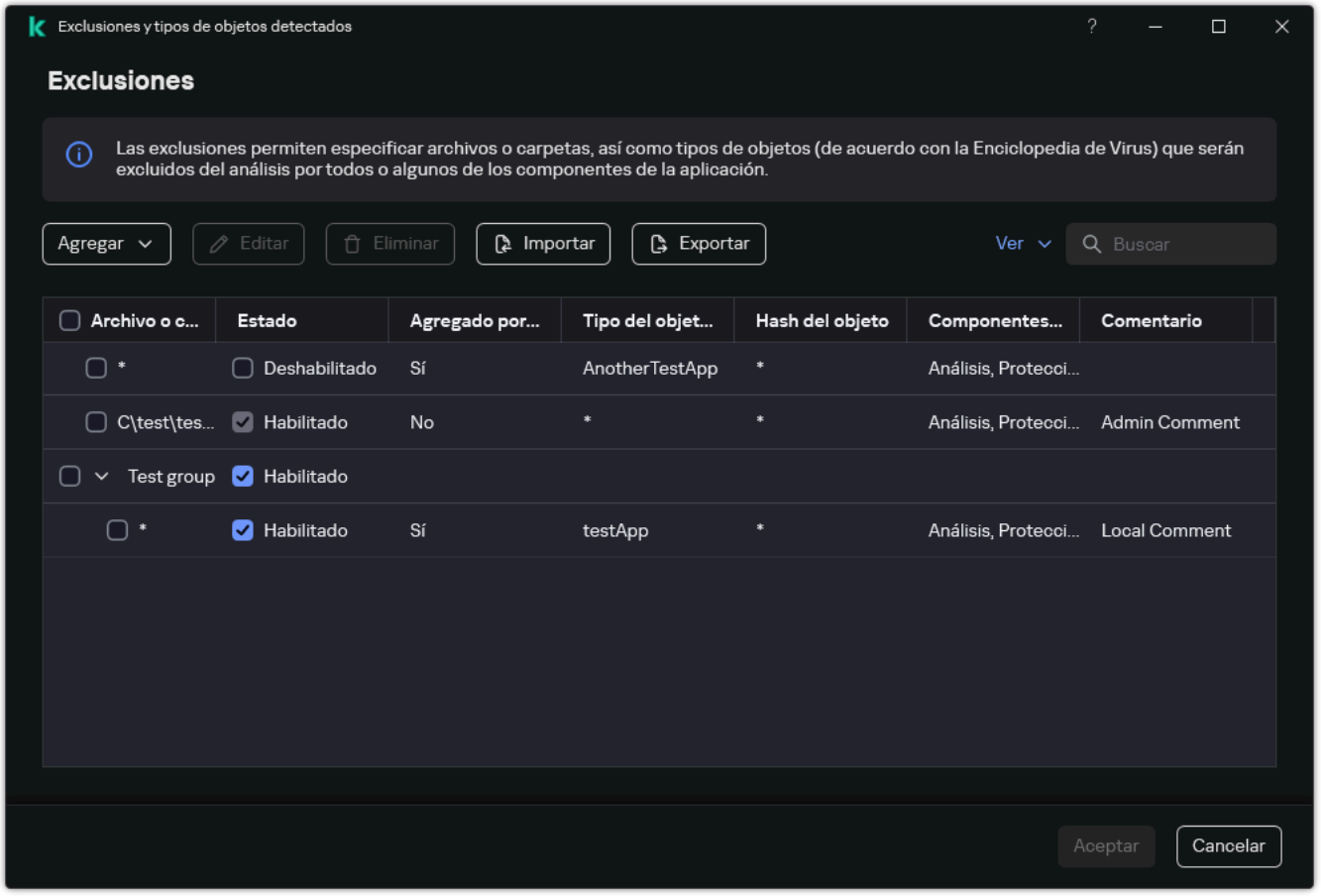
9. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

10. Seleccione el estado **Activo** para la exclusión.

11. Haga clic en **Agregar**.

    La nueva exclusión se agregará a la lista. Puede deshabilitar la exclusión en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

12. Guarde los cambios.



Lista de exclusiones

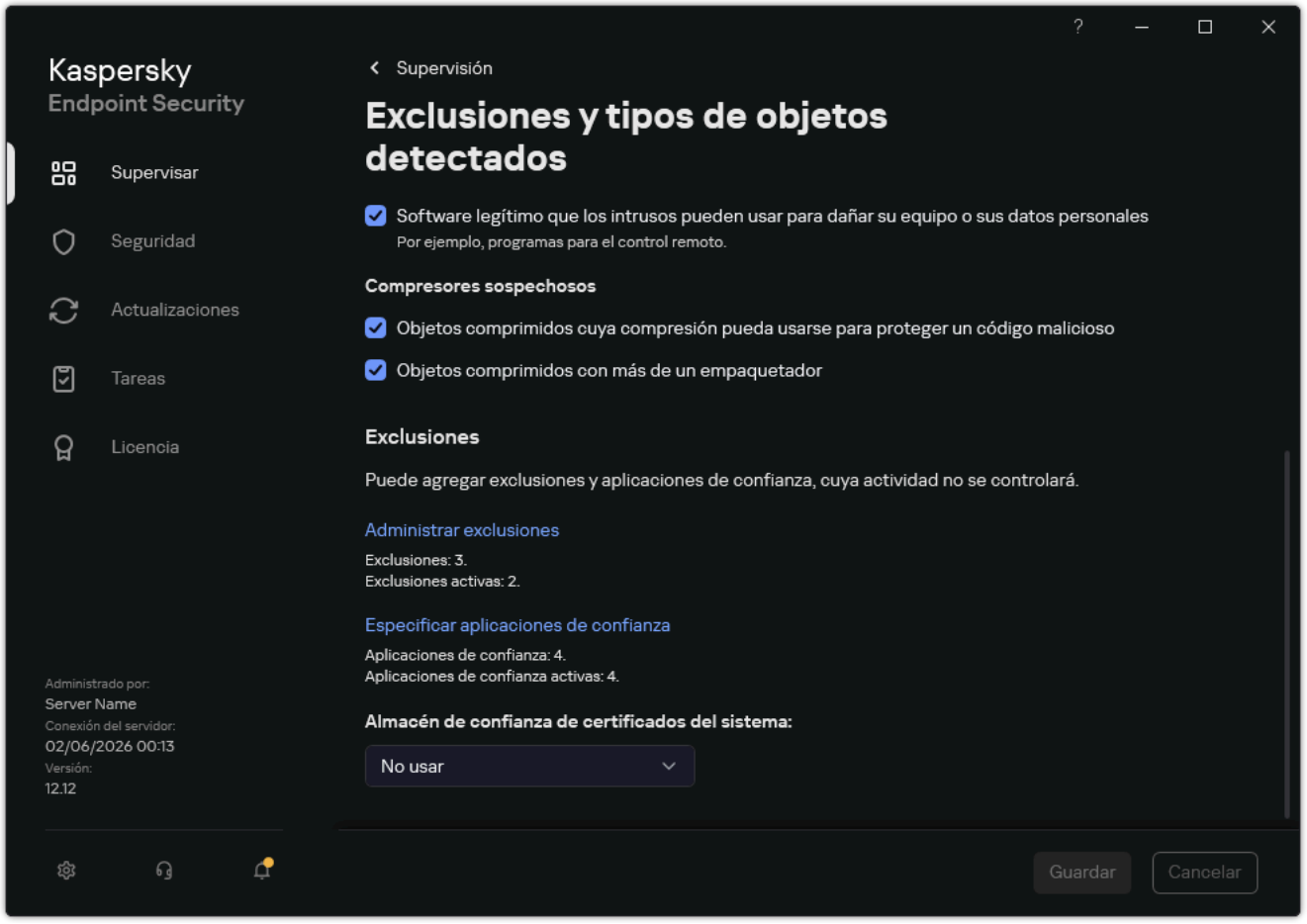
Cómo agregar una aplicación a la lista de aplicaciones de confianza locales en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **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 **Permitir el uso de aplicaciones de confianza locales** está desactivada).



Configuración de exclusiones

4. Haga clic en **Agregar** y seleccione una acción:

- **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.
- **Nueva exclusión**. Kaspersky Endpoint Security agrega la 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 agregaron aplicaciones de confianza predefinidas para admitir la configuración de la aplicación en entornos virtuales de Citrix y VMware. Debe seleccionar las aplicaciones de confianza predefinidas según el propósito del servidor protegido.

Para agregar una nueva aplicación de confianza a una categoría específica, seleccione la casilla de verificación junto a esa categoría y seleccione la opción **Nueva exclusión**.

5. Seleccione los criterios de confianza:

- **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza**. Ingrese la ruta al archivo ejecutable de la aplicación de confianza.

  Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

Kaspersky Endpoint Security distingue mayúsculas y minúsculas en el nombre de archivo de una aplicación de confianza. Si el nombre del archivo que ingresa es incorrecto, Kaspersky Endpoint Security no reconocerá la aplicación de confianza.

- **Usar hash de archivo de proceso para que se considere de confianza**.

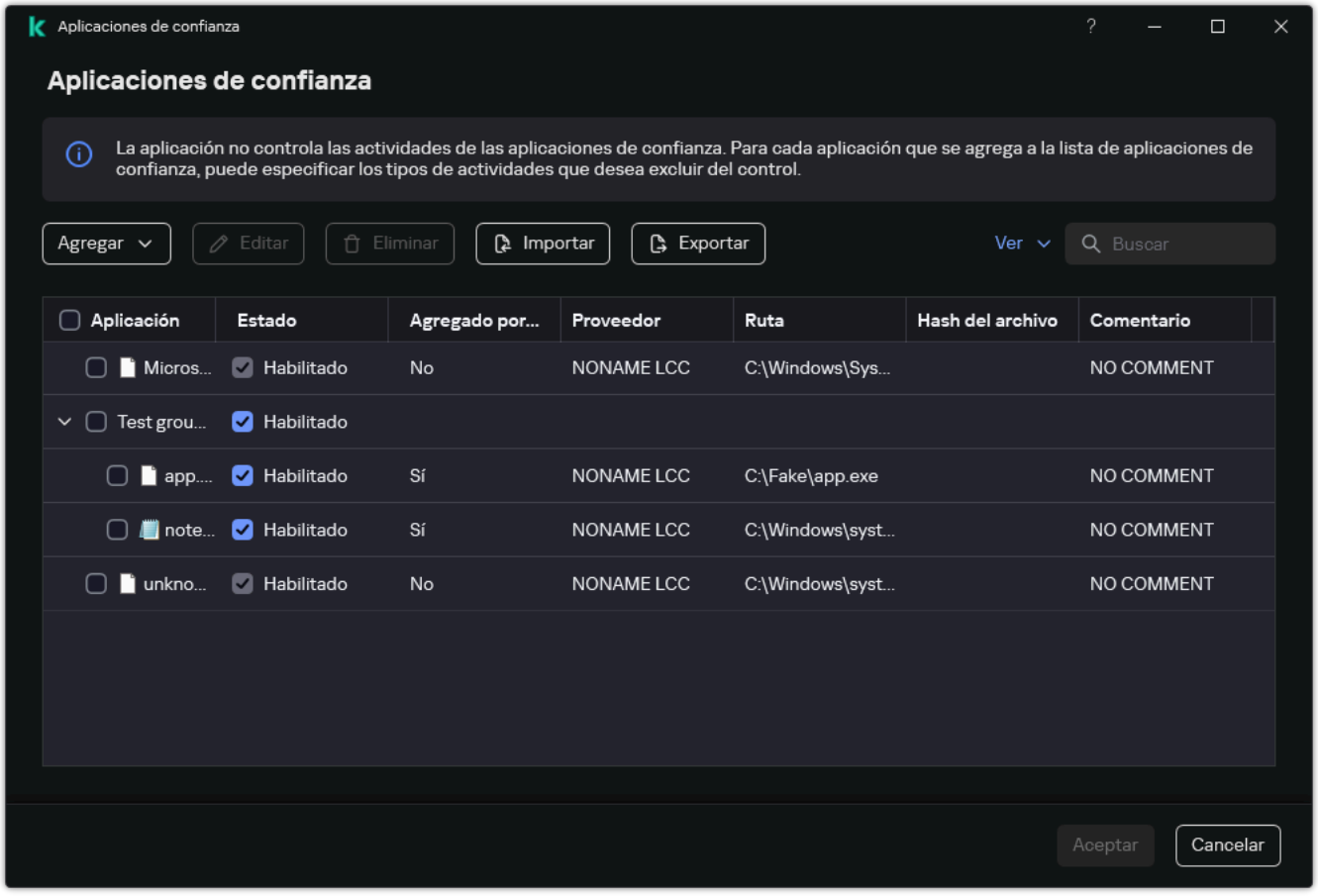
Kaspersky Endpoint Security es compatible con variables de entorno y convierte la ruta en la interfaz local de la aplicación. Es decir, si ingresa la ruta de archivo `%userprofile%\Documents\File.exe`, se agregará un registro `C:\Users\Fred123\Documents\File.exe` en la interfaz local de la aplicación para el usuario Fernando123. De forma similar, Kaspersky Endpoint Security omite el programa de confianza `File.exe` para otros usuarios. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, defina la configuración avanzada.

7. Haga clic en **Aceptar**.

   La nueva aplicación de confianza se agregará 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

Exportar e importar la zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurados 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. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de exclusiones del mismo tipo. También puede usar 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), en Web Console y en 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 Web Console.
- CSV solo está disponible en la interfaz local de la aplicación.

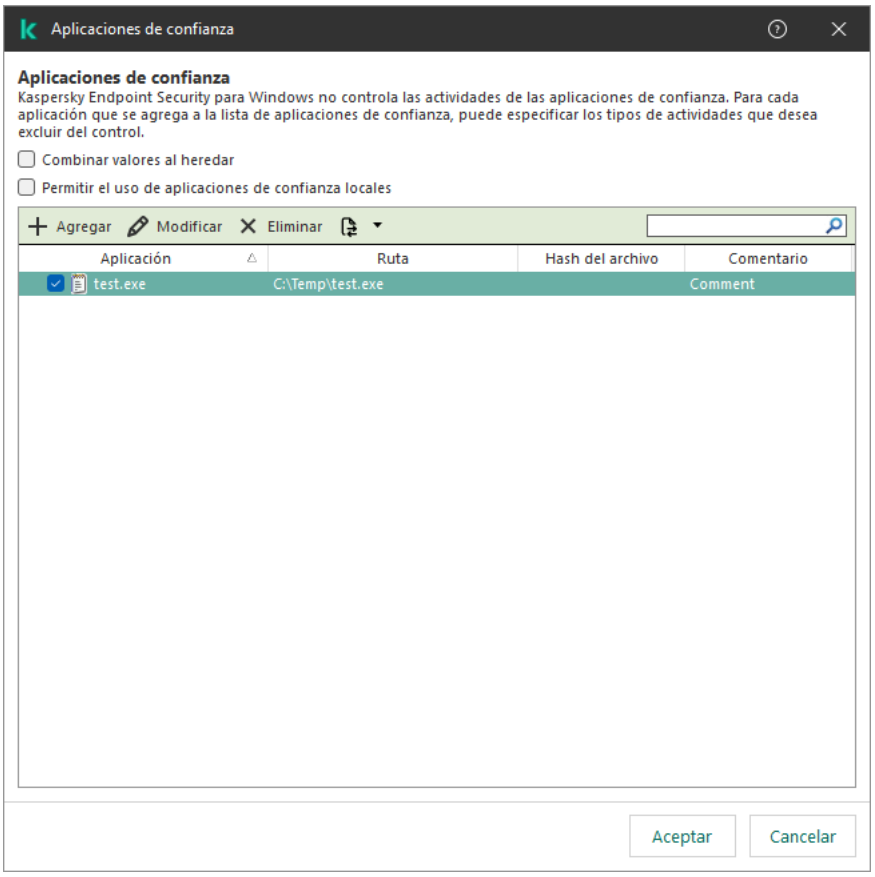
Kaspersky Endpoint Security utiliza el formato XML para exportar e importar la *lista de aplicaciones de confianza*.

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 correspondiente 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 objetos**.
4. En **Exclusiones de análisis y aplicaciones de confianza**, seleccione el componente de la zona de confianza que desee exportar o importar: **Exclusiones de 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, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

d. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de exclusiones completa al archivo XML.
Kaspersky Endpoint Security también permite exportar 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 que se usará para importar la lista de exclusiones.

   c. Abra el archivo.

   Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML. Kaspersky Endpoint Security también permite importar una lista de exclusiones desde un archivo DAT.

8. Guarde los cambios.

Cómo exportar o 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 ficha **Configuración de la aplicación**.

4. Vaya a la sección **Zona de confianza**.

5. Para exportar la lista de reglas:

   a. Haga clic en el vínculo **Exclusiones del análisis de malware**.

   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 desea 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 vínculo **Exclusiones del análisis de malware**.

   b. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON que se usará para importar la lista de exclusiones.

   c. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

8. Para importar una lista de aplicaciones de confianza:

   a. Haga clic en el vínculo **Aplicaciones**.

   b. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo JSON que se usará para importar la lista de aplicaciones de confianza.

   c. Abra el archivo.

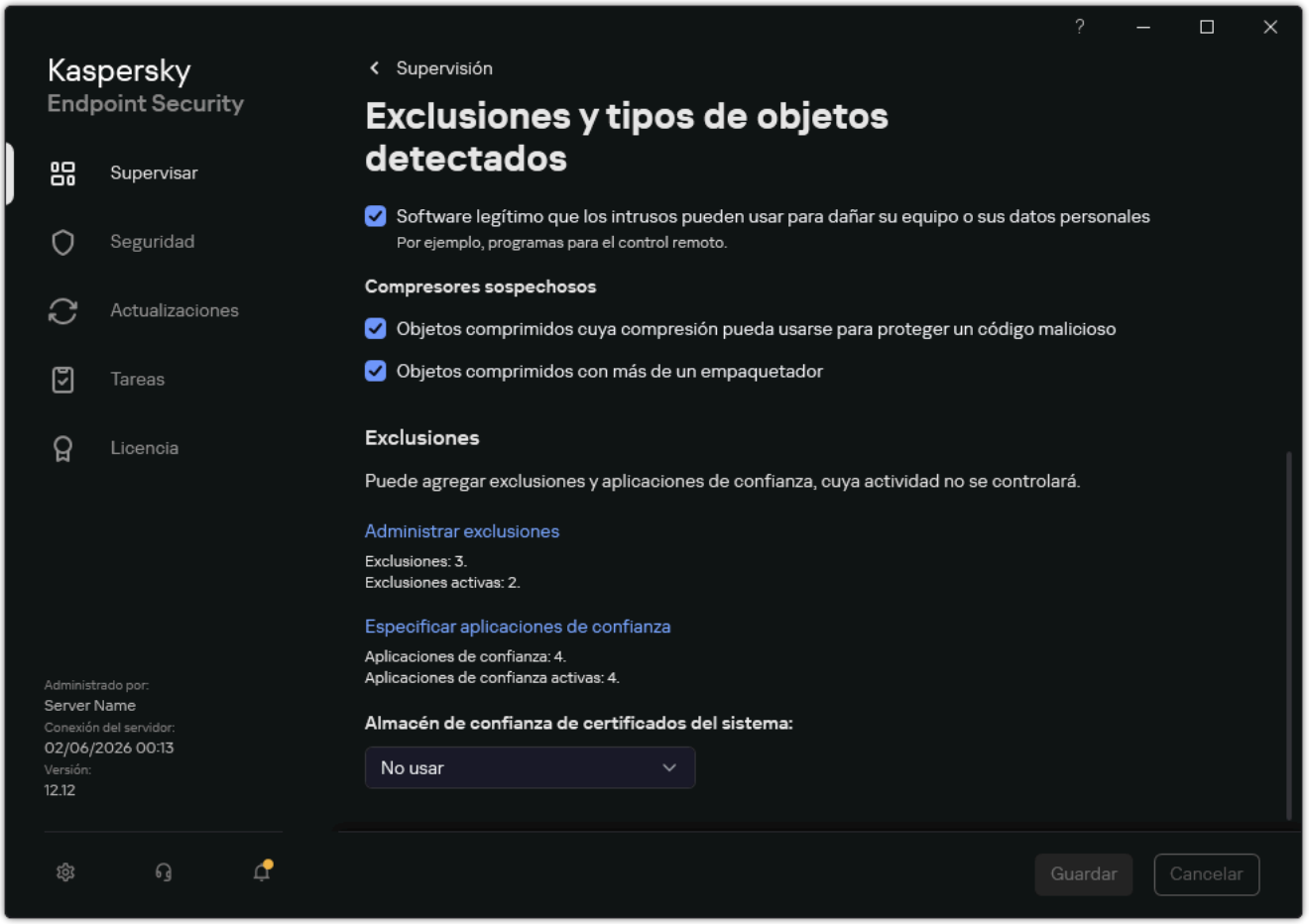
      Cuando ya exista una lista de aplicaciones de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas nuevas del archivo JSON.

9. Guarde los cambios.

Cómo exportar o importar la zona de confianza en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 vínculo **Administrar exclusiones**.

   b. Seleccione las exclusiones que desea exportar.

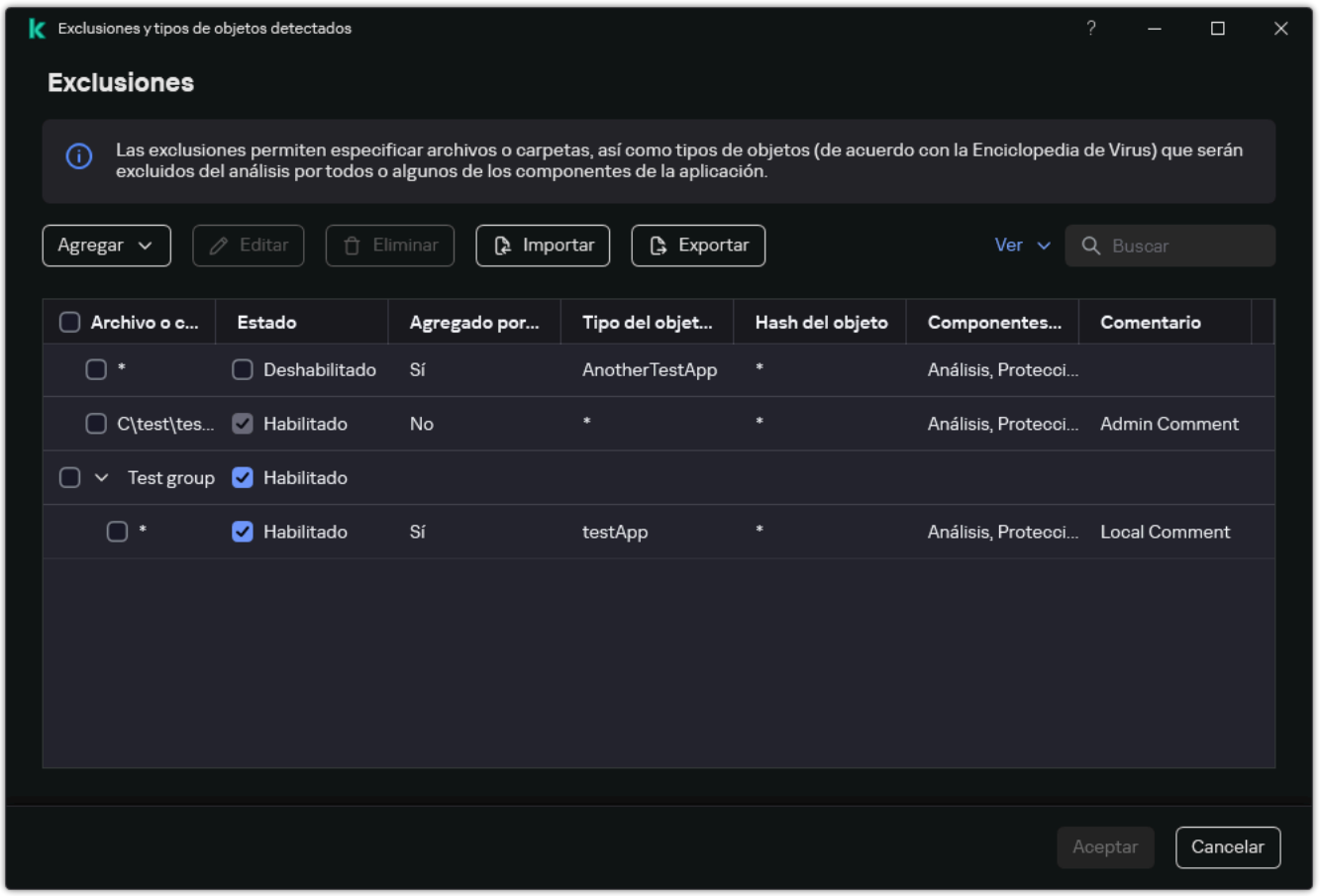
   c. Haga clic en **Exportar**.

   d. Confirme que desea exportar solo las exclusiones seleccionadas, o bien exporte la lista completa de exclusiones.

   e. En la ventana que se abre, escriba el nombre del archivo CSV en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

f. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de exclusiones completa al archivo CSV.



Lista de exclusiones

4. Para exportar la lista de aplicaciones de confianza:

   a. En el bloque **Exclusiones**, haga clic en el vínculo **Especificar aplicaciones de confianza**.

   b. Seleccione las aplicaciones de confianza que desea exportar.

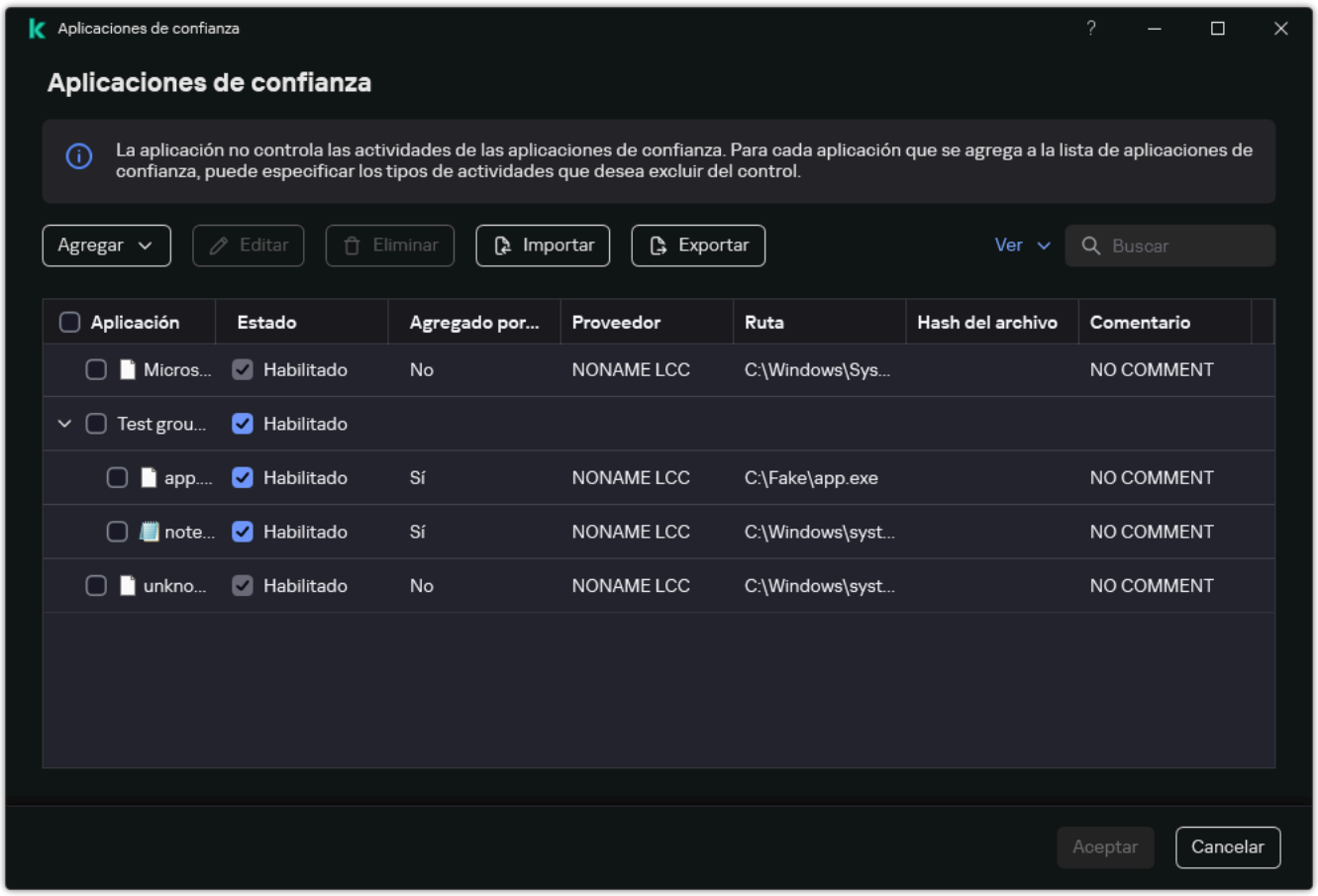
   c. Haga clic en **Exportar**.

   d. Confirme que desea exportar solo las aplicaciones de confianza seleccionadas, o bien exporte la lista completa.

   e. En la ventana que se abre, ingrese el nombre del archivo XML en el que se exportará la lista de aplicaciones de confianza. Seleccione la carpeta en la que se guardará este archivo.

f. Guarde el archivo.

Kaspersky Endpoint Security exportará la lista de aplicaciones de confianza completa al archivo XML.



Lista de aplicaciones de confianza

5. Para importar la lista de exclusiones:

   a. En el bloque **Exclusiones**, haga clic en el vínculo **Administrar exclusiones**.

   b. Haga clic en **Importar**.

   c. En la ventana que se abre, seleccione el archivo CSV que se usará para importar la lista de exclusiones.

   d. Abra el archivo.

   Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo CSV.

6. Para importar una lista de aplicaciones de confianza:

   a. En el bloque **Exclusiones**, haga clic en el vínculo **Especificar aplicaciones de confianza**.

   b. Haga clic en **Importar**.

   c. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de aplicaciones de confianza.

d. Abra el archivo.

Cuando ya exista una lista de aplicaciones de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas nuevas del archivo XML.

7. Guarde los cambios.

Administrar aplicaciones con una firma digital de confianza

Utilizar el almacenamiento de certificados de sistema le permite excluir aplicaciones firmadas con una firma digital de confianza del análisis antivirus. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al grupo *De confianza*.

Cómo iniciar el uso de un almacén 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 correspondiente 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 objetos**.
4. En el bloque **Almacén de confianza de certificados del sistema**, seleccione la casilla **Usar un almacén de confianza de certificados del sistema**.
5. En la lista desplegable, seleccione qué almacén del sistema debe ser considerado como de confianza por Kaspersky Endpoint Security.
6. Guarde los cambios.

Cómo iniciar el uso de un almacén 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 ficha **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 de confianza**.
6. En la ventana que se abre, seleccione la casilla **Usar un almacén de confianza de certificados del sistema**.
7. Seleccione qué almacén del sistema debe considerar Kaspersky Endpoint Security como de confianza.
8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo iniciar el uso de un almacén de certificados del sistema de confianza en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 qué almacén del sistema debe ser considerado como de confianza por Kaspersky Endpoint Security.
4. Guarde los cambios.

Apéndice. Exclusiones de análisis y aplicaciones de confianza predefinidas

A partir de Kaspersky Endpoint Security 12.6 para Windows, las exclusiones de análisis y aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 el modo de Light Agent para proteger entornos virtuales. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de Citrix y VMware.

Puede seleccionar exclusiones predefinidas y aplicaciones de confianza de las siguientes formas:

- Instalación de la aplicación.
  - Instalación local a través del Asistente
  - Propiedades del paquete de instalación
- Configuración de la política.
  - Asistente para nuevas directivas
  - Propiedades de la directiva: exclusiones de análisis y aplicaciones de confianza

Servidor SQL

Durante la instalación de Kaspersky Endpoint Security en un servidor SQL, debe crear una zona de confianza a partir de exclusiones y aplicaciones de confianza 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

Servidor Microsoft Exchange

Durante la instalación de Kaspersky Endpoint Security en un servidor de Microsoft Exchange, debe crear una zona de confianza a partir de exclusiones y aplicaciones de confianza 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

System Center Configuration Manager

Exclusiones de análisis predefinidas

Ruta	Versión de System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Durante la instalación de Kaspersky Endpoint Security en un entorno virtual de 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.

Exclusiones de análisis predefinidas

Ruta
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf

Ruta
%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
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Aplicaciones de confianza predefinidas

Ruta	Solución de
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Aplicacior escritor virtuale
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Aplicacior escritor virtuale

Ruta	Solución de
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Aplicacior escritor virtuale
%SystemRoot%\System32\drivers\CVhdFilter.sys	Aplicacior escritor virtuale
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Aplicacior escritor virtuale
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Aplicacior escritor virtuale
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Aplicacior escritor virtuale
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Aplicacior escritor virtuale
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Aplicacior escritor virtuale
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Aplicacior escritor virtuale

Ruta	Solución de
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Aplicacior escritor virtuale
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Aplicació espacio de t
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Aplicació espacio de t
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Aprovisiona
%SystemRoot%\System32\drivers\bnistack6.sys	Aprovisiona
%SystemRoot%\System32\drivers\CfsDep2.sys	Aprovisiona
%SystemRoot%\System32\drivers\cnicteam.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Aprovisiona
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFr
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFr

VMware

Durante la instalación de 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 de 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
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

Ruta	Solución de VMware
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

Administración del Depósito de copias de seguridad

El depósito *Copia de seguridad* contiene copias de respaldo de los archivos que se modifican o eliminan cuando se realiza una desinfección. Una *copia de seguridad* es una copia del archivo creada antes de desinfectar o eliminar el archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. Se conceden accesos limitados a esta carpeta al usuario cuya cuenta se utilizó para instalar Kaspersky Endpoint Security.

Kaspersky Endpoint Security no brinda la capacidad de configurar permisos de acceso de usuario a copias de seguridad de archivos.

A veces no es posible mantener la integridad de los archivos durante la desinfección. Si después de la desinfección pierde acceso total o parcial a información importante del archivo desinfectado, puede intentar restaurar el archivo desde su copia de seguridad a su carpeta original.

Si Kaspersky Endpoint Security se está ejecutando bajo la administración 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 administración de las copias de seguridad en Kaspersky Security Center, consulte la sección de ayuda de Kaspersky Security Center.

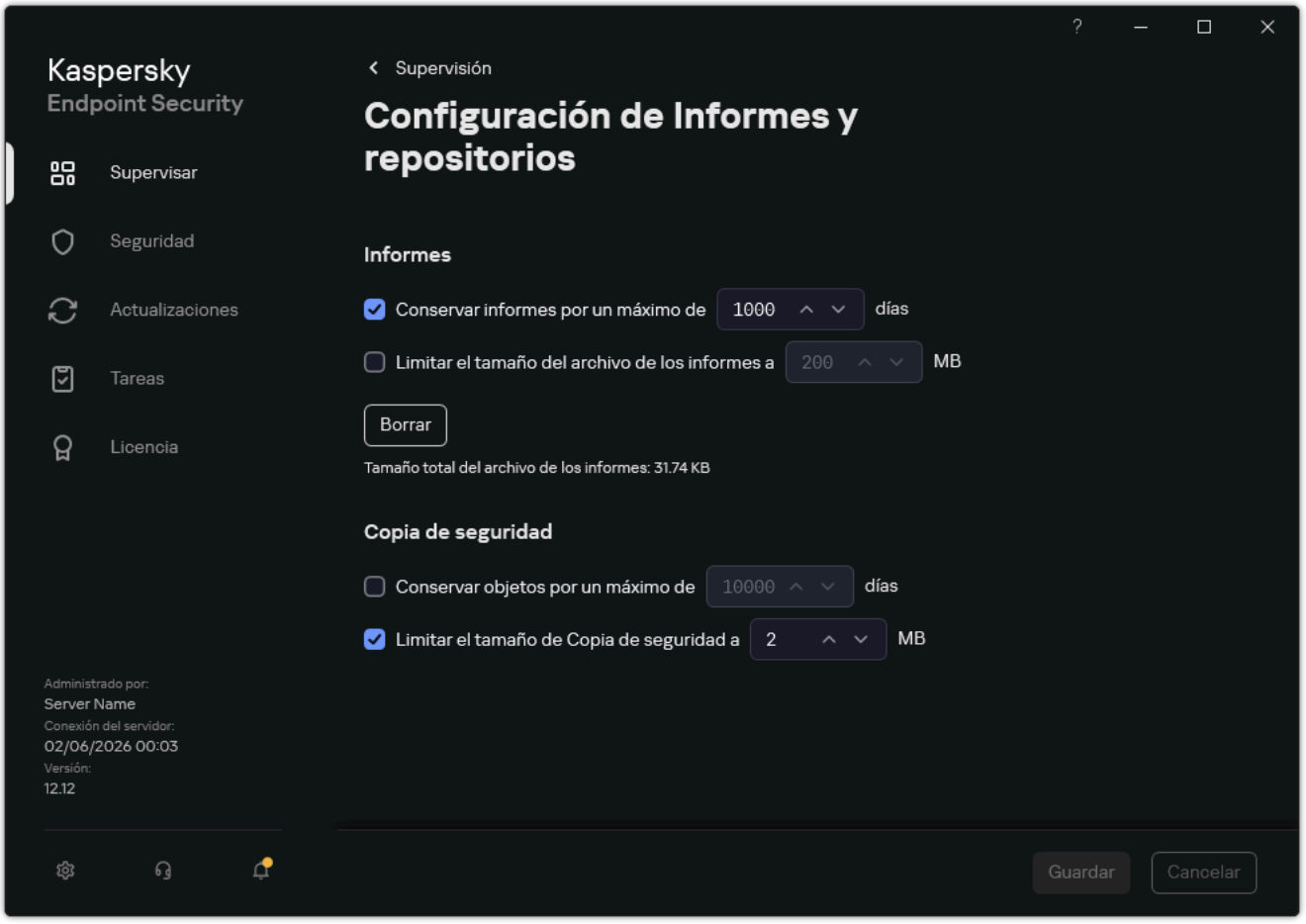
Configuración del período de almacenamiento máximo de los archivos en Copias de seguridad

De manera predeterminada, el plazo máximo de almacenamiento de las copias de archivos en Copias de seguridad es de 30 días. Al caducar el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos de Copia de seguridad.

Para configurar el período de almacenamiento máximo de los archivos en Copias de seguridad, realice lo siguiente:

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

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el ícono **Informes y repositorios**.



Opciones de copia de seguridad

3. Si desea limitar el período de almacenamiento para las copias de archivos en Copia de seguridad, seleccione la casilla **Conservar objetos por un máximo de N días** en el bloque **Copia de seguridad**. Ingrese la duración máxima de almacenamiento de las copias de archivos en Copia de seguridad.

4. Guarde los cambios.

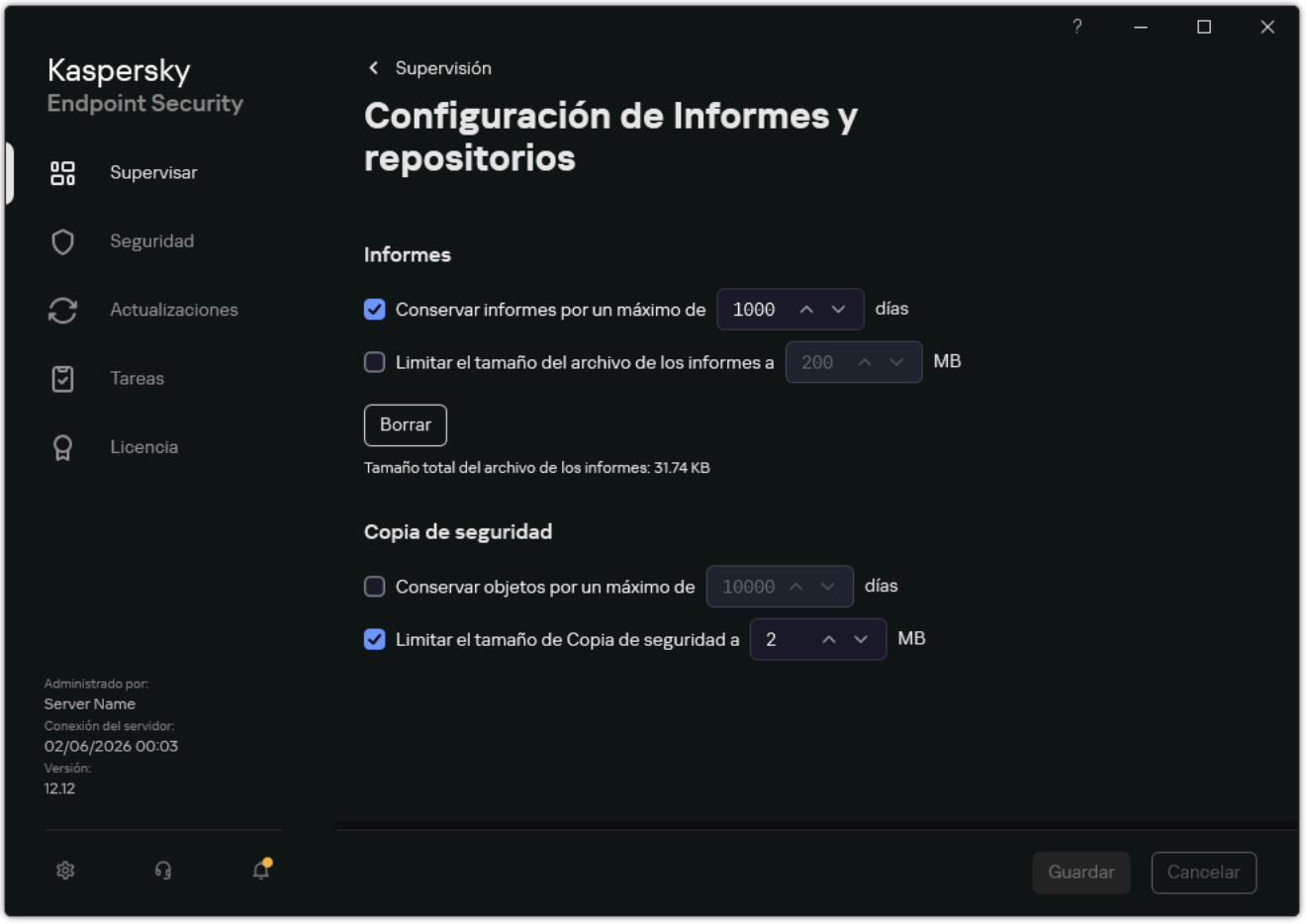
Configuración del tamaño máximo de Copias de seguridad

Puede especificar el tamaño máximo de Copia de seguridad. El tamaño de Copias de seguridad es ilimitado de forma predeterminada. Una vez alcanzado el tamaño máximo, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos de Copias de seguridad.

Para configurar el tamaño máximo de Copias de seguridad, realice lo siguiente:

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

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el ícono **Informes y repositorios**.



Opciones de copia de seguridad

3. En el bloque **Copia de seguridad**, seleccione la casilla **Limitar el tamaño de Copia de seguridad a N MB**. Si la casilla está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo 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 desde copias de seguridad

Si se detecta código malicioso en el archivo, Kaspersky Endpoint Security bloquea el archivo, le asigna el estado *No desinfectados*, coloca una copia en Copia de seguridad e intenta desinfectarlo. Si se lleva a cabo una desinfección de un archivo, el estado de la copia de seguridad del archivo cambia a *Desinfectado*. El archivo queda disponible en su carpeta original. Si no se puede desinfectar un archivo, Kaspersky Endpoint Security lo elimina de su carpeta original. Puede restaurar el archivo de su copia de seguridad a su carpeta original.

Los archivos de estado *Se eliminará al reiniciar el equipo* no se pueden restaurar. Reinicie el equipo para que el estado cambie a *Desinfectado* o *Eliminados*. Si tiene una copia de seguridad del archivo, puede restaurarla a su carpeta original.

Después de detectar código malintencionado en un archivo que es parte de la aplicación Tienda Windows, Kaspersky Endpoint Security inmediatamente elimina el archivo sin pasar una copia a Copia de seguridad. Puede restaurar la integridad de la aplicación de la Tienda Windows con las herramientas adecuadas del sistema operativo (consulte los archivos de ayuda de Microsoft Windows para obtener información sobre la restauración de una aplicación de la Tienda Windows).

El conjunto de copias de seguridad de los archivos se presenta en forma de 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.

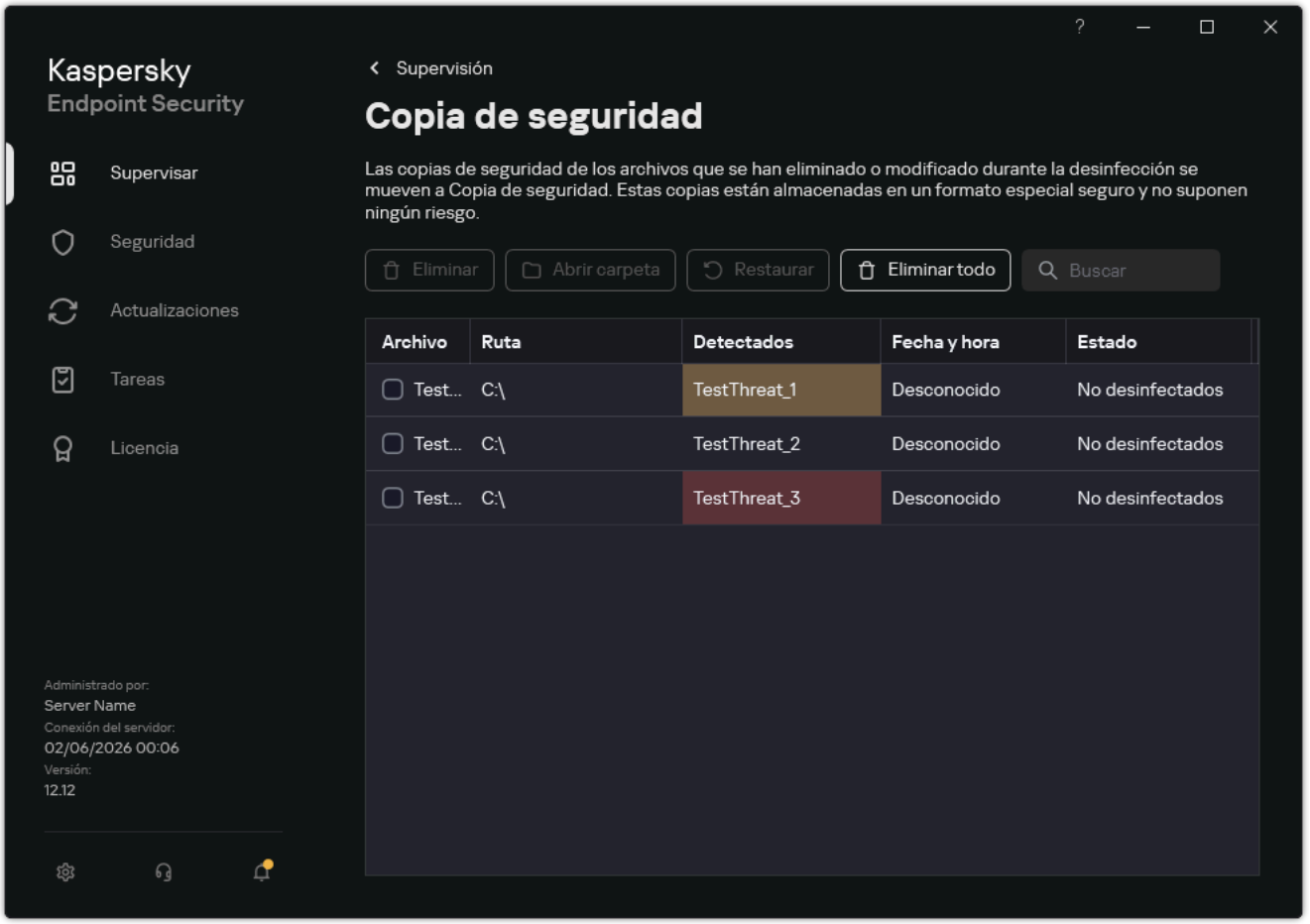
Si varios archivos con nombres idénticos y contenido diferente localizados en la misma carpeta se mueven a Copias de seguridad, solamente se podrá restaurar el archivo que se movió en último lugar a Copias de seguridad.

Para restaurar los archivos desde el Depósito de copias de seguridad:

1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Copia de seguridad**.

2. Se abre la lista de archivos en Copia de seguridad; y en dicha lista, seleccione los archivos que desea restaurar y haga clic en **Restaurar**.

Kaspersky Endpoint Security restaura archivos desde las copias de seguridad seleccionadas a sus carpetas originales.



Copias de seguridad

Eliminar copias de seguridad de archivos de Copias de seguridad

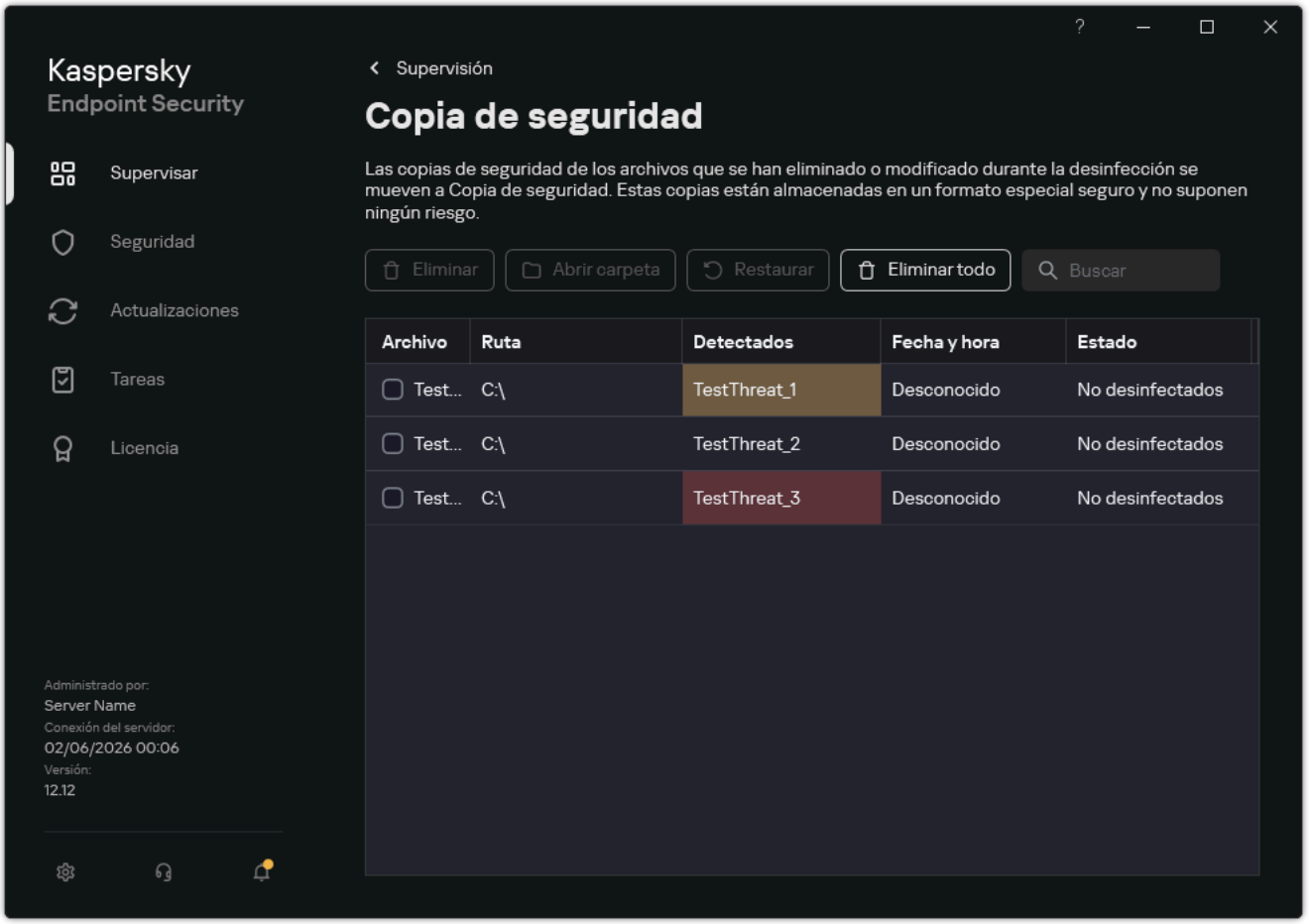
Una vez transcurrido el plazo de almacenamiento definido en la configuración de la aplicación, Kaspersky Endpoint Security elimina automáticamente las copias de seguridad de los archivos con cualquier estado. También puede eliminar manualmente de Copias de seguridad cualquier copia de un archivo.

Para eliminar copias de seguridad de archivos desde el Depósito de copias de seguridad:

1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Copia de seguridad**.

2. Se abre la lista de archivos en Copia de seguridad; y en dicha lista, seleccione los archivos que desea eliminar de Copia de seguridad y haga clic en **Eliminar**.

Kaspersky Endpoint Security elimina todas las copias de seguridad de archivos seleccionadas del Depósito de copias de seguridad.



Copias de seguridad

Servicio de notificación

Se producen todo tipo de eventos durante el funcionamiento de Kaspersky Endpoint Security. Las notificaciones de estos eventos pueden ser puramente informativas o contener información crítica. Por ejemplo, una notificación puede sencillamente informar que las bases de datos y los módulos se han actualizado correctamente, o puede dar aviso de un problema en un componente que deba resolverse.

Kaspersky Endpoint Security admite el registro de información sobre eventos en la operación del registro de aplicación de Microsoft Windows o el registro de eventos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security proporciona notificaciones de las siguientes maneras:

- usando notificaciones emergentes en el área de notificaciones de la barra de tareas de Microsoft Windows;
- por correo electrónico.

Puede configurar la entrega de notificaciones de eventos. El método de entrega de notificación se configura para cada tipo de evento.

Cuando usa la tabla de eventos para configurar el servicio de notificaciones, puede realizar las siguientes acciones:

- Filtrar eventos de servicio de notificación mediante el valor de columna o con condiciones de filtros personalizadas.
- Usar la función de búsqueda para eventos de servicio de notificación.
- Ordenar eventos de servicios de notificación.
- Cambiar el orden y el conjunto de columnas que se muestran en la lista de eventos de servicio de notificación.

Configuración de los parámetros del registro de eventos

Para configurar los parámetros del registro de eventos:

1. En la ventana principal de la aplicación 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 las notificaciones**.

   Los componentes y las tareas de Kaspersky Endpoint Security se muestran en la parte izquierda de la ventana. En la parte derecha de la ventana se enumeran los eventos generados para la tarea o el componente seleccionado.

   Los Eventos pueden contener los siguientes datos del usuario:

   - Rutas a archivos analizados por Kaspersky Endpoint Security.
   - Rutas a claves del Registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.

- Nombre de usuario de Microsoft Windows.
- Las direcciones de páginas web abiertas por el usuario.

4. En la parte izquierda de la ventana, seleccione el componente o la tarea para el cual desea configurar los parámetros del registro de eventos.
5. En las columnas **Guardar en informe local** y **Guardar en Registro de eventos de Windows**, seleccione las casillas ubicadas junto a los eventos que le resulten pertinentes.

   Los eventos cuyas casillas están seleccionadas en la columna **Guardar en informe local** se muestran en los application logs. Los eventos que tienen seleccionada la casilla de 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 el envío de notificaciones

Para configurar la visualización y el envío de notificaciones:

1. En la ventana principal de la aplicación 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 las notificaciones**.

   Los componentes y las tareas de Kaspersky Endpoint Security se muestran en la parte izquierda de la ventana. En la parte derecha de la ventana se enumeran los eventos generados para la tarea o el componente seleccionado.

   Los Eventos pueden contener los siguientes datos del usuario:

   - Rutas a archivos analizados por Kaspersky Endpoint Security.
   - Rutas a claves del Registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
   - Nombre de usuario de Microsoft Windows.
   - Las direcciones de páginas web abiertas por el usuario.
4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los cuales desea configurar el envío de notificaciones.
5. En la columna **Notificar en pantalla**, seleccione las casillas junto a eventos relevantes.

   La información acerca de los eventos seleccionados se muestra en la pantalla como mensajes emergentes en el área de notificación de la barra de tareas de Microsoft Windows.
6. En la columna **Notificar por correo electrónico**, seleccione las casillas junto a eventos relevantes.

   La información sobre los eventos seleccionados se entrega por correo electrónico si se configuraron los parámetros de entrega de notificaciones por correo.
7. Haga clic en **Aceptar**.

8. Si habilitó las notificaciones por correo electrónico, defina la configuración para la entrega de correo electrónico:

   a. Haga clic en **Configurar las notificaciones de correo electrónico**.

   b. Seleccione la casilla **Notificar sobre eventos** para habilitar el envío de notificaciones sobre los eventos de Kaspersky Endpoint Security seleccionados en la columna **Notificar por correo electrónico**.

   c. Especifique los parámetros de envío de notificaciones por correo electrónico.

   d. Haga clic en **Aceptar**.

9. Guarde los cambios.

Configuración de la visualización de advertencias acerca del estado de la aplicación en el área de notificación

Para configurar la visualización de advertencias acerca del estado de la aplicación en el área de notificación:

1. En la ventana principal de la aplicación 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 que se encuentran frente a las categorías de eventos de los que quiere ver notificaciones en el área de notificación de Microsoft Windows.

4. Guarde los cambios.

Cuando se registren eventos asociados con las categorías seleccionadas, el icono de la aplicación en el área de notificación pasará a o a , en función de la gravedad de la advertencia.

Comunicación entre el administrador y los usuarios

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 tenga que enviar un mensaje al administrador de la red corporativa local en los siguientes casos:

- El 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 una solicitud de permiso para iniciar una aplicación bloqueada está disponible en la interfaz de Kaspersky Endpoint Security, en la sección Control de aplicaciones.

- El Control web bloqueó el acceso a un recurso web.

  La plantilla del mensaje para una solicitud de 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 se está ejecutando una directiva Kaspersky Security Center activa en el equipo que tiene Kaspersky Endpoint Security instalado, y de si hay una conexión con el Servidor de administración de Kaspersky Security Center. Pueden darse las siguientes situaciones:

- Cuando el equipo con Kaspersky Endpoint Security no se encuentra sujeto a una directiva de Kaspersky Security Center, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

  Los campos del mensaje se completan con los valores de los campos de la plantilla definida en la interfaz local de Kaspersky Endpoint Security.

- Cuando el equipo con Kaspersky Endpoint Security se encuentra sujeto a una directiva de Kaspersky Security Center, se envía un mensaje estándar al Servidor de administración de Kaspersky Security Center.

  En este caso, el administrador encontrará los mensajes de los usuarios en el repositorio de eventos de Kaspersky Security Center (vea las instrucciones para acceder a estos mensajes más abajo). Los campos del mensaje se completan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

- Si se está ejecutando una directiva por ausencia de la oficina de Kaspersky Security Center en el equipo con Kaspersky Endpoint Security instalado, el método usado para enviar mensajes depende de si hay 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 no hay ninguna conexión con Kaspersky Security Center, el mensaje de un usuario se envía al administrador de la red de área local por correo electrónico.

  En ambos casos, los campos del mensaje se completan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

Para visualizar el mensaje de un usuario en el almacenamiento de eventos de Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la pestaña **Eventos**.

   En el espacio de trabajo de Kaspersky Security Center se muestran todos los eventos que ocurren durante el funcionamiento de Kaspersky Endpoint Security, incluidos los mensajes al administrador que se reciben de usuarios de la red LAN.

3. Para configurar el filtro de eventos, en la lista desplegable **Selecciones de eventos**, seleccione **Solicitudes de usuario**.

4. Seleccione el mensaje enviado al administrador.

5. Haga clic en el botón **Abrir ventana de propiedades del evento** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

Administración 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.14.1\Report`.

Los Informes pueden contener los siguientes datos del usuario:

- Rutas a archivos analizados por Kaspersky Endpoint Security.
- Rutas a claves del Registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
- Nombre de usuario de Microsoft Windows.
- Las direcciones de páginas web abiertas por el usuario.

Los datos de un informe se presentan en forma de tabla. Cada fila de la tabla contiene información sobre un evento individual. Los atributos del evento se ubican en las columnas de la tabla. Ciertas columnas son compuestas y contienen columnas anidadas con atributos adicionales. Para ver los atributos adicionales, haga clic en el botón ⊞ que verá junto al nombre de la columna. Los eventos registrados mientras los distintos componentes o las distintas tareas están en ejecución poseen diferentes conjuntos de atributos.

Están disponibles los siguientes informes:

- Informe de **Auditoría del sistema**. Contiene información sobre eventos que ocurren durante la interacción entre el usuario y la aplicación y en el transcurso del funcionamiento de la aplicación en general, que no están relacionados con ningún componente ni tarea en particular de Kaspersky Endpoint Security.
- Informes sobre el funcionamiento de los componentes de Kaspersky Endpoint Security.
- Informes de las tareas de Kaspersky Endpoint Security.
- Informe de **Cifrado de datos**. Contiene información sobre eventos que ocurren durante el cifrado y descifrado de datos.

En los informes se usan los siguientes niveles de importancia de eventos:

ⓘ **Mensajes informativos**. Eventos informativos que normalmente no contienen información importante.

⚠ **Advertencias**. Eventos que requieren atención dado que reflejan situaciones importantes relacionadas con el funcionamiento de Kaspersky Endpoint Security.

⊘ **Eventos críticos**. Eventos de importancia crítica que indican problemas en el funcionamiento de Kaspersky Endpoint Security o vulnerabilidades en la protección del equipo del usuario.

Para el procesamiento conveniente de los informes, es posible modificar la presentación de los datos en la pantalla de las siguientes formas:

- Filtrar la lista de eventos según distintos criterios.
- Usar la función de búsqueda para encontrar un evento específico.
- Ver el evento seleccionado en una sección separada.
- Ordenar la lista de eventos por cada columna del informe.
- Usar el botón ⊞ para mostrar y ocultar eventos que se hayan agrupado con el filtro de eventos.
- Cambiar el orden y la organización de las columnas que se muestran en el informe.

Puede guardar el informe generado en un archivo de texto, si es necesario. También puede eliminar la información del informe sobre los componentes y las tareas de Kaspersky Endpoint Security que están combinados en grupos.

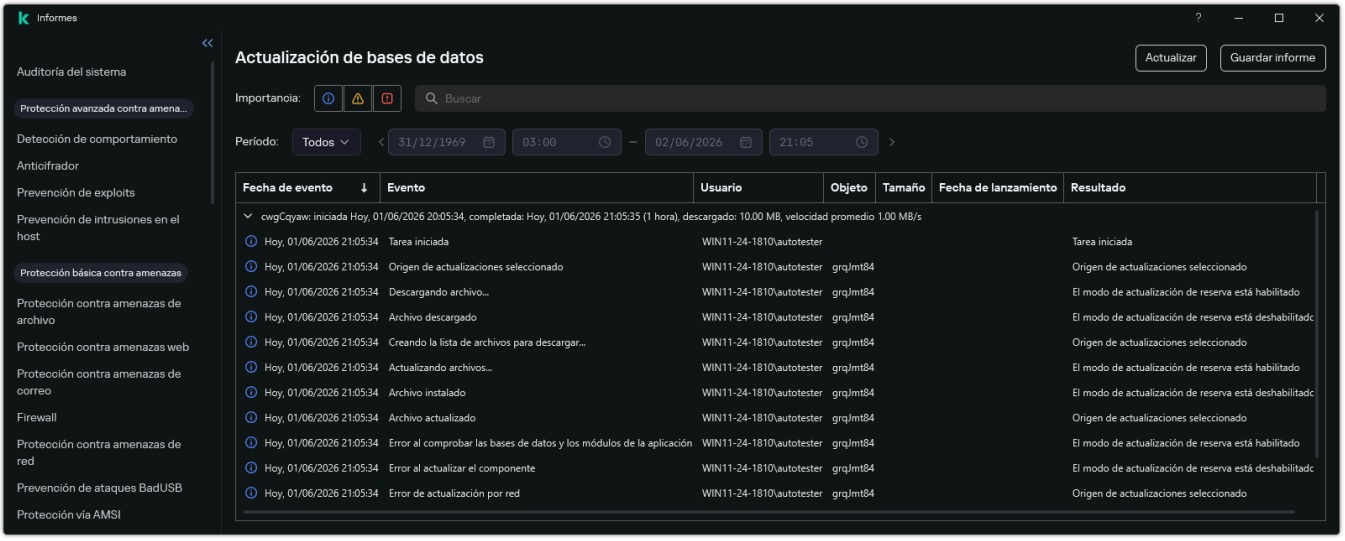
Cuando Kaspersky Endpoint Security se ejecuta bajo la administración de Kaspersky Security Center, puede transmitir información sobre los eventos al Servidor de administración de Kaspersky Security Center (para más detalles, consulte la Ayuda de Kaspersky Security Center).

Cómo acceder a los 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 **Supervisar**, haga clic en el ícono **Informes**.



Informes

2. En la lista de componentes y tareas, seleccione un componente o una tarea.

   La parte derecha de la ventana muestra un informe que contiene una lista de eventos resultantes de la operación del componente o tarea seleccionado de Kaspersky Endpoint Security. Puede clasificar los eventos en el informe utilizando los valores en las celdas de una de las columnas.

3. Para ver los detalles de un evento en particular, seleccione el evento que le interese en el informe.

Se presenta un bloque con el resumen del evento en la parte inferior de la ventana.

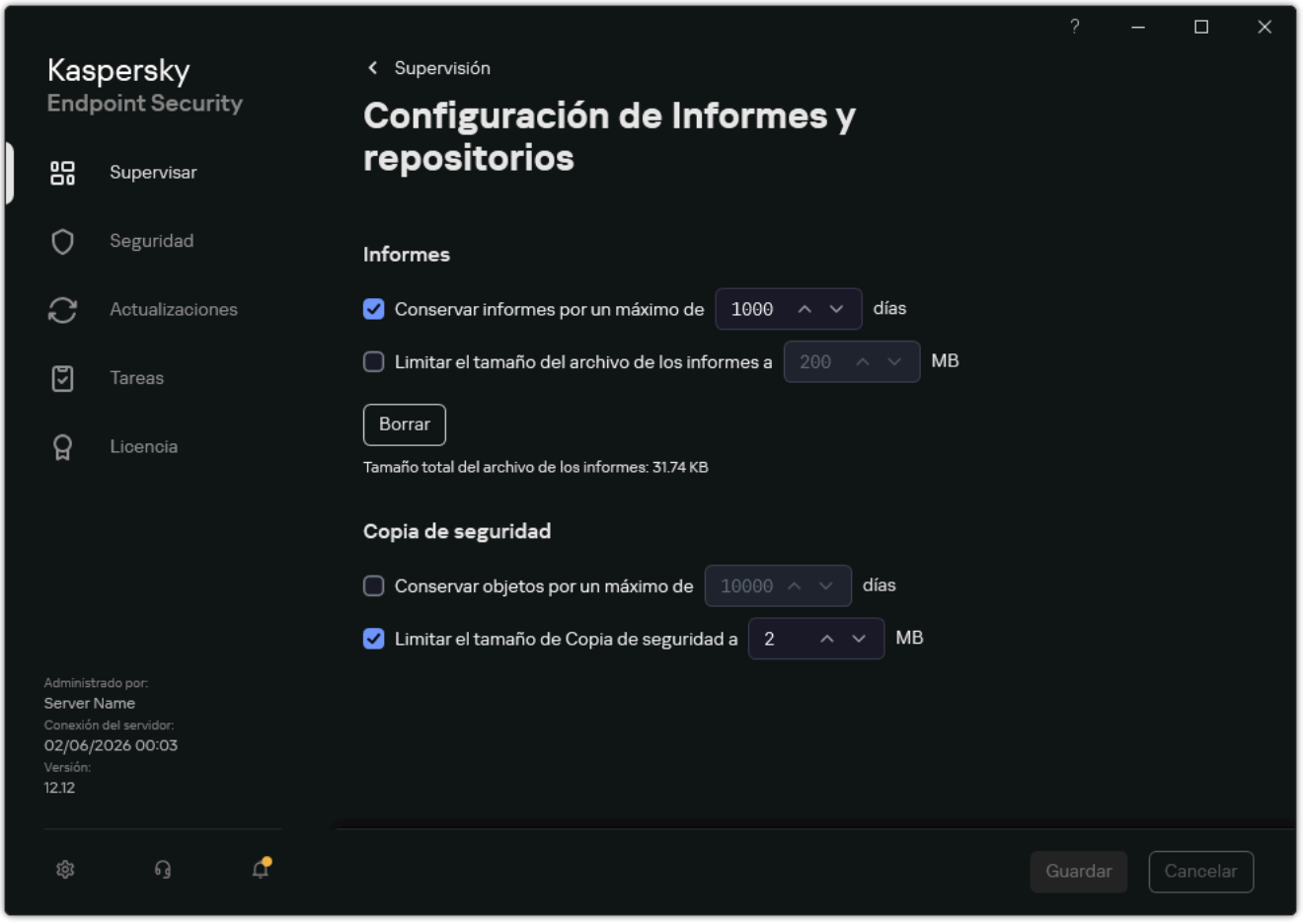
Configuración de la duración máxima del almacenamiento de informes

El plazo de almacenamiento máximo de los informes sobre eventos registrados en Kaspersky Endpoint Security es de 30 días. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.

Para modificar la duración máxima del almacenamiento de informes:

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

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el ícono **Informes y repositorios**.



Configuración del informe

3. Si desea limitar el período de almacenamiento de informes, seleccione la casilla **Conservar informes por un máximo de N días** en el bloque **Informes**. Defina la duración máxima del almacenamiento de informes.

4. Guarde los cambios.

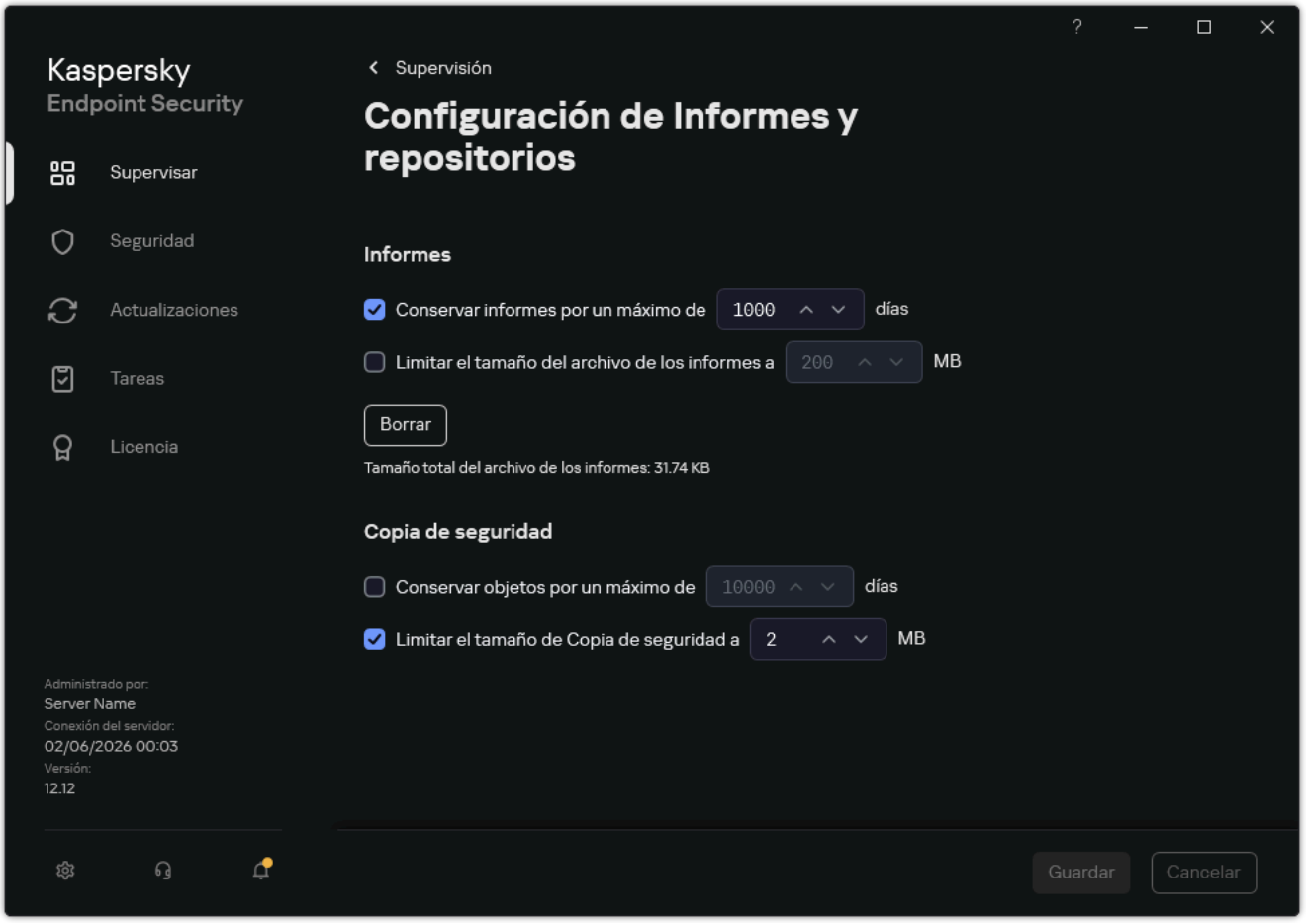
Configuración del tamaño máximo del archivo del informe

Puede especificar el tamaño máximo del archivo que contiene el informe. El tamaño máximo predeterminado del archivo del informe es de 1024 MB. Para evitar que se exceda el tamaño máximo del archivo del informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas de este archivo cuando alcanza el tamaño máximo.

Para configurar el tamaño máximo del archivo del informe:

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

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el ícono **Informes y repositorios**.



Configuración del informe

3. En el bloque **Informes**, seleccione la casilla **Limitar el tamaño del archivo de los informes a N MB** si desea limitar el tamaño de un archivo de informe. Defina el tamaño máximo del archivo del informe.

4. Guarde los cambios.

Almacenamiento de informes en archivos

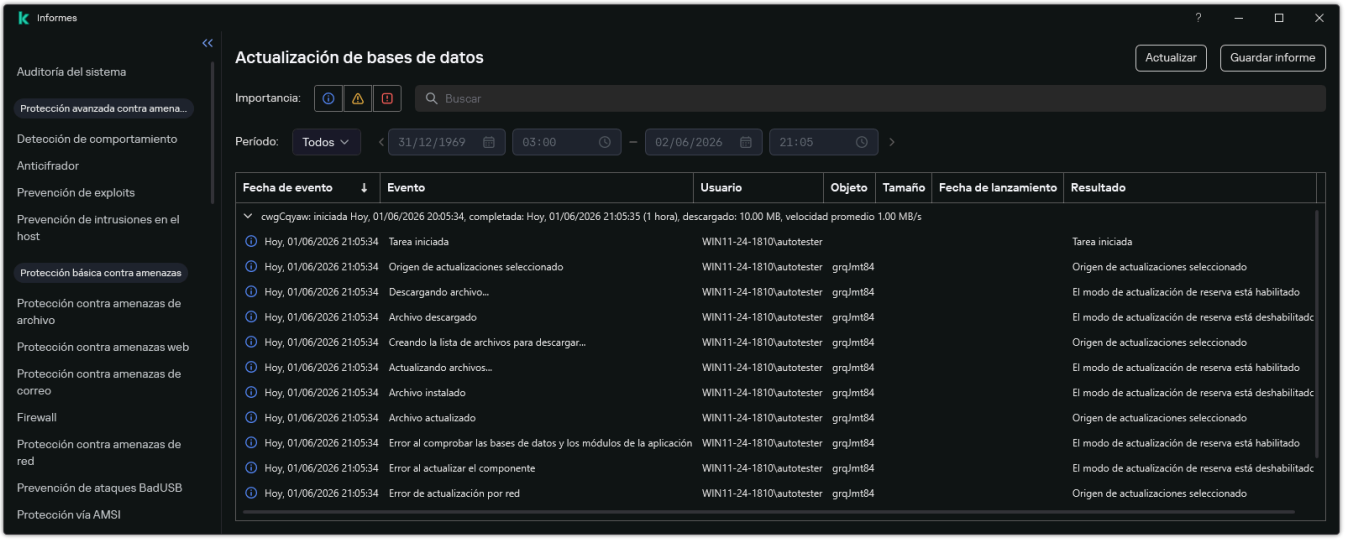
El usuario es responsable personalmente de asegurar la seguridad de la información desde un informe guardado al archivo, y en particular de controlar y restringir el acceso a esta información.

Puede guardar el informe generado en un archivo en formato de texto (TXT) o en un archivo CSV.

Kaspersky Endpoint Security registra los eventos en el informe de la misma manera en la que aparecen en pantalla: en otras palabras, con el mismo conjunto y la misma secuencia de atributos del evento.

Para guardar un informe en un archivo:

1. En la ventana principal de la aplicación, en la sección **Supervisar**, haga clic en el ícono **Informes**.



Informes

2. Se abre una ventana; en esta ventana, seleccione el componente o la tarea.

   Se muestra un informe a la derecha de la ventana, el cual contiene una lista de los eventos que tuvieron lugar durante el funcionamiento del componente o la tarea de Kaspersky Endpoint Security que se hayan seleccionado.

3. Si es necesario, puede modificar la presentación de datos en el informe mediante las siguientes acciones:

   - Filtrar eventos
   - Ejecutar una búsqueda de eventos
   - Reorganizar las columnas
   - Ordenar los eventos

4. Haga clic en el botón **Guardar informe** en la parte derecha de la ventana.

5. En la ventana que se abre, especifique la carpeta de destino para el archivo de informe.

6. Ingrese el nombre del archivo de informe.

7. Seleccione el formato de archivo de informe necesario: TXT o CSV.

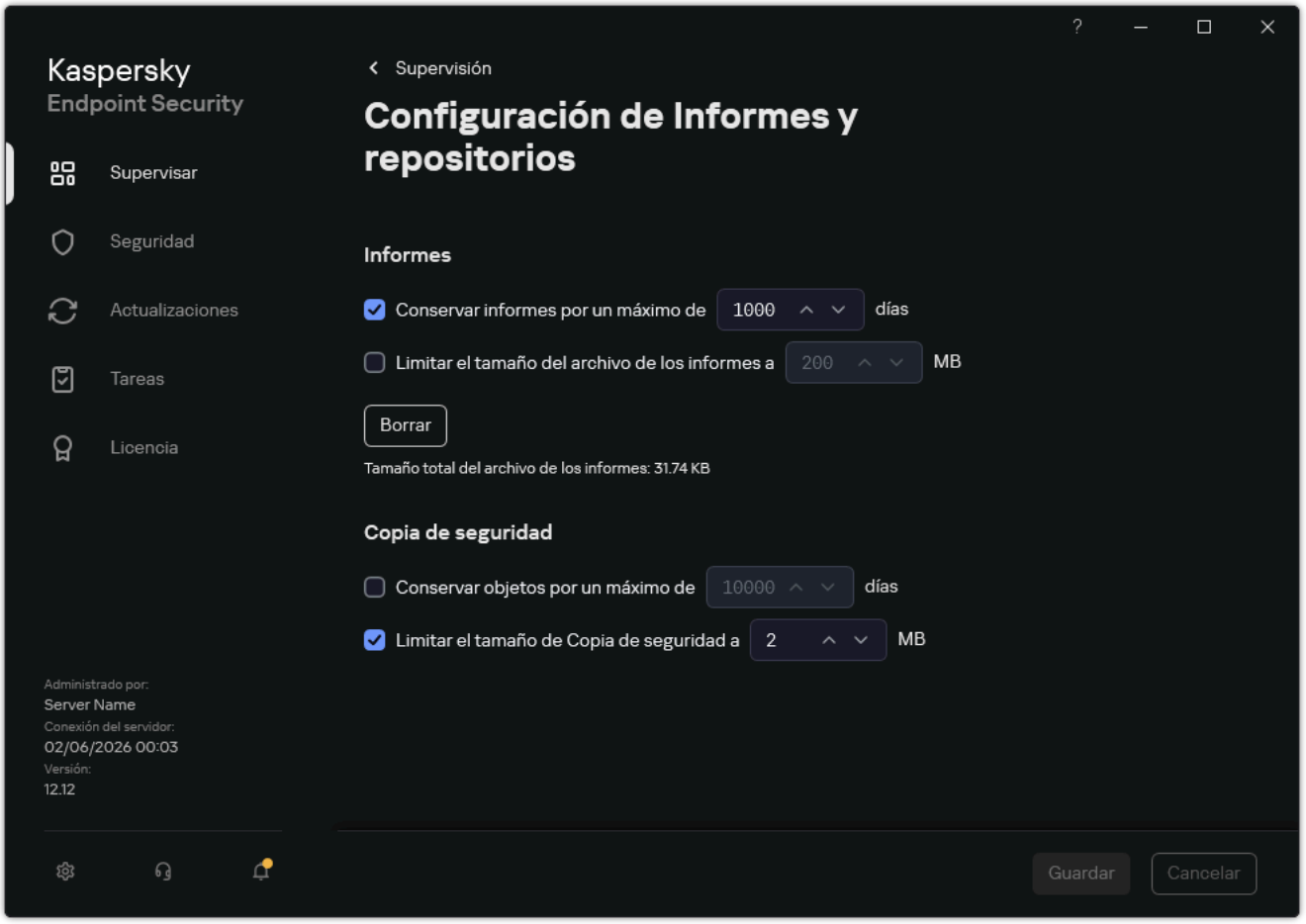
8. Guarde los cambios.

Borrado de informes

Para eliminar información de los informes:

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

2. En la ventana de configuración de la aplicación, en **Configuración general** haga clic en el ícono **Informes y repositorios**.



Configuración del informe

3. En el bloque **Informes**, haga clic en el botón **Borrar**.

4. Si la Protección con contraseña está habilitada, 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 las tareas de la aplicación.

Autoprotección de Kaspersky Endpoint Security

La 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 Autoprotección también incluye protección con contraseña y protección de la conexión del Servidor de administración.

La protección con contraseña permite restringir el acceso a Kaspersky Endpoint Security conforme a los permisos que los usuarios tienen asignados (por ejemplo, el permiso para cerrar 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 evita que los procesos de Kaspersky Endpoint Security se vean afectados por acciones maliciosas. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019.	✓	✓
Mecanismo de protección de administración externa	Esta tecnología evita que otras aplicaciones (por ejemplo, TeamViewer o RemotelyAnywhere) obtengan acceso a Kaspersky Endpoint Security.	✓	– (excepto para Windows 7)

Habilitar y deshabilitar el componente Autoprotección

Kaspersky Endpoint Security impide la alteración y la 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

El mecanismo de Autoprotección de Kaspersky Endpoint Security está habilitado por defecto.

Cómo habilitar o deshabilitar 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 correspondiente 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 **Habilitar la Autoprotección** para habilitar o deshabilitar el mecanismo de autoprotección.
5. Guarde los cambios.

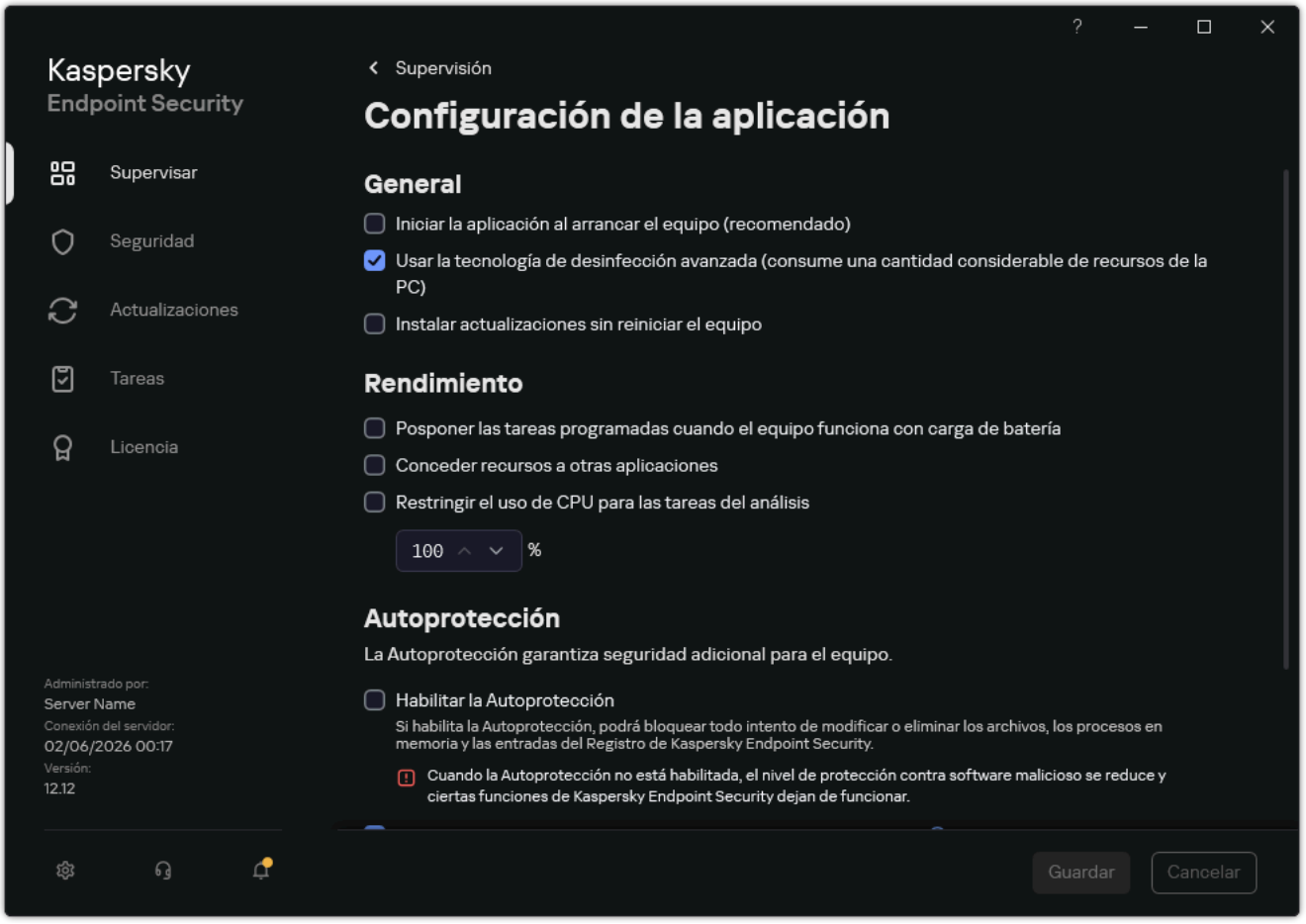
Cómo habilitar o deshabilitar la Autoprotección en Web Console y Cloud Console

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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.
5. Utilice el interruptor **Autoprotección HABILITADA** para habilitar o deshabilitar el mecanismo de Autoprotección.
6. Guarde los cambios.

Cómo habilitar o deshabilitar la Autoprotección en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 **Habilitar la Autoprotección** para habilitar o deshabilitar el mecanismo de autoprotección.

4. Guarde los cambios.

Habilitar y deshabilitar la compatibilidad con AM-PPL

Kaspersky Endpoint Security es compatible con una tecnología de Microsoft denominada Antimalware Protected Process Light (en adelante, "AM-PPL"). AM-PPL evita que los procesos de Kaspersky Endpoint Security se vean afectados por acciones malintencionadas; puede impedir, por ejemplo, el cierre de la aplicación. AM-PPL no permite que un proceso se ejecute si no es de confianza. Los procesos de Kaspersky Endpoint Security, al estar firmados como lo exigen los requisitos de seguridad de Windows, se consideran de confianza. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está habilitada por defecto.

Kaspersky Endpoint Security también cuenta con mecanismos propios para proteger sus procesos. Si opta por utilizar AM-PPL, la protección de los procesos quedará en manos del sistema operativo. Con ello, se reducirá el uso de recursos del equipo y aumentará la velocidad de la aplicación.

Use la tecnología AM-PPL de forma constante. AM-PPL es un componente importante para la protección del sistema operativo. Deshabilitar la compatibilidad con AM-PPL podría causar que fallen algunas funciones de Kaspersky Endpoint Security (por ejemplo, la integración de la aplicación con Windows Security Center). Deshabilitar la compatibilidad con AM-PPL solo se permite en un entorno de prueba por separado para fines de resolución de problemas.

La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019.

Para habilitar o deshabilitar la tecnología AM-PPL:

1. Desactive el mecanismo de Autoprotección de la aplicación.

   El mecanismo de Autoprotección evita que los procesos de la aplicación se modifiquen o se eliminen de la memoria del equipo. Una de las acciones contra las que protege es la modificación del estado de AM-PPL.

2. Abra el símbolo del sistema (cmd.exe) como administrador.

3. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

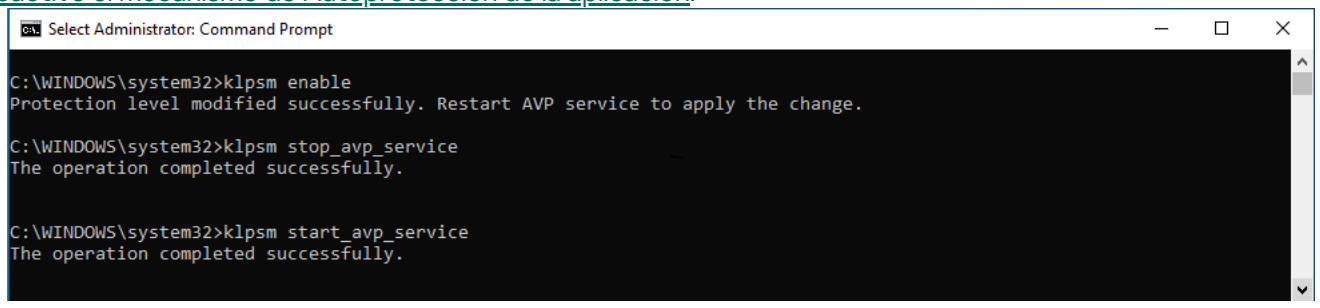
   Puede agregar la ruta al archivo ejecutable a la variable de sistema %PATH% durante la instalación de la aplicación.

4. En la línea de comandos, escriba lo siguiente:

   - `klpsm.exe enable`: habilitar la compatibilidad con la tecnología AM-PPL (vea la siguiente imagen).
   - `klpsm.exe disable`: deshabilitar la compatibilidad con la tecnología AM-PPL.

5. Reinicie Kaspersky Endpoint Security.

6. Reactive el mecanismo de Autoprotección de la aplicación.



Habilitar la compatibilidad con la tecnología AM-PPL

Protección de los servicios de aplicación contra la administración externa

La protección de los servicios de aplicación contra la administración externa bloquea los intentos de los usuarios y otras aplicaciones de detener los servicios de Kaspersky Endpoint Security. La protección garantiza el funcionamiento de los siguientes servicios:

- Kaspersky Endpoint Security service (AVP.KES.14.1)
- Kaspersky Seamless Update Service service (AVPSUS.KES.14.1)

Para salir de la aplicación desde la línea de comandos, deshabilite la protección de los servicios de Kaspersky Endpoint Security contra la administración externa.

Puede permitir la administración externa de servicios de aplicaciones solo en equipos que no sean compatibles con la tecnología AM-PPL o en equipos que tengan la tecnología deshabilitada.

Cómo habilitar o deshabilitar la Protección de los servicios de 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 correspondiente 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 **Bloquear la administración externa de los servicios de la aplicación** para habilitar o deshabilitar la protección de los servicios de Kaspersky Endpoint Security contra la administración externa.
5. Guarde los cambios.

Cómo habilitar o deshabilitar la Protección de los servicios de aplicación contra la administración externa en Web Console y Cloud Console

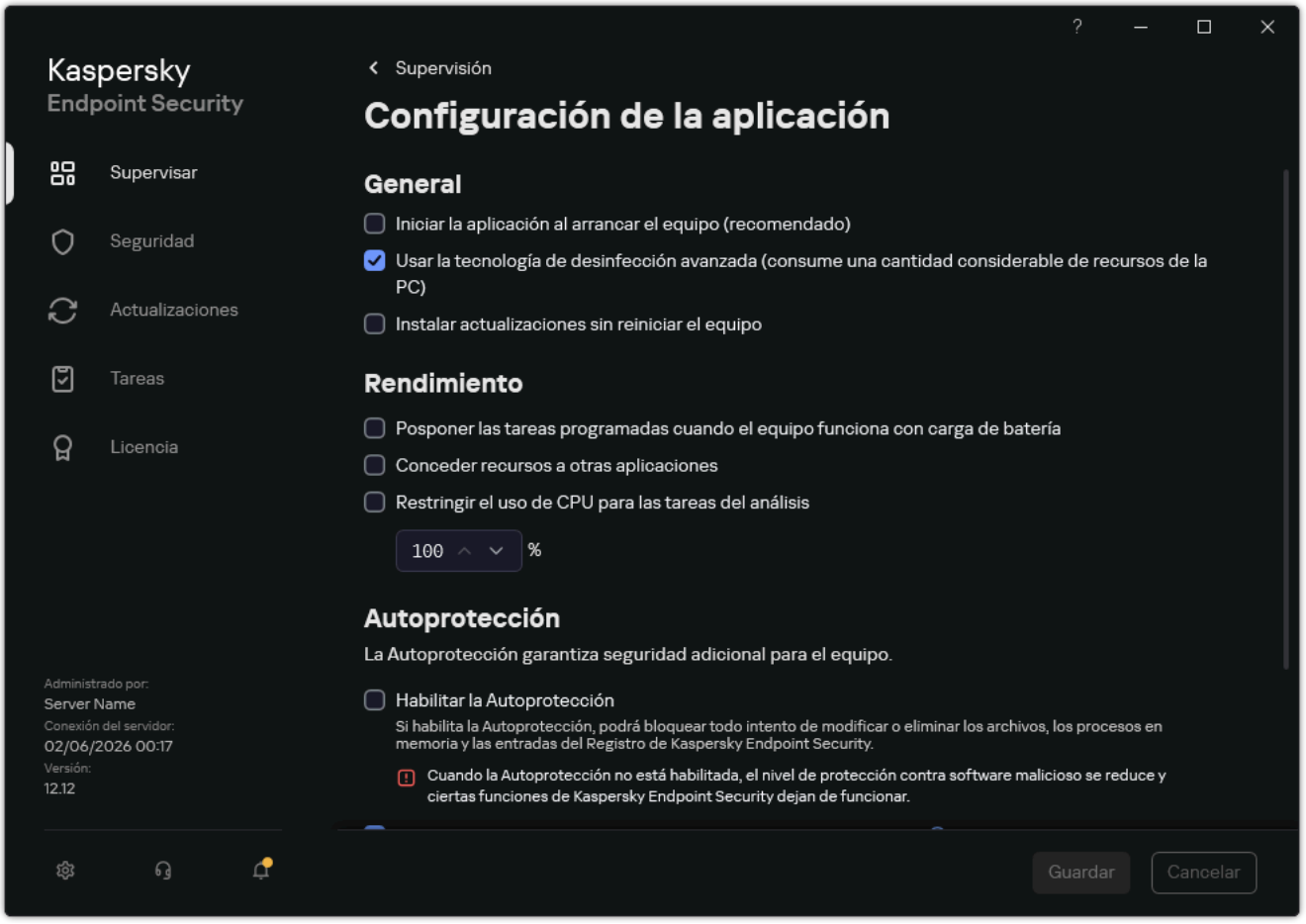
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.
5. Utilice la casilla **Bloqueo de la administración externa de los servicios de la aplicación** para habilitar o deshabilitar la protección de los servicios de Kaspersky Endpoint Security contra la administración externa.
6. Guarde los cambios.

Cómo habilitar o deshabilitar la Protección de los servicios de aplicación contra la administración externa en la interfaz de la aplicación

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

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

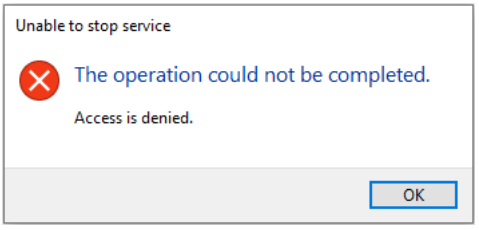


Configuración de Kaspersky Endpoint Security para Windows

3. Utilice la casilla **Bloquear administración externa de los servicios de la aplicación** para habilitar o deshabilitar la protección de los servicios de Kaspersky Endpoint Security contra la administración externa.

4. Guarde los cambios.

Como consecuencia, cuando un usuario intente detener los servicios de aplicación, aparecerá una ventana del sistema con un mensaje de error. El usuario solo puede administrar los servicios de aplicación desde la interfaz de Kaspersky Endpoint Security.



Error de acceso a los servicios de la aplicación

Compatibilidad con aplicaciones de administración remota

Ocasionalmente, puede necesitar usar una aplicación de administración remota mientras está habilitada la protección de administración externa.

Para habilitar el funcionamiento de aplicaciones de administración remota:

1. En la ventana principal de la aplicación 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 vínculo **Especificar aplicaciones de confianza**.
4. En la ventana que se abre, haga clic en el botón **Agregar**.
5. Seleccione el archivo ejecutable de la aplicación de administración remota.

   También puede escribir la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
6. Seleccione la casilla de verificación **Permitir interacción con la interfaz de Kaspersky Endpoint Security**.
7. Guarde los cambios.

Protección con contraseña

Un equipo puede ser utilizado por múltiples usuarios con diferentes niveles de conocimientos informáticos. Si los usuarios tienen acceso no restringido a Kaspersky Endpoint Security y a su configuración, es posible que se reduzca el nivel general de protección del equipo. La protección con contraseña permite restringir el acceso a Kaspersky Endpoint Security conforme a los permisos que los usuarios tienen asignados (por ejemplo, el permiso para cerrar 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:

- Usar un nombre de usuario y contraseña.

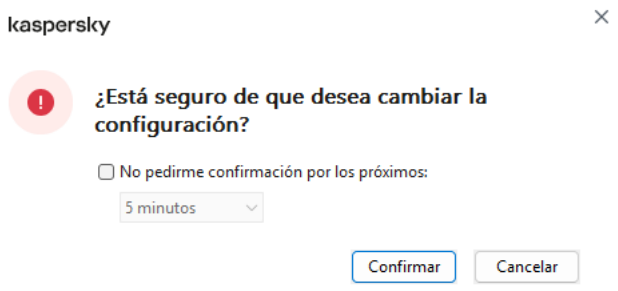
  Este es el método más conveniente para las operaciones cotidianas. Para realizar una acción protegida con contraseña, se introducen las credenciales de una cuenta de dominio perteneciente a un usuario con el permiso necesario. Para usar esta opción, es necesario que el equipo esté conectado al dominio en cuestión. Si el equipo no está conectado al dominio, puede usar la cuenta KLAdmin o una cuenta agregada manualmente.

- Usar una contraseña temporal.

  Este método está pensado para que un usuario ajeno a la red corporativa pueda, en forma temporal, realizar una acción bloqueada (por ejemplo, cerrar la aplicación). Una vez que la contraseña temporal caduca o la sesión finaliza, Kaspersky Endpoint Security restablece su configuración anterior.

Como se ve en la siguiente imagen, cuando un usuario intenta realizar una acción protegida con contraseña, Kaspersky Endpoint Security le solicita su nombre de usuario y contraseña o una contraseña temporal.

En la ventana de entrada de la contraseña, puede cambiar de idioma con solo presionar **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 en Kaspersky Endpoint Security

Nombre de usuario y contraseña

Para acceder a Kaspersky Endpoint Security, debe ingresar las credenciales de la cuenta. La protección con contraseña admite las siguientes cuentas:

- **KLAdmin**. Cuenta de administración con acceso ilimitado a Kaspersky Endpoint Security. La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña. Los permisos de KLAdmin no pueden revocarse. Cuando habilite la protección con contraseña, Kaspersky Endpoint Security le pedirá que defina la contraseña de esta cuenta.

- **Cuenta agregada manualmente**. Una cuenta fuera del dominio de Active Directory. Puede usar esta cuenta del servicio en lugar de KLAdmin si no desea compartir la contraseña del administrador. Puede establecer cualquier nombre de usuario y contraseña, y configurar los permisos individuales.

- **El grupo Everyone**. Grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa. Los usuarios del grupo Everyone tendrán acceso a la aplicación conforme a los permisos que se les asigne.

- **Usuarios o grupos individuales**. Cuentas de usuario a las que pueden asignarse permisos individuales. Es posible, por ejemplo, autorizar a un usuario o grupo en particular a realizar una acción que se encuentra bloqueada para el grupo Everyone.

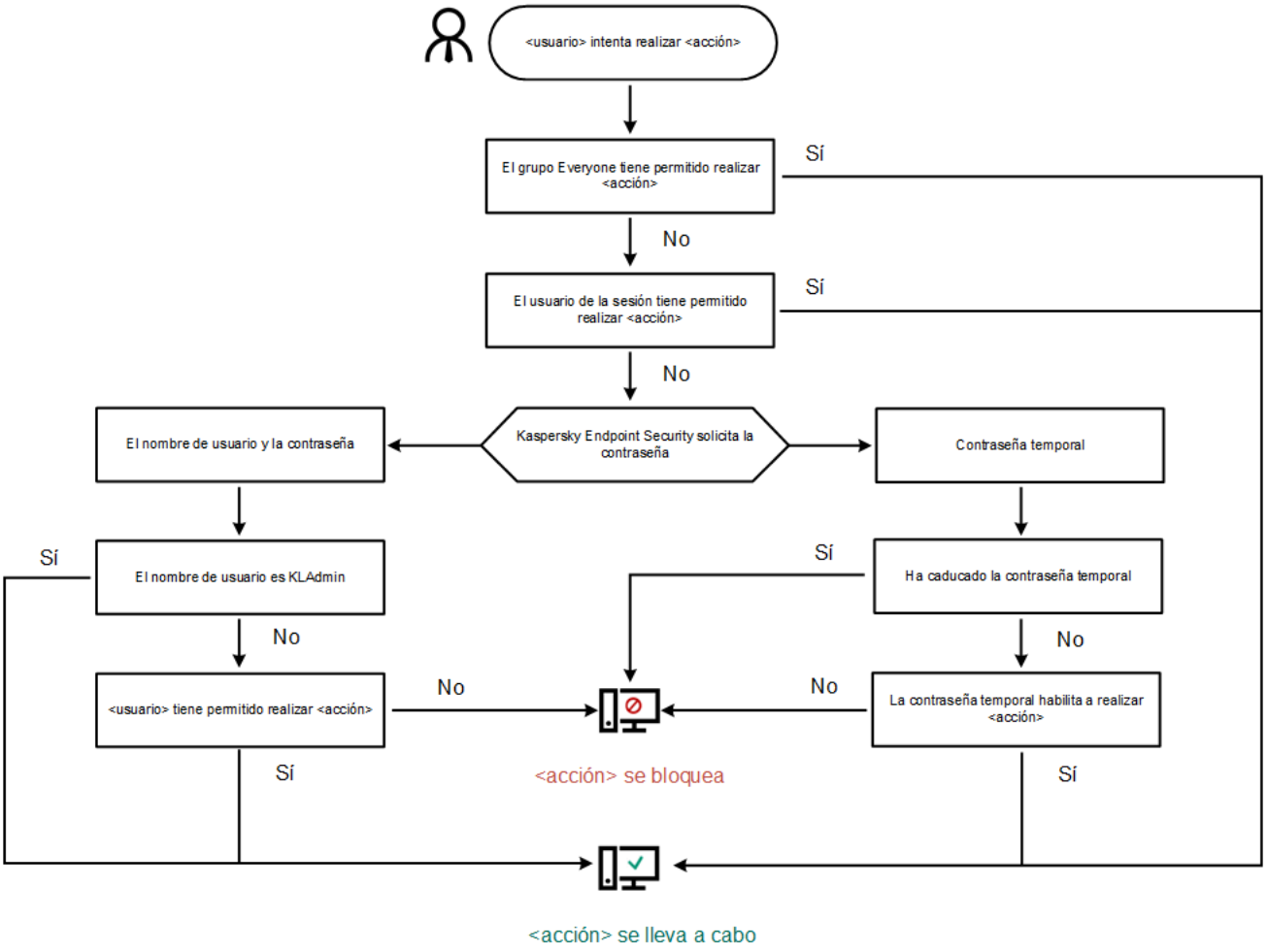
- **Usuario de la sesión**. Cuenta del usuario que inició sesión en Windows. Cuando la aplicación le solicite la contraseña, podrá cambiar a otro usuario de sesión (casilla **Guardar contraseña para esta sesión**). En tal caso, Kaspersky Endpoint Security considerará como usuario de la sesión al usuario a quien pertenezcan las credenciales de cuenta especificadas y no al que haya iniciado sesión en Windows.

Contraseña temporal

Una contraseña temporal se utiliza para brindar acceso no permanente a Kaspersky Endpoint Security en un equipo ajeno a la red corporativa. El administrador genera la contraseña temporal para un equipo específico en Kaspersky Security Center, dentro de las propiedades del equipo. A continuación, especifica qué acciones estarán protegidas por dicha contraseña y cuál será su período de vigencia.

Algoritmo de funcionamiento de la protección con contraseña

Para determinar si una acción protegida con contraseña debe permitirse o bloquearse, Kaspersky Endpoint Security usa el algoritmo de la siguiente imagen.



Algoritmo de funcionamiento de la protección con contraseña

Habilitar la protección con contraseña

La protección con contraseña permite restringir el acceso a Kaspersky Endpoint Security conforme a los permisos que los usuarios tienen asignados (por ejemplo, el permiso para cerrar la aplicación).

Cómo habilitar 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 correspondiente 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 con contraseña.
5. Utilice la casilla **Habilitar la protección con contraseña** para habilitar o deshabilitar el componente.
6. En **Permisos**, seleccione la cuenta KLAdmin.
7. Esto abre una ventana; en esa ventana, haga clic en **Contraseña** y establezca una contraseña para la cuenta KLAdmin.

   La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña.

   > Si olvidó la contraseña de su cuenta de KLAdmin, puede restablecer la contraseña en las propiedades de la directiva.

8. Vuelva a la lista de cuentas.
9. Configure los permisos de los que dispondrán todos los usuarios de la red corporativa:

   a. En **Permisos**, seleccione el grupo "Todos".

      El grupo *Everyone* es un grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa.

   b. En la ventana que se abrió, seleccione las casillas adyacentes a las acciones que los usuarios podrán realizar sin que se les solicite la contraseña.

      Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

      > Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.

10. Guarde los cambios.

Cómo habilitar 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.

5. En **Protección con contraseña**, use el conmutador **Protección con contraseña HABILITADA** para habilitar o deshabilitar el componente.

6. Defina la contraseña de la cuenta KLAdmin y confírmela.

   La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña.

   > Si olvidó la contraseña de su cuenta de KLAdmin, puede restablecer la contraseña en las propiedades de la directiva.

7. Vuelva a la lista de cuentas.

8. Configure los permisos de los que dispondrán todos los usuarios de la red corporativa:

   a. En la tabla de cuentas, seleccione el grupo "Todos".

      El grupo *Everyone* es un grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa.

   b. En la ventana que se abrió, seleccione las casillas adyacentes a las acciones que los usuarios podrán realizar sin que se les solicite la contraseña.

      Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

      > Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.

9. Guarde los cambios.

Cómo habilitar la protección con contraseña en la interfaz de la aplicación

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

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

3. Use el interruptor **Protección con contraseña** para habilitar o deshabilitar el componente.

4. Defina la contraseña de la cuenta KLAdmin y confírmela.

   La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña.

   > Si el equipo está sujeto a una directiva, el administrador puede restablecer la contraseña de la cuenta KLAdmin a través de las propiedades de la directiva. La contraseña no puede recuperarse si la olvida y el equipo no está conectado a Kaspersky Security Center.

5. Configure los permisos de los que dispondrán todos los usuarios de la red corporativa:

   a. En la tabla de la cuenta, haga clic en **Editar** para abrir la lista de permisos del grupo Todos.

      El grupo *Everyone* es un grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa.

b. Active las casillas adyacentes a las acciones que los usuarios podrán realizar sin que se les solicite la contraseña.

Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

> Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.

6. Guarde los cambios.

Una vez que la protección con contraseña esté habilitada, Kaspersky Endpoint Security restringirá el acceso de los usuarios sobre la base de los permisos otorgados al grupo Everyone. Cuando necesite realizar una acción que esté prohibida para el grupo Everyone, deberá usar la cuenta KLAdmin, una cuenta que disponga de los permisos necesarios o una contraseña temporal.

> Para deshabilitar la protección con contraseña, deberá iniciar sesión con el usuario KLAdmin. La protección con contraseña no puede deshabilitarse cuando se está usando una contraseña temporal o cualquier otra cuenta.

Al momento de escribir la contraseña, puede activar la casilla **Guardar contraseña para esta sesión**. Con ello, en tanto la sesión de usuario continúe activa, podrá realizar otras acciones protegidas sin que Kaspersky Endpoint Security le solicite nuevamente la contraseña.

Asignación de permisos a usuarios o grupos individuales

La protección con contraseña permite otorgarle a Kaspersky Endpoint Security acceso a cuentas de usuario individuales de Active Directory y cuentas de usuario agregadas manualmente.

Cuentas de usuario de Active Directory

Puede otorgarle a Kaspersky Endpoint Security acceso a usuarios o grupos individuales dentro del dominio de Active Directory. Por ejemplo, un usuario específico puede contar con el permiso **Salir de la aplicación** aun cuando los miembros del grupo Everyone tengan prohibido cerrar el programa. Con ello, la aplicación únicamente podrá cerrarse cuando se haya iniciado sesión como ese usuario específico o como KLAdmin.

> Para acceder a la aplicación utilizando las credenciales de una cuenta de dominio, el equipo debe estar conectado al dominio en cuestión. Si el equipo no está conectado al dominio, use la cuenta KLAdmin o una contraseña temporal.

Cuentas de usuario agregadas manualmente

Puede crear una cuenta de usuario que no esté presente en Active Directory y asignar permisos individuales a esa cuenta de usuario. Es decir, puede crear una *cuenta de usuario de servicio* y usarla en lugar de KLAdmin. De esta manera, no necesita compartir su contraseña de KLAdmin con otros usuarios ni crear nuevas cuentas de usuario de Active Directory. Puede especificar cualquier nombre de usuario y contraseña. Por ejemplo, puede otorgar el permiso **Ver informes** a la cuenta de usuario del servicio. Como resultado, si la visualización de informes está prohibida en el grupo "Todos", puede abrir los informes usando la cuenta de usuario de servicio o la cuenta de usuario de KLAdmin.

Asignación de 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 correspondiente 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 con contraseña.
5. En la tabla de cuentas, haga clic en **Agregar**.
6. Seleccione el tipo de cuenta de usuario que desee agregar:

   - **Seleccionar un usuario/grupo de Active Directory**: cuentas de usuario de Active Directory

     Para seleccionar una cuenta de usuario, haga clic en **Seleccionar**. Seleccione un usuario o grupo de Active Directory y confirme su elección.
   - Seleccione **Agregar un usuario/grupo de usuarios manualmente** para una cuenta de usuario de servicio agregada manualmente.

     Para agregar una cuenta de usuario de servicio, escriba un nombre de usuario y una contraseña (por ejemplo, SecureAdmin).

     > Puede restablecer la contraseña de una cuenta de usuario de servicio en la configuración de directivas. La contraseña de la cuenta de usuario de servicio debe restablecerse de la misma forma que la contraseña de KLAdmin. Si se permite la edición de la configuración de la 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 de servicio en la interfaz de la aplicación. Para ello, confirme los cambios de la información de la cuenta de usuario de servicio utilizando la contraseña de KLAdmin.
7. En la lista **Permisos**, seleccione las casillas adyacentes a las acciones que el usuario o grupo seleccionado podrá realizar sin que se le solicite una contraseña.

   Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.

8. Guarde los cambios.

Cómo otorgar permisos a usuarios individuales o grupos 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.
5. En el bloque **Protección con contraseña**, haga clic en el vínculo **Permisos de usuario**.

   Esta acción abre el formulario para otorgar permisos de habilitación con contraseña.
6. Haga clic en **Agregar**.
7. Seleccione el tipo de cuenta de usuario que desee agregar:

   - **Seleccionar desde Active Directory**: cuentas de usuario de Active Directory

     Para seleccionar una cuenta de usuario, haga clic en **Editar**. Seleccione un usuario o grupo de Active Directory y confirme su elección.
   - Seleccione **Agregar manualmente** para una cuenta de usuario de servicio agregada manualmente.

     Para agregar una cuenta de usuario del servicio, ingrese un nombre de usuario y una contraseña (por ejemplo, SecureAdmin).

     Puede restablecer la contraseña de una cuenta de usuario de servicio en la configuración de directivas. La contraseña de la cuenta de usuario de servicio debe restablecerse de la misma forma que la contraseña de KLAdmin. Si se permite la edición de la configuración de la 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 de servicio en la interfaz de la aplicación. Para ello, confirme los cambios de la información de la cuenta de usuario de servicio utilizando la contraseña de KLAdmin.
8. En la lista **Permisos**, seleccione las casillas adyacentes a las acciones que el usuario o grupo seleccionado podrá realizar sin que se le solicite una contraseña.

   Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

   Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.
9. Haga clic en **Agregar**.
10. Guarde los cambios.

Cómo otorgar permisos a usuarios individuales o grupos en la interfaz de usuario de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En la tabla de cuentas, haga clic en **Agregar**.
4. Seleccione el tipo de cuenta de usuario que desee agregar:
   - **Seleccionar un usuario/grupo de Active Directory**: cuentas de usuario de Active Directory

     Para seleccionar una cuenta de usuario, haga clic en **Seleccionar usuario o grupo**. Seleccione un usuario o grupo de Active Directory y confirme su elección.
   - Seleccione **Agregar un usuario manualmente** para una cuenta de usuario de servicio agregada manualmente.

     Para agregar una cuenta de usuario de servicio, escriba un nombre de usuario y una contraseña (por ejemplo, SecureAdmin).

     > Puede restablecer la contraseña de una cuenta de usuario de servicio en la configuración de directivas. La contraseña de la cuenta de usuario de servicio debe restablecerse de la misma forma que la contraseña de KLAdmin. Si se permite la edición de la configuración de la 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 de servicio en la interfaz de la aplicación. Para ello, confirme los cambios de la información de la cuenta de usuario de servicio utilizando la contraseña de KLAdmin.
5. En la lista **Permisos**, seleccione las casillas adyacentes a las acciones que el usuario o grupo seleccionado podrá realizar sin que se le solicite una contraseña.

   Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

   > Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.
6. Guarde los cambios.

Como resultado, si el grupo Everyone tiene acceso restringido a Kaspersky Endpoint Security, el acceso de los usuarios se regulará conforme a los permisos que se les haya asignado individualmente.

Uso de una contraseña temporal para otorgar permisos

Una contraseña temporal se utiliza para brindar acceso no permanente a Kaspersky Endpoint Security en un equipo ajeno a la red corporativa. Permite que un usuario realice una acción bloqueada sin tener que conocer las credenciales de la cuenta KLAdmin. El equipo en el que va a usarse la contraseña temporal debe estar incluido en 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Haga doble clic en un equipo para abrir su ventana de propiedades.
5. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.1)** 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**.

   Se abre la ventana Administración de contraseñas temporales.
10. Haga clic en **Agregar**.
11. En el campo **Fecha de caducidad**, especifique cuándo caducará la contraseña temporal.
12. En la tabla **Alcance de la contraseña temporal**, active las casillas adyacentes a las acciones que el usuario podrá realizar una vez que introduzca la contraseña temporal.
13. Haga clic en **Generar**.

    Se abre una ventana con la contraseña temporal (vea la siguiente imagen).
14. Copie la contraseña y envíesela al usuario.

Cómo permitir que un usuario realice una acción bloqueada con una contraseña temporal a través de Web Console web 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 donde quiere permitir que un usuario realice una acción bloqueada.
3. Seleccione la ficha **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.
5. Seleccione la ficha **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 **Agregar**.

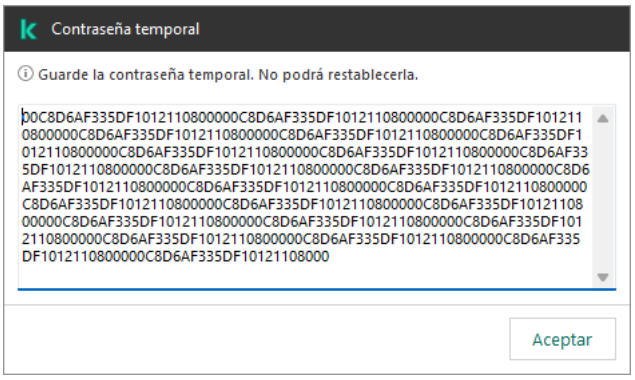
8. En el campo **Fecha de caducidad**, especifique cuándo caducará la contraseña temporal.

9. En la tabla **Alcance de la contraseña temporal**, active las casillas adyacentes a las acciones que el usuario podrá realizar una vez que introduzca la contraseña temporal.

10. Haga clic en **Generar**.

    Se abre una ventana con la contraseña temporal.

11. Copie la contraseña y envíesela al usuario.



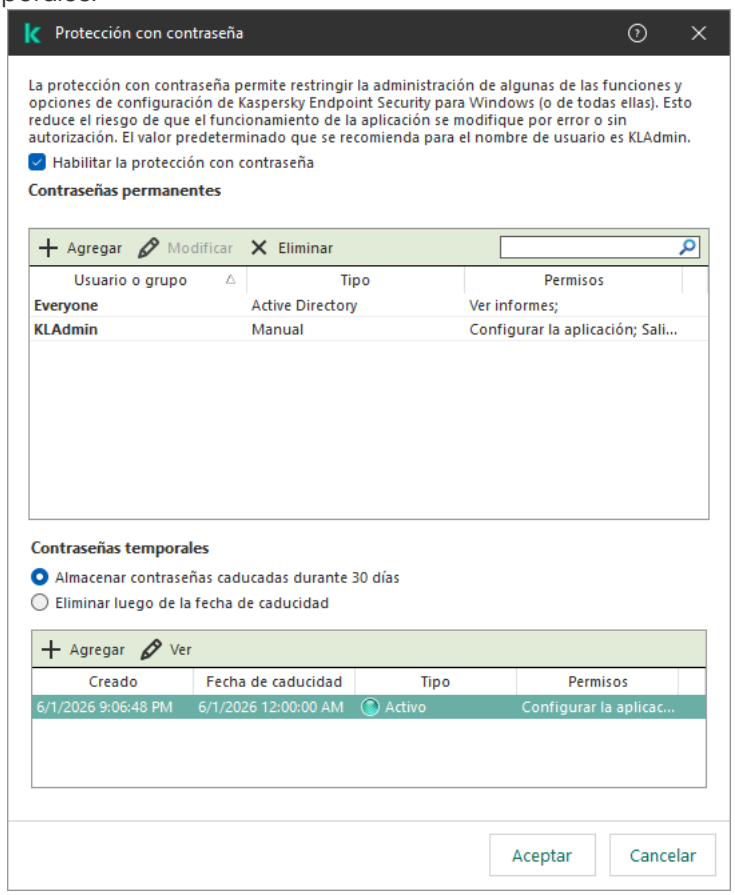
Contraseña temporal

Revocación de contraseña temporal

A partir de la versión 12.9, Kaspersky Endpoint Security para Windows incluye la funcionalidad *Administración de contraseñas temporales*. Administración de contraseñas temporales le permite realizar las siguientes acciones:

- Guardar el historial de contraseñas (hasta 30 días).
- Controlar el estado de la contraseña temporal: *Activo*, *Caducada*, *Revocado*.

- Revocar contraseñas temporales.



Administración de contraseñas temporales

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 las contraseñas temporales con 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Haga doble clic en un equipo para abrir su ventana de propiedades.
5. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows (14.1)** 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. Se abre una ventana. En **Contraseña temporal**, configure el almacenamiento para las contraseñas caducadas.
10. Haga clic en **Lista de contraseñas temporales**.

    Se abre la ventana Administración de contraseñas temporales. 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 los equipos, cierre los candados .

Cómo revocar contraseñas temporales con 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 donde quiere permitir que un usuario realice una acción bloqueada.

3. Seleccione la ficha **Aplicaciones**.

4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.

5. Seleccione la ficha **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 vínculo **Contraseña temporal**.

   Se abre la ventana Administración de contraseñas temporales. 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 los equipos, cierre los candados .

Como resultado, 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 de inmediato.

Aspectos especiales de los permisos de la protección con contraseña

Los permisos de protección con contraseña están sujetos a ciertas consideraciones y limitaciones especiales.

Configurar la aplicación

Cuando el equipo de un usuario esté sujeto a una directiva, asegúrese de verificar que todos los parámetros pertinentes de esta puedan editarse (es decir, que los atributos estén abiertos).

Salir de la aplicación

No hay ninguna consideración o limitación que se deba tener en cuenta.

Deshabilitar componentes de protección

- No es posible autorizar al grupo Everyone a deshabilitar los componentes de protección. Para que KLAdmin no sea el único usuario autorizado a deshabilitar los componentes de control, agregue un usuario o grupo que tenga el permiso **Deshabilitar componentes de protección** en la Configuración de la protección con contraseña.
- Cuando el equipo de un usuario esté sujeto a una directiva, asegúrese de verificar que todos los parámetros pertinentes de esta puedan editarse (es decir, que los atributos estén abiertos).
- Para deshabilitar los componentes de protección en la configuración de la aplicación, el usuario debe contar con el permiso **Configurar la aplicación**.
- Para deshabilitar los componentes de protección a través del menú contextual (usando el elemento **Suspender protección**), el usuario debe contar tanto con el permiso **Deshabilitar componentes de protección** como con el permiso **Deshabilitar componentes de control**.

Deshabilitar componentes de control

- No es posible autorizar al grupo Everyone a deshabilitar los componentes de control. Para que KLAdmin no sea el único usuario autorizado a deshabilitar los componentes de control, agregue un usuario o grupo que tenga el permiso **Deshabilitar componentes de control** en la Configuración de la protección con contraseña.
- Cuando el equipo de un usuario esté sujeto a una directiva, asegúrese de verificar que todos los parámetros pertinentes de esta puedan editarse (es decir, que los atributos estén abiertos).
- Para deshabilitar los componentes de control en la configuración de la aplicación, el usuario debe contar con el permiso **Configurar la aplicación**.
- Para deshabilitar los componentes de control a través del menú contextual (usando el elemento **Suspender protección**), el usuario debe contar tanto con el permiso **Deshabilitar componentes de control** como con el permiso **Deshabilitar componentes de protección**.

Deshabilitar 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 deshabilitar la directiva, agregue un usuario o grupo que tenga el permiso **Deshabilitar la directiva de Kaspersky Security Center** en la Configuración de la protección con contraseña.

Eliminar una clave

No hay ninguna consideración o limitación que se deba tener en cuenta.

Eliminar, modificar o restaurar la aplicación

Si permitió eliminar, modificar y restaurar la aplicación para el grupo "Todos", Kaspersky Endpoint Security no solicitará una contraseña cuando el usuario intente llevar a cabo estas operaciones. Por lo tanto, todos los usuarios, incluidos aquellos que estén fuera del dominio, podrán instalar, modificar o restaurar la aplicación.

Restaurar el acceso a los datos de unidades cifradas

Para restaurar el acceso a los datos de unidades cifradas, deberá iniciar sesión con el usuario KLAdmin. El permiso para realizar esta acción no puede otorgarse a ningún otro usuario.

Ver informes

No hay ninguna consideración o limitación que se deba tener en cuenta.

Restaurar objetos de Copia de seguridad

No hay ninguna consideración o limitación que se deba tener en cuenta.

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 KLAdmin. Al exportar la configuración de la aplicación, solo se crea un archivo de configuración con los ajustes 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 realizadas mediante los componentes de la aplicación.

Restablecimiento de la contraseña de KLAdmin

Si olvidó la contraseña de su cuenta de 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 ingrese las credenciales de KLAdmin.

La contraseña no puede recuperarse si la olvida y el equipo no está conectado a Kaspersky Security Center.

Cómo restablecer la contraseña de la cuenta de 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 correspondiente 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, borre la casilla **Habilitar la protección con contraseña**.
6. Guarde los cambios.
7. Vuelva a seleccionar la casilla **Habilitar la protección con contraseña**.
8. Haga clic en **Aceptar**.
   Se abre la ventana de la contraseña del administrador.
9. Defina la contraseña nueva de la cuenta de KLAdmin y confírmela.
10. Guarde los cambios.

Cómo restablecer la contraseña de la cuenta de 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 ficha **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.
   Se abre la configuración local de la aplicación.
5. Seleccione la ficha **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 activar el conmutador **Protección con contraseña**.
10. Defina la contraseña nueva de la cuenta de KLAdmin y confírmela.
11. Guarde los cambios.

De esta manera, la contraseña de su cuenta de KLAdmin se actualiza después de aplicar la directiva.

Protección de la conexión del Servidor de administración

Puede conectar el equipo al Servidor de administración a través del componente *Agente de red* de Kaspersky Security Center. Si un intruso tiene suficientes derechos para modificar la configuración de conexión con el servidor, existe el riesgo de conectar el equipo a un servidor no confiable. Esto permitiría que el intruso aplique sus propias directivas de grupo y, por ejemplo, deshabilite la autoprotección de la aplicación. Kaspersky Endpoint Security puede prevenir la reconexión no autorizada de un equipo a un servidor diferente. Para proteger la conexión al servidor, la aplicación sugiere establecer una contraseña y utilizar la función Password-Based key Derivation Function (PBKDF2). Como consecuencia, no es posible acceder a la aplicación sin contraseña.

Para garantizar una protección completa de Kaspersky Endpoint Security y el Agente de red frente a accesos no autorizados, recomendamos habilitar la protección adicional. Para Kaspersky Endpoint Security, recomendamos habilitar Protección con contraseña. Para proteger el Agente de red, recomendamos configurar una contraseña de desinstalación. Para obtener más información sobre cómo evitar la eliminación del Agente de red, consulte la Ayuda de Kaspersky Security Center.

Puede administrar la conexión del equipo con el Servidor de administración a través de la tarea *Protección de la conexión del Servidor de administración*. La tarea le permite realizar las siguientes acciones:

- Establecer una contraseña para proteger la conexión con el servidor.
- Cambiar la contraseña.
- Reconectar el equipo con un servidor diferente.
- Deshabilitar la protección de la conexión con el servidor.

Autenticación del equipo durante la conexión con el Servidor de administración

Después de establecer una contraseña, la aplicación crea un conjunto de datos mediante la transformación de PBKDF2 de la contraseña. Luego, la aplicación cifra este conjunto de datos usando la clave del Agente de red. La aplicación usa el conjunto de datos cifrado para verificar los derechos y privilegios del Servidor de administración para conexiones posteriores.

Entonces, cada vez que se intente reconectar el equipo con el Servidor de administración, la aplicación descifra el conjunto de datos con la clave del Agente de red y la compara con la copia local. Si no se corresponden, se restringe el acceso a la aplicación.

Protección de la conexión del Servidor de administración

Cómo establecer una contraseña para proteger la conexión con el 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Protección de la conexión del Servidor de administración**.

Paso 2. Protección de la conexión con el Servidor de administración

Establezca una contraseña para proteger la conexión con el Servidor de administración:

1. En **Protección de la conexión del Servidor de administración**, seleccione **Proteger con una contraseña**.

2. En la lista desplegable **Servidor de administración**, seleccione **Nuevo servidor**.

3. En el campo **Contraseña de la conexión al Servidor de administración**, establezca la contraseña de 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 de verificación **Habilitar compatibilidad de cifrado de contraseñas para versiones anteriores de la aplicación (12.7 y versiones anteriores)**.

   A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si tiene instalada Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desmarque 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 con la que se ejecutará la tarea

Seleccione **Cuenta predeterminada**. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

Paso 4. Programación de la tarea

En **Inicio programado**, seleccione **Manual**.

Paso 5. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo, *Contraseña de conexión con el servidor principal*.

Paso 6. Completar creación de la tarea

Salga del Asistente. Seleccione la casilla de verificación **Ejecutar la tarea al finalizar el asistente** o ejecute la tarea manualmente. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo establecer una contraseña para proteger la conexión con el 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Protección de la conexión del Servidor de administración**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve, por ejemplo, *Contraseña de conexión con el servidor principal*.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

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. Salga del Asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Seleccione la tarea **Protección de la conexión del Servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. En **Protección de la conexión del Servidor de administración**, seleccione **Proteger con una contraseña**.

10. En la lista desplegable **Conexión con el Servidor de administración**, seleccione **Contraseña nueva**.

11. En el campo **Contraseña**, establezca la contraseña de 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 de verificación **Habilitar compatibilidad de cifrado de contraseñas para versiones anteriores de la aplicación (12.7 y versiones anteriores)**.

    A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si tiene instalada Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desmarque 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.

Reconexión del equipo con un Servidor de administración diferente

La reconexión del equipo con un Servidor de administración diferente requiere los siguientes pasos:

1. En la consola del servidor actual `[KSC1]`, ejecute la tarea *Cambiar Servidor de administración* del Agente de red.

   Después de ejecutar la tarea, el equipo se reconecta al nuevo servidor `[KSC2]`.

   El equipo se mostrará en la consola del servidor `[KSC1]` con el estado *Crítico*. No es posible configurar la aplicación a través de directivas ni ejecutar tareas de forma remota en el equipo.

2. En la consola del nuevo servidor `[KSC2]`, cree una nueva tarea *Protección de la conexión del Servidor de administración* para Kaspersky Endpoint Security. En las propiedades de la tarea, escriba la contraseña del servidor anterior y establezca una contraseña para el nuevo servidor.

   Cómo establecer una contraseña nueva para la reconexión con 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**.

   Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Protección de la conexión del Servidor de administración**.

Paso 2. Protección de la conexión con el Servidor de administración

Establezca una contraseña para proteger la conexión con el nuevo Servidor de administración:

1. En **Protección de la conexión del Servidor de administración**, seleccione **Proteger con una contraseña**.
2. En la lista desplegable **Servidor de administración**, seleccione **Reconectar desde otro servidor**.
3. En el campo **Contraseña actual**, escriba la contraseña establecida para la conexión con el servidor de confianza usado anteriormente.
4. En el campo **Contraseña nueva**, establezca la contraseña de 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 de verificación **Habilitar compatibilidad de cifrado de contraseñas para versiones anteriores de la aplicación (12.7 y versiones anteriores)**.

   A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si tiene instalada Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desmarque 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 con la que se ejecutará la tarea

Seleccione **Cuenta predeterminada**. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

Paso 4. Programación de la tarea

En **Inicio programado**, seleccione **Manual**.

Paso 5. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo, *Contraseña de conexión con el servidor principal*.

Paso 6. Completar creación de la tarea

Salga del Asistente. Seleccione la casilla de verificación **Ejecutar la tarea al finalizar el asistente** o ejecute la tarea manualmente. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo establecer una contraseña nueva para la reconexión con 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Protección de la conexión del Servidor de administración**.

   c. En el campo **Nombre de la tarea**, escriba una descripción breve, por ejemplo, *Contraseña de conexión con el servidor principal*.

   d. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

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. Salga del Asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Seleccione la tarea **Protección de la conexión del Servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. En **Protección de la conexión del Servidor de administración**, seleccione **Proteger con una contraseña**.

10. En la lista desplegable **Conexión con el Servidor de administración**, seleccione **Reconectar desde otro servidor**.

11. En el campo **Contraseña actual**, escriba la contraseña establecida para la conexión con el servidor de confianza usado anteriormente.

12. En el campo **Contraseña nueva**, establezca la contraseña de 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 de verificación **Habilitar compatibilidad de cifrado de contraseñas para versiones anteriores de la aplicación (12.7 y versiones anteriores)**.

    A partir de Kaspersky Endpoint Security 12.8 para Windows, la aplicación utiliza un cifrado de contraseña más seguro. Si tiene instalada Kaspersky Endpoint Security 12.8 o una versión posterior, le recomendamos que desmarque 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.

Después de completar la tarea, asegúrese de que en la consola del nuevo servidor `[KSC2]`, el equipo tenga el estado *Aceptar*. Pruebe si puede ejecutar tareas de forma remota y configurar la aplicación mediante directivas.

Restablecer la contraseña de la conexión con el Servidor de administración

Si olvidó la contraseña de la conexión con el Servidor de administración o la contraseña está en riesgo, puede restablecer la contraseña en las propiedades de la tarea. También puede restablecer la contraseña y establecer una nueva contraseña para un grupo de equipos con diferentes estados de protección de la conexión del Servidor de administración. Es decir, si algunos equipos tienen la protección habilitada y otros la tienen deshabilitada, la tarea establece una contraseña para todos los equipos.

> Solo se puede restablecer la contraseña de la conexión al Servidor de administración en la consola del servidor de confianza al que está conectado el equipo.

Cómo restablecer la contraseña de la 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 del 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 del Servidor de administración**, seleccione **Proteger y cambiar contraseña**.

6. En el campo **Contraseña de la conexión al Servidor de administración**, establezca la nueva contraseña de la conexión al servidor de confianza actual y confírmela.

7. Guarde los cambios.

8. Ejecute la tarea.

Cómo restablecer la contraseña de la 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 del Servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

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

4. En **Protección de la conexión del Servidor de administración**, seleccione **Proteger y cambiar contraseña**.

5. En el campo **Contraseña**, establezca la nueva contraseña de la conexión al servidor de confianza actual y confírmela.

6. Guarde los cambios.

7. Active la casilla ubicada junto a la tarea.

8. Haga clic en **Iniciar**.

Como consecuencia, se restablece la contraseña de la conexión al Servidor de administración al finalizar la tarea.

Protección de la conexión del Servidor de administración

Solo se puede deshabilitar de forma remota la protección de la conexión del Servidor de administración en la consola del servidor de confianza al que está conectado el equipo. También puede deshabilitar la protección de manera local en la línea de comandos.

Cómo deshabilitar la protección de la conexión del 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 del 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 del 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 deshabilitar la protección de la conexión del 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 del Servidor de administración** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

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

4. En **Protección de la conexión del Servidor de administración**, seleccione **No proteger**.

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 deshabilitar la protección de la conexión del servidor en la línea de comandos

1. Abra el símbolo del sistema (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>]
   ```

   en el que `<password>` es la contraseña de la cuenta de usuario de KLAdmin o la contraseña de la tarea *Protección de la conexión del Servidor de administración*. Si no se especifica el parámetro, Kaspersky Endpoint Security le pedirá una contraseña en la siguiente línea.

   > Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada.

Ejemplo

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Cifrado de datos

Kaspersky Endpoint Security le permite cifrar archivos y carpetas que están almacenados en unidades locales o extraíbles, o unidades extraíbles y discos duros en su totalidad. El cifrado de datos minimiza el riesgo de fugas de información que pueden ocurrir como consecuencia del robo o la pérdida de un equipo portátil, un disco extraíble o un disco duro, o cuando acceden a los datos usuarios o aplicaciones no autorizados. Kaspersky Endpoint Security utiliza el algoritmo de cifrado Advanced Encryption Standard (AES).

Si caducó la licencia, la aplicación no cifra nuevos datos, y los datos cifrados anteriores permanecen cifrados y disponibles para su uso. En este caso, el cifrado de datos nuevos requiere que la aplicación se active con una licencia nueva 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.

No se garantiza que los archivos que cifre se mantengan cifrados si su licencia caduca, si infringe el Contrato de licencia de usuario final, si desinstala Kaspersky Endpoint Security o si elimina la clave de licencia o los componentes de cifrado. Esto se debe a que algunas aplicaciones, como Microsoft Office Word, crean una copia temporal de los archivos durante la modificación. Cuando se guarda el archivo original, la copia temporal reemplaza el archivo original. Por lo tanto, en un equipo que no tiene funcionalidad de cifrado o en el que esta es inaccesible, el archivo permanece no cifrado.

Kaspersky Endpoint Security ofrece los siguientes aspectos de protección de datos:

- **Cifrado de archivos en discos de equipos locales**. Puede compilar listas de archivos por extensión o grupo de extensiones y listas de carpetas almacenadas en discos locales del equipo, además de crear reglas para cifrar archivos que son creados por aplicaciones específicas. Luego de que se aplique una directiva, Kaspersky Endpoint Security cifrará y descifrará los siguientes archivos:
  - archivos agregados individualmente a listas para cifrado y descifrado;
  - archivos almacenados en carpetas agregadas a listas para cifrado y descifrado;
  - Archivos creados por aplicaciones por separado.
- **Cifrado de unidades extraíbles**. Se puede especificar una regla de cifrado predeterminada según la cual la aplicación realiza la misma acción en todos los discos extraíbles, o especificar reglas de cifrado para discos extraíbles individuales.

  La regla de cifrado predeterminada tiene menos prioridad que las reglas de cifrado creadas para discos extraíbles individuales. Las reglas de cifrado creadas para discos extraíbles del modelo de dispositivo especificado tienen menos prioridad que las reglas de cifrado creadas para discos extraíbles con el identificador del dispositivo especificado.

  Para seleccionar una regla de cifrado para archivos de un disco extraíble, Kaspersky Endpoint Security comprueba si el modelo y el identificador del dispositivo son conocidos. Luego, la aplicación realiza una de las siguientes operaciones:
  - Si se conoce el modelo del dispositivo, la aplicación usa la regla de cifrado (si la hubiera) creada para discos extraíbles del modelo de dispositivo específico.
  - Si solo se conoce el identificador del dispositivo, la aplicación usa la regla de cifrado (si la hubiera) creada para discos extraíbles con el identificador de dispositivo específico.

- Si se conocen el modelo y el identificador del dispositivo, la aplicación usa la regla de cifrado (si la hubiera) creada para discos extraíbles con el identificador de dispositivo específico. Si no hay ninguna de esas reglas, pero sí una regla de cifrado creada para discos extraíbles con el modelo del dispositivo específico, la aplicación aplica esta regla. Si no se especifica ninguna regla de cifrado para el identificador del dispositivo ni para el modelo del dispositivo específico, la aplicación aplica la regla de cifrado predeterminada.

- Si no se conoce ni el modelo ni el id. del dispositivo, la aplicación utiliza la regla de cifrado predeterminada.

La aplicación permite preparar un disco extraíble para utilizar datos cifrados almacenados en el disco en modo portátil. Después de habilitar el modo portátil, se puede acceder a los archivos cifrados en los discos extraíbles conectados a un equipo sin funcionalidad de cifrado.

- **Administración de reglas de acceso de aplicaciones a archivos cifrados**. Para cualquier aplicación, puede crear una regla de acceso a archivos cifrados que bloquee el acceso a archivos cifrados o que permita el acceso a archivos cifrados solo como texto cifrado, que es una secuencia de caracteres obtenidos cuando se aplica el cifrado.

- **Creación de paquetes cifrados**. Puede crear archivos de almacenamiento cifrados y proteger el acceso a ellos con una contraseña. Solo se puede acceder al contenido de los archivos de almacenamiento cifrados si se ingresan las contraseñas con las que protegió el acceso a esos archivos de almacenamiento. Estos archivos de almacenamiento se pueden transmitir de manera 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 tiene un Trusted Platform Module (TPM), BitLocker lo usa para almacenar claves de recuperación que proporcionan acceso a un disco duro cifrado. Cuando se inicia el equipo, BitLocker solicita las claves de recuperación del disco duro al Módulo de plataforma segura y desbloquea la unidad. Puede configurar el uso de una contraseña y/o de un código PIN para acceder a claves de recuperación.

  Puede especificar la regla predeterminada de cifrado de disco completo y crear una lista de los discos duros que se excluirán del cifrado. Kaspersky Endpoint Security lleva a cabo el cifrado de disco completo sector por sector una vez aplicada la directiva de Kaspersky Security Center. La aplicación cifra simultáneamente todas las particiones lógicas de los discos duros.

  Una vez cifrados los discos duros del sistema, la próxima vez que se inicie el equipo, el usuario deberá superar la autenticación por medio del Agente de autenticación para poder acceder a los discos duros y cargar el sistema operativo. El usuario puede autenticarse de dos maneras: puede escribir la contraseña de un token o de una tarjeta inteligente que conecte al equipo, o puede introducir el nombre de usuario y la contraseña de la cuenta del Agente de autenticación que el administrador de la red de área local haya creado con la tarea de *Administrar cuentas del Agente de autenticación*. Estas cuentas se basan en las cuentas de Microsoft Windows con las que el usuario inicia sesión en el sistema operativo. También existe la posibilidad de usar la tecnología Single Sign-On (SSO), que le permite iniciar sesión en el sistema operativo automáticamente con el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

  > Si realiza una copia de seguridad de un equipo y, posteriormente, cifra los datos del equipo, después de lo cual restaura la copia de seguridad del equipo y vuelve a cifrar los datos del equipo, Kaspersky Endpoint Security crea duplicados de las cuentas del Agente de autenticación. Para eliminar las cuentas duplicadas, emplee la utilidad 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.

Para acceder a un disco duro cifrado, es necesario utilizar un equipo en el que se haya instalado Kaspersky Endpoint Security con la característica de cifrado de disco completo. Esta precaución minimiza el riesgo de fugas de datos desde un disco duro cifrado cuando se intenta acceder al disco desde fuera de la red de área local de la empresa.

Para cifrar discos duros y discos extraíbles, puede usar la función Solo cifrar el espacio de disco usado. Se recomienda usar esta función solo para dispositivos nuevos que no se han usado anteriormente. Si está aplicando el cifrado a un dispositivo que ya está en uso, le recomendamos que cifre todo el dispositivo. De esta manera, se asegurará de que toda la información —incluida la información eliminada, que podría contener datos recuperables— esté protegida.

Antes de que comience el cifrado, Kaspersky Endpoint Security obtiene el mapa de sectores del sistema de archivos. La primera tanda de cifrado incluye los sectores que están ocupados por archivos al momento de iniciarse el cifrado. La segunda tanda de cifrado incluye los sectores que se escribieron después de iniciado el cifrado. Una vez finalizado el cifrado, todos los sectores que contienen datos estarán cifrados.

Una vez finalizado el cifrado, si un usuario elimina un archivo, los sectores que almacenaban el archivo eliminado se vuelven disponibles para almacenar información nueva 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 **Solo cifrar el espacio de disco usado**.

El Servidor de administración de Kaspersky Security Center que controló el equipo cuando se realizó el cifrado brinda los datos necesarios para descifrar los archivos. Si el equipo que contiene los objetos cifrados estuvo, por algún motivo, controlado por un Servidor de administración diferente, existen distintos métodos para obtener acceso a la información cifrada:

- Cuando los Servidores de administración pertenecen a la misma jerarquía:
  - No es necesario realizar ninguna acción. El usuario seguirá teniendo acceso a los objetos cifrados. Las claves de cifrado se distribuyen a todos los Servidores de administración.
- Cuando los Servidores de administración son independientes:
  - Solicítele al administrador de la LAN que le brinde acceso a los objetos cifrados.
  - Restaure de datos de dispositivos cifrados con la Utilidad de restauración.
  - Restaure la configuración del Servidor de administración de Kaspersky Security Center que controló al equipo durante el cifrado desde una copia de seguridad y utilice esta configuración en el Servidor de administración que ahora controla al equipo con objetos cifrados.

Si no puede acceder a la información que se ha cifrado, siga las instrucciones especiales para el caso (Procedimiento para recuperar el acceso a archivos cifrados, Trabajar con dispositivos cifrados cuando no tenemos acceso a ellos).

Limitaciones de la función de cifrado

La característica de cifrado de datos tiene las siguientes limitaciones:

- La aplicación crea archivos de servicio durante el cifrado. Para almacenarlos, se requiere aproximadamente un 0,5 % de espacio libro sin fragmentar en el disco duro. Si no hay suficiente espacio libre sin fragmentar en el disco duro, el cifrado no iniciará hasta que libere suficiente espacio.
- Las funciones para administrar los componentes de cifrado están disponibles en la Consola de administración de Kaspersky Security Center y en Kaspersky Security Center Web Console. Kaspersky Security Center Cloud Console solo puede utilizarse para administrar BitLocker.

- Para que las funciones de cifrado estén disponibles, Kaspersky Endpoint Security debe utilizarse en conjunto con los sistemas de administración Kaspersky Security Center o Kaspersky Security Center Cloud Console (en este último caso, únicamente tendrá acceso a las funciones de BitLocker). Utilizar la característica de cifrado de datos cuando Kaspersky Endpoint Security opera en modo sin conexión no es posible porque la aplicación almacena las claves de cifrado en Kaspersky Security Center.

- Si Kaspersky Endpoint Security se ha instalado en un equipo con Microsoft Windows para servidores, la única tecnología disponible para el cifrado de discos completos será Cifrado de unidad BitLocker. Si Kaspersky Endpoint Security se ha instalado en un equipo con Microsoft Windows para estaciones de trabajo, podrán utilizarse todas las características de cifrado de datos.

- Si Kaspersky Endpoint Security está instalado en un equipo basado en Arm, solo está disponible el cifrado de disco completo con la tecnología Cifrado de unidad BitLocker, no son compatibles otros componentes de cifrado.

El cifrado de disco completo usando la tecnología de Cifrado de disco de Kaspersky no está disponible para discos duros que no cumplen con los requisitos de hardware y software.

No está soportada la compatibilidad entre la funcionalidad de cifrado de disco completo de Kaspersky Endpoint Security y Kaspersky Anti-Virus para UEFI. Kaspersky Anti-Virus para 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 para UEFI se cierre con un error. La característica de cifrado de archivos (FLE) no afecta el funcionamiento de Kaspersky Anti-Virus para UEFI.

Kaspersky Endpoint Security admite las siguientes configuraciones:

- Unidades de disco duro, SSD y USB.

  La tecnología Cifrado de disco de Kaspersky (FDE) permite trabajar con SSD y preserva el rendimiento y la vida útil de las unidades SSD.

- Unidades conectadas por bus: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Unidades no extraíbles conectadas por 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 Legacy BIOS.

- Software integrado del estándar UEFI con arranque seguro.

  Arranque seguro es una tecnología diseñada para verificar firmas digitales para aplicaciones y controladores de cargadores UEFI. El arranque seguro bloquea el inicio de aplicaciones y controladores UEFI que no están firmados o firmados por editores desconocidos. Cifrado de disco de Kaspersky (FDE) es totalmente compatible con el arranque seguro. 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 compatible con Fast Boot.

Fast Boot es una tecnología que ayuda a que el equipo se inicie más rápido. Cuando la tecnología Fast Boot está habilitada, normalmente el equipo carga solo el conjunto mínimo de controladores UEFI necesarios para iniciar el sistema operativo. Cuando la tecnología Fast Boot está habilitada, es posible que los teclados, ratones, tokens USB, paneles táctiles y pantallas táctiles USB no funcionen mientras el Agente de autenticación se está ejecutando.

Para utilizar Cifrado de disco de Kaspersky (FDE), se recomienda deshabilitar la tecnología Fast Boot. Puede usar la Utilidad de prueba FDE para poner a prueba el funcionamiento de Cifrado de disco de Kaspersky (FDE).

Kaspersky Endpoint Security no admite las siguientes configuraciones:

- El cargador del inicio está ubicado en una unidad mientras que el sistema operativo está en otra.
- El sistema contiene software integrado del estándar UEFI 32.
- El sistema tiene tecnología Intel® Rapid Start y unidades que tienen una partición de hibernación, incluso cuando la tecnología Intel® Rapid Start está deshabilitada.
- Unidades en formato MBR con más de 10 particiones extendidas.
- El sistema tiene un archivo de intercambio ubicado en una unidad que no es del sistema.
- Sistema multiarranque con varios sistemas operativos instalados a la vez.
- Particiones dinámicas (solo se admiten particiones primarias).
- Unidades con menos del 0,5 % de espacio de disco no fragmentado libre.
- Unidades con un tamaño de sector diferente 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 Cifrado de disco de Kaspersky (FDE) no es compatible con otras tecnologías de cifrado de disco completo (como BitLocker, McAfee Drive Encryption y WinMagic SecureDoc).
- La tecnología Cifrado de disco de Kaspersky (FDE) no es compatible con la tecnología ExpressCache.
- No se admite la creación, eliminación y modificación de particiones en una unidad cifrada. Podría perder datos.
- No se permite formatear el sistema de archivos. Podría perder datos.

  Si necesita formatear una unidad que se cifró con la tecnología 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 de inicio de sesión único no es compatible con otras tecnologías de desarrolladores externos.
- La tecnología Cifrado de disco de Kaspersky (FDE) no es compatible con los siguientes modelos de dispositivos:
  - Dell Latitude E6410 (modo UEFI)
  - HP Compaq nc8430 (modo Legacy BIOS)
  - Lenovo ThinkCentre 8811 (modo Legacy BIOS)
- El Agente de autenticación no admite trabajar con tokens USB cuando Legacy USB Support está habilitado. Solo se podrá utilizar la autenticación basada en contraseña en el equipo.
- Al cifrar una unidad en modo Legacy BIOS, se recomienda habilitar Legacy USB Support 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
  - PC microtorre de HP Compaq dx2450

- 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 madre)

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 depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución. Están disponibles tanto una variante de *cifrado "fuerte" (AES256)* como una de *cifrado "ligero" (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

La longitud de la clave de cifrado solo puede cambiarse en Kaspersky Endpoint Security 11.2.0 y versiones posteriores.

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 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 la capacidad de cambiar la longitud de la clave de cifrado.

Para cambiar la longitud de la clave de cifrado, ejecute los archivos 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.

Para cambiar la longitud de la clave de cifrado utilizando un paquete de distribución correspondiente a la versión que ya está instalada en el equipo, primero deberá desinstalar la aplicación.

Cifrado de Disco de Kaspersky

El Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.

La tecnología Cifrado de disco de Kaspersky puede usarse únicamente en equipos con ediciones de Windows para estaciones de trabajo. En equipos que tengan una edición de Windows para servidores, deberá utilizar 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 comenzar el cifrado de disco completo, la aplicación ejecuta una serie de verificaciones para determinar si el dispositivo puede cifrarse, lo que incluye la verificación del disco duro del sistema para detectar la compatibilidad con el Agente de autenticación o con los componentes de cifrado de BitLocker. Es necesario reiniciar el equipo para verificar la compatibilidad. Una vez reiniciado el equipo, la aplicación realiza todas las verificaciones necesarias de forma automática. Si el control de compatibilidad se realiza correctamente, el cifrado de disco completo se inicia después de que el sistema operativo y la aplicación se inician. Si se descubre que el disco duro del sistema es incompatible con el Agente de autenticación o con los componentes de cifrado de BitLocker, se deberá reiniciar el equipo presionando el botón físico para Restablecer. Kaspersky Endpoint Security lleva un registro de la información sobre la incompatibilidad. Sobre la base de esta información, la aplicación no inicia la tarea de cifrado de disco completo al inicio del sistema operativo. La información sobre este evento se mantiene en los informes de Kaspersky Security Center.

Si se cambia la configuración de hardware del equipo, se debe eliminar la información sobre incompatibilidad registrada por la aplicación durante la verificación anterior, a fin de verificar la compatibilidad del disco duro del sistema con el Agente de autenticación y con los componentes de cifrado de BitLocker. Para hacerlo, antes del cifrado de disco completo, ingrese `avp pbatestreset` en la línea de comandos. Si el sistema operativo no logra cargarse luego de verificar la compatibilidad del disco duro del sistema con el Agente de autenticación, deberá eliminar los objetos y los datos restantes luego de la operación de prueba del Agente de autenticación; para ello, emplee la Utilidad de Restauración y, luego, inicie Kaspersky Endpoint Security y vuelva a ejecutar el comando `avp pbatestreset`.

Una vez iniciado el cifrado de disco completo, Kaspersky Endpoint Security cifra todos los datos que se escriben 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 el inicio 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 sale del modo de hibernación. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el cifrado de disco completo, Kaspersky Endpoint Security reanuda el cifrado de disco completo cuando el sistema operativo sale del modo de suspensión sin cargar el Agente de autenticación.

La autenticación de usuarios en el Agente de autenticación se puede realizar de dos formas:

- Ingrese el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red LAN que está utilizando las herramientas de Kaspersky Security Center.
- Ingrese la contraseña de un token o tarjeta inteligente conectados al equipo.

  El uso de un token o de una tarjeta inteligente está disponible solo si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, se rechazará la adición del archivo de certificado electrónico al comando.

El agente de autenticación es compatible con la disposición de teclado para los siguientes idiomas:

- Inglés (Reino Unido)
- Inglés (Estados Unidos)
- Árabe (Argelia, Marruecos, Túnez; disposición AZERTY)
- Español (América Latina)
- Italiano
- Alemán (Alemania y Austria)
- Alemán (Suiza)
- Portugués (Brasil, disposición ABNT2)
- Ruso (para teclados IBM/Windows de 105 teclas con disposición QWERTY)

- Turco (disposición QWERTY)
- Francés (Francia)
- Francés (Suiza)
- Francés (Bélgica; disposición AZERTY)
- Japonés (para teclados de 106 teclas con disposición QWERTY)

Una disposición de teclado se vuelve disponible en el Agente de autenticación si se la ha agregado en la configuración de idioma y regional del sistema operativo y se ha vuelto disponible en la pantalla de bienvenida de Microsoft Windows.

Si el nombre de la cuenta del Agente de autenticación contiene símbolos que no se pueden introducir con las distribuciones de teclado disponibles en el Agente de autenticación, deberá realizar uno de dos procedimientos para poder acceder a los discos duros cifrados: realizar una restauración con la Utilidad de restauración, o restablecer el nombre de usuario y la contraseña de la cuenta 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 de la unidad correspondiente.
- Si una unidad SSD está en uso y tiene datos confidenciales, seleccione una de las siguientes opciones:
  - Limpie completamente la unidad SSD (Borrado seguro), instale el sistema operativo y ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado habilitada.
  - Ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado deshabilitada.

El cifrado de una unidad SSD requiere entre 5 y 10 GB de espacio libre. Los requisitos de espacio libre para almacenar datos de administración de cifrado se proporcionan en la siguiente tabla.

Requisitos 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

Cómo iniciar el cifrado de disco de Kaspersky

Antes de cifrar un disco completo, recomendamos verificar que el equipo no esté infectado. Para hacerlo, inicie la tarea de Análisis completo o la de Análisis de áreas críticas. La realización del cifrado de disco completo en un equipo que está infectado con un rootkit puede hacer que el equipo se vuelva inoperable.

Antes de iniciar el cifrado de disco, debe verificar la configuración de las cuentas del Agente de autenticación. El Agente de autenticación es un componente necesario para operar con unidades que se han protegido con la tecnología Cifrado de disco de Kaspersky (FDE). El usuario debe autenticarse con el Agente antes de que se cargue el sistema operativo. Kaspersky Endpoint Security permite crear las cuentas del Agente de autenticación automáticamente antes de que se cifre una unidad. La opción para que las cuentas del Agente de autenticación se creen de forma automática puede habilitarse en la configuración de la directiva de cifrado de disco completo (consulte las instrucciones a continuación). También es posible usar la tecnología de inicio de sesión único (SSO).

Kaspersky Endpoint Security le permite crear automáticamente un Agente de autenticación para los siguientes grupos de usuarios:

- **Todas las cuentas del equipo**. Todas las cuentas del equipo que estuvieron activas en cualquier momento.
- **Todas las cuentas de dominio del equipo**. Todas las cuentas del equipo que pertenecen a algún dominio y que estuvieron activas en algún momento.
- **Todas las cuentas locales del equipo**. Todas las cuentas locales del equipo que estuvieron activas en cualquier momento.
- **Cuenta del servicio con una contraseña de un solo uso**. La cuenta del servicio es necesaria para acceder al equipo (por ejemplo, cuando el usuario olvida la contraseña). También puede utilizar la cuenta del servicio como cuenta de reserva. Debe ingresar el nombre de la cuenta (de manera predeterminada, `ServiceAccount`). Kaspersky Endpoint Security crea una contraseña automáticamente. Puede encontrarla 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. De manera predeterminada, el rol de administrador del equipo no está definido (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.

Para configurar los ajustes de autenticación de los usuarios, utilice la tarea *Administrar cuentas del Agente de autenticación*. Puede usar esta tarea para agregar nuevas cuentas, modificar la configuración de las cuentas actuales o eliminar cuentas si es necesario. Puede optar por usar tareas locales para equipos específicos o tareas de grupo para selecciones de equipos o equipos que pertenezcan a diferentes grupos de administración.

Cómo ejecutar el cifrado de disco de Kaspersky 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 correspondiente 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 de Cifrado de disco de Kaspersky no se puede utilizar si el equipo tiene discos duros que fueron cifrados con 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 dichos 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 a través de 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 ficha **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 de Cifrado de disco de Kaspersky no se puede utilizar si el equipo tiene discos duros que fueron cifrados con BitLocker.

6. En el bloque **Acción en los dispositivos**, seleccione **Cifrar todos los discos duros**.

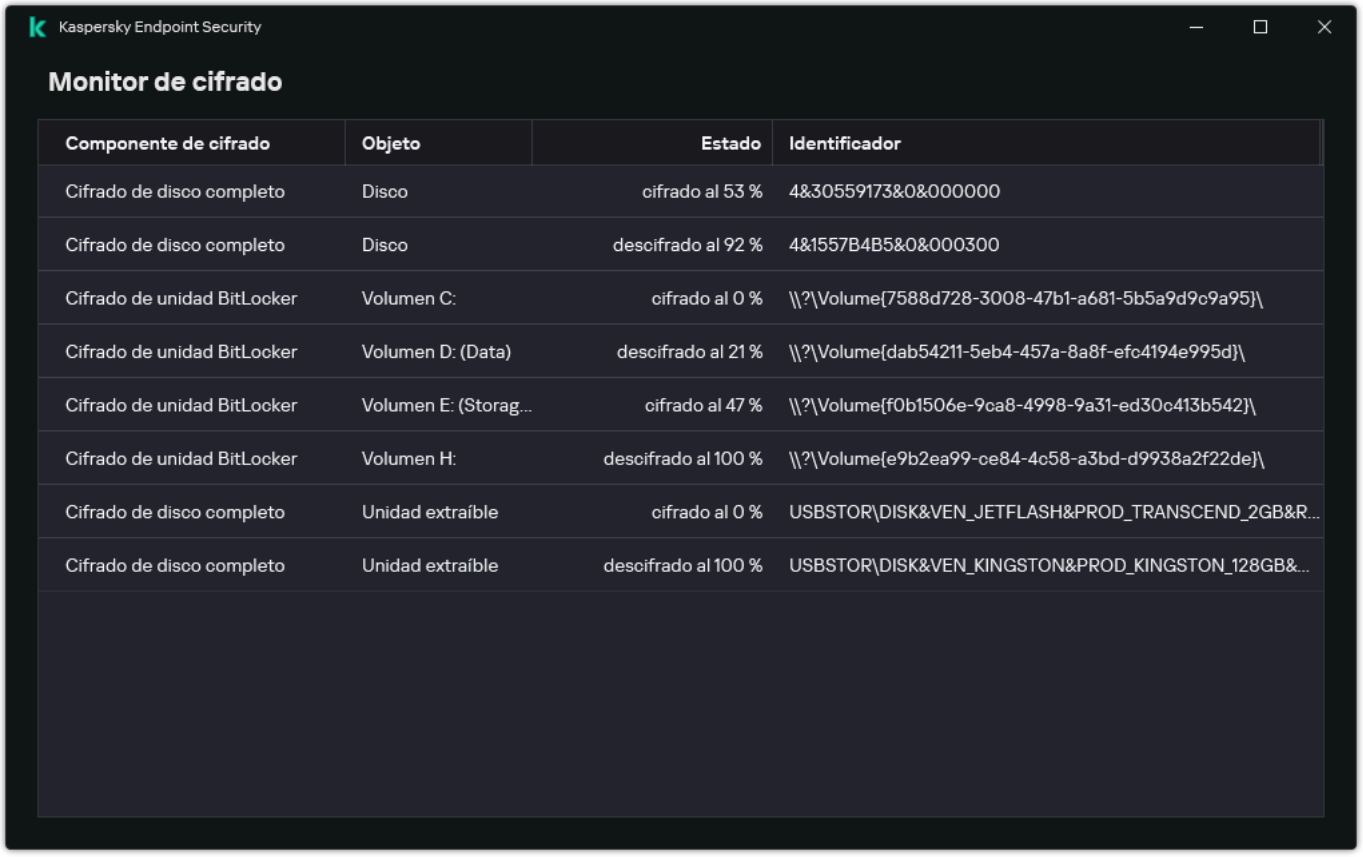
   Si el equipo tiene varios sistemas operativos instalados, después del cifrado podrá solo cargar el sistema operativo en el cual se realizó el cifrado.

   Si tiene que excluir algunos de los discos duros del cifrado, cree una lista de dichos discos duros.

7. Configure las opciones avanzadas de cifrado de disco de Kaspersky (consulte la tabla a continuación).

8. Guarde los cambios.

Si desea supervisar el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.



Monitor de cifrado

Si los discos duros del sistema están cifrados, se carga el Agente de autenticación antes del inicio del sistema operativo. Utilice el Agente de autenticación para completar el proceso de autenticación a fin de obtener acceso a los discos duros cifrados del sistema y cargar el sistema operativo. Después de la finalización correcta del procedimiento de autenticación, se carga el sistema operativo. El proceso de autenticación se repite cada vez que se reinicia el sistema operativo.

Parámetros del componente Cifrado de disco de Kaspersky

Parámetro	Descripción
Crear automáticamente cuentas de Agente de autenticación para usuarios durante cifrado	Cuando esta casilla está activada, la aplicación crea cuentas del Agente de autenticación para las cuentas de usuario de Windows disponibles en el equipo. De manera predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario haya iniciado sesión en el sistema operativo en los treinta días anteriores.
Crear automáticamente cuentas de Agente de autenticación para todos los usuarios de este equipo al iniciar sesión	Si activa esta casilla de verificación, la aplicación analizará las cuentas de Windows disponibles en el equipo antes de que se inicie el Agente de autenticación. Si detecta que una cuenta de Windows no tiene su correspondiente cuenta para el Agente de autenticación, crea esa cuenta para que el usuario pueda acceder a las unidades cifradas de su equipo. La nueva cuenta del Agente de autenticación tendrá las siguientes opciones por defecto: inicio de sesión con contraseña únicamente y cambio de contraseña obligatorio tras el primer inicio de sesión. Gracias a esta función, ya no necesitará agregar cuentas del Agente de autenticación manualmente con la tarea *Administrar cuentas del Agente de autenticación* para los equipos que ya tengan sus unidades cifradas.
Guardar el nombre de usuario utilizado 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 que ingrese el nombre de la cuenta la próxima vez que intente completar la autorización en el Agente de Autenticación bajo la misma cuenta.

Parámetro	Descripción
Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)	Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado. Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado. Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se agregan. Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente. Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De manera predeterminada, la casilla está desactivada.
Usar Legacy USB Support (no recomendado)	Esta casilla habilita/deshabilita la funcionalidad Legacy USB Support. *Legacy USB Support* es una función de la BIOS o UEFI que permite utilizar dispositivos USB (por ejemplo, tokens de seguridad) durante el arranque del equipo, en la etapa anterior al inicio del sistema operativo (modo BIOS). La funcionalidad Legacy USB Support no afecta la capacidad de usar dispositivos USB después de iniciar el sistema operativo. Si la casilla se selecciona, la compatibilidad con dispositivos USB durante el primer inicio del equipo se habilitará. Si habilita la función Legacy USB Support y el Agente de autenticación se instaló en modo BIOS, no podrá usar tokens USB. Se recomienda usar esta opción solo cuando hay un problema de compatibilidad del hardware y solo para esos equipos en los cuales el problema ocurrió.

Creación de una lista de discos duros excluidos del cifrado

Puede crear una lista de exclusiones del cifrado solo para la tecnología de Cifrado de disco de Kaspersky.

Para elaborar 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 correspondiente 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 correspondientes a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**. Esta tabla está vacía si no elaboró previamente una lista de discos duros excluidos del cifrado.

5. Para agregar discos duros a la lista de discos duros excluidos del cifrado:

   a. Haga clic en **Agregar**.

   b. En la ventana que se abre, especifique los valores de **Nombre del disp**, **Equipo**, **Tipo de disco** y **Cifrado de disco de Kaspersky**.

   c. Haga clic en **Actualizar**.

   d. En la columna **Nombre**, seleccione las casillas de las filas de la tabla que correspondan a los discos duros que quiera agregar 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. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 otro servidor.

Cómo exportar e importar una lista de exclusiones de cifrado de disco duro a la Consola de administración (MMC)

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

2. Seleccione la directiva correspondiente 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 correspondientes 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, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.

   c. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

7. Guarde los cambios.

Cómo exportar e importar una lista de exclusiones de cifrado de disco duro a 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 ficha **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 vínculo **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 que se usará para importar la lista de exclusiones.

   b. Abra el archivo.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo JSON.

8. Guarde los cambios.

Habilitación de la tecnología de inicio de sesión único (SSO)

La tecnología Single Sign-On (SSO) permite iniciar sesión en el sistema operativo automáticamente con las credenciales del Agente de autenticación. Esto significa que un usuario debe ingresar una contraseña solo una vez al iniciar sesión en Windows (la 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 cambia la contraseña de la cuenta de Windows.

Si opta por usar la tecnología SSO, el Agente de autenticación no tendrá en cuenta los requisitos que puedan haberse definido en Kaspersky Security Center para controlar la seguridad de las contraseñas. Para controlar la seguridad de las contraseñas, utilice las opciones del sistema operativo.

Habilitación de la tecnología de inicio de sesión único

Cómo habilitar el uso de la tecnología SSO 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 correspondiente 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 contraseñas**, haga clic en el botón **Configuración**.
5. En la ventana que se abre en la ficha **Agente de autenticación**, seleccione la casilla de verificación **Usar tecnología de inicio de sesión único (SSO)**.
6. Si está utilizando un proveedor de credenciales de terceros, seleccione la casilla de verificación **Cifrar proveedores de credenciales de terceros**.
7. Guarde los cambios.

Como resultado, el usuario necesitará autenticarse una sola vez, a través del Agente. No será necesario que complete el procedimiento de autenticación para que el sistema operativo se cargue. El sistema operativo se cargará automáticamente.

Cómo habilitar el uso de la tecnología SSO 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 ficha **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 contraseñas**, seleccione la casilla **Usar tecnología de inicio de sesión único (SSO)**.

7. Si está utilizando un proveedor de credenciales de terceros, seleccione la casilla de verificación **Cifrar proveedores de credenciales de terceros**.

8. Guarde los cambios.

   Como resultado, el usuario necesitará autenticarse una sola vez, a través del Agente. No será necesario que complete el procedimiento de autenticación para que el sistema operativo se cargue. El sistema operativo se cargará automáticamente.

Para poder utilizar la tecnología SSO, la contraseña de la cuenta de Windows debe ser la misma que la contraseña de la cuenta del Agente de autenticación. Si las contraseñas no son las mismas, el usuario deberá autenticarse dos veces: una vez en la interfaz del Agente de autenticación, y una segunda vez antes de que se cargue el sistema operativo. Estas acciones deben realizarse solo una vez para sincronizar las contraseñas. Tras ello, Kaspersky Endpoint Security reemplazará la contraseña de la cuenta del Agente de autenticación por la contraseña de la cuenta de Windows. Cuando se cambia 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

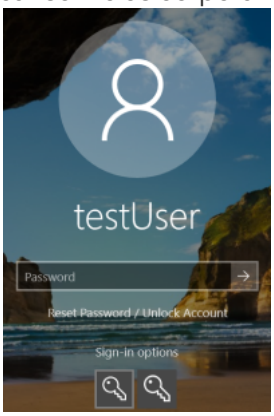
Kaspersky Endpoint Security es compatible con el proveedor de credenciales de terceros ADSelfService Plus.

Cuando se trabaja con proveedores de credenciales de terceros, el Agente de autenticación intercepta la contraseña antes de que se inicie el sistema operativo. Esto significa que un usuario debe ingresar una contraseña solo una vez al iniciar sesión en Windows. Después de iniciar sesión en Windows, el usuario puede utilizar las capacidades de un proveedor de credenciales de terceros para, por ejemplo, autenticar servicios corporativos. Los proveedores de credenciales de terceros también permiten a los usuarios restablecer su propia contraseña de forma independiente. En este caso, Kaspersky Endpoint Security actualizará automáticamente la contraseña del 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 el funcionamiento de la tecnología de inicio de sesión único. Al iniciar sesión en Windows, el usuario tendrá a su disposición dos perfiles: el proveedor de credenciales del sistema y el proveedor de credenciales de terceros. Los íconos de estos perfiles serán idénticos (consulte la imagen a continuación). Para continuar, el usuario podrá hacer lo siguiente:

- Si el usuario selecciona 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 cambió la contraseña de la cuenta de Windows, Kaspersky Endpoint Security no puede actualizar la contraseña de la cuenta del Agente de autenticación. De esta manera, el usuario deberá autenticarse dos veces: una vez en la interfaz del Agente de autenticación y una segunda vez antes de que se inicie el sistema operativo. En este caso, el usuario puede utilizar las capacidades de un proveedor de credenciales de terceros para, por ejemplo, autenticar servicios corporativos.

- Si el usuario selecciona el *proveedor de credenciales del sistema*, el Agente de autenticación sincroniza las contraseñas con la cuenta de Windows. En este caso, el usuario no puede utilizar las capacidades de un proveedor externo para, por ejemplo, autenticar servicios corporativos.



Perfil de autenticación del sistema y perfil de autenticación de terceros para iniciar sesión en Windows

Administración de cuentas del Agente de autenticación

El Agente de autenticación es un componente necesario para operar con unidades que se han protegido con la tecnología Cifrado de disco de Kaspersky (FDE). El usuario debe autenticarse con el Agente antes de que se cargue el sistema operativo. Para configurar los ajustes de autenticación de los usuarios, utilice la tarea *Administrar cuentas del Agente de autenticación*. Puede optar por usar tareas locales para equipos específicos o tareas de grupo para selecciones de equipos o equipos que pertenezcan a diferentes grupos de administración.

La ejecución de la tarea *Administrar cuentas del Agente de autenticación* no puede programarse. Tampoco es posible detener esta tarea a 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Administrar cuentas del Agente de autenticación**.

Paso 2. Selección del comando para administrar las cuentas del Agente de autenticación

Genere una lista de comandos para administrar las cuentas del Agente de autenticación. Los comandos de administración le permitirán agregar, modificar y eliminar cuentas (consulte las instrucciones más abajo). Solo los usuarios que tengan una cuenta del Agente de autenticación podrán completar el procedimiento de autenticación, cargar el sistema operativo y acceder a la unidad cifrada.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Cuentas de administrador*.

Paso 5. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Como resultado, la tarea se completará cuando el equipo vuelva a iniciarse y el nuevo usuario podrá autenticarse, cargar el sistema operativo y acceder 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 **Agregar**.

Se inicia el Asistente de tareas. 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 (14.1)**.

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**, seleccione el alcance de la tarea.

Paso 2. Administración de cuentas del Agente de autenticación

Genere una lista de comandos para administrar las cuentas del Agente de autenticación. Los comandos de administración le permitirán agregar, modificar y eliminar cuentas (consulte las instrucciones más abajo). Solo los usuarios que tengan una cuenta del Agente de autenticación podrán completar el procedimiento de autenticación, cargar el sistema operativo y acceder a la unidad cifrada.

Paso 3. Completar creación de la tarea

Salga del 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, la tarea se completará cuando el equipo vuelva a iniciarse y el nuevo usuario podrá autenticarse, cargar el sistema operativo y acceder a la unidad cifrada.

Para agregar una cuenta del Agente de autenticación, deberá agregar un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Recomendamos utilizar una tarea de grupo si, por ejemplo, desea agregar una cuenta de administración en todos los equipos.

Kaspersky Endpoint Security permite crear las cuentas del Agente de autenticación automáticamente antes de que se cifre una unidad. La opción para que las cuentas del Agente de autenticación se creen de forma automática puede habilitarse en la configuración de la directiva de cifrado de disco completo. También es posible usar la tecnología de inicio de sesión único (SSO).

Cómo agregar 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 Propiedades de la tarea, seleccione la sección **Configuración**.

3. Haga clic en **Agregar** → **Comando de adición de cuenta**.

4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows que se usará para crear la cuenta del Agente de autenticación.

5. Si escribió el nombre de la cuenta de Windows manualmente, haga clic en el botón **Permitir** para que se determine el identificador de seguridad (SID) de la cuenta.

   Si opta por no determinar el identificador de seguridad (SID) haciendo clic en el botón **Permitir**, el SID será determinado al momento de ejecutar la tarea en el equipo.

   > Determinar el identificador de seguridad de una cuenta de Windows tiene la finalidad de verificar que el nombre de la cuenta se haya escrito correctamente. Si la cuenta de Windows no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con un error.

6. Seleccione la casilla **Reemplazar cuenta existente** para que la cuenta que se cree tenga un nombre idéntico al nombre de cuenta del Agente de autenticación previamente creada que se reemplaza.

   > Este paso está disponible cuando se agrega un comando de creación de cuenta del Agente de autenticación en las propiedades de una tarea de grupo para administrar cuentas del Agente de autenticación. Este paso está disponible cuando se agrega un comando de creación de cuenta del Agente de autenticación en las propiedades de la tarea local *Administrar cuentas del Agente de autenticación*.

7. En el campo **Nombre de usuario**, escriba el nombre de la cuenta del Agente de autenticación que se debe ingresar durante la autenticación para poder acceder a discos duros cifrados.

8. Seleccione la casilla **Permitir la autenticación por contraseña** si desea que la aplicación le solicite al usuario ingresar la contraseña de la cuenta del Agente de autenticación durante la autenticación para poder acceder a discos duros cifrados. Defina una contraseña para la cuenta del Agente de autenticación. Si lo considera necesario, puede exigir que el usuario cambie la contraseña la primera vez que se autentique.

9. Seleccione la casilla **Permitir la autenticación por certificado** si desea que la aplicación le solicite al usuario que conecte un token o una tarjeta inteligente al equipo durante la autenticación para poder acceder a discos duros cifrados. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token.

10. Si es necesario, en el campo **Descripción del comando**, ingrese los detalles de la cuenta del Agente de autenticación que necesita 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 agregar 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 de propiedades de la tarea.

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

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Agregar**.

   Se abre un asistente para administrar las cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Agregar**.

6. Seleccione una cuenta de usuario. Puede escribir el nombre de la cuenta manualmente o elegir una de las disponibles en la lista de cuentas de dominio. Vaya al siguiente paso.

   Kaspersky Endpoint Security determinará el identificador de seguridad (SID) de la cuenta. Esto se hace para verificar que la cuenta se haya especificado correctamente. Si se cometió un error al escribir el nombre de usuario, Kaspersky Endpoint Security finalizará la tarea con un error.

7. Configure los ajustes de la cuenta del Agente de autenticación.

   - **Crear una nueva cuenta del Agente de autenticación para reemplazar la existente**. Kaspersky Endpoint Security hará un relevamiento de las cuentas del equipo. Si el id. de seguridad del usuario en el equipo coincide con el de la tarea, Kaspersky Endpoint Security modificará la configuración de la cuenta de usuario como lo indique la tarea.

   - **Nombre de usuario**. En una cuenta del Agente de autenticación, el nombre de usuario predeterminado se corresponde con el nombre del usuario en el dominio.

   - **Permitir la autenticación por contraseña**. Defina una contraseña para la cuenta del Agente de autenticación. Si lo considera necesario, puede exigir que el usuario cambie la contraseña la primera vez que se autentique. De este modo, cada usuario tendrá su propia contraseña. Si desea definir requisitos de seguridad para la contraseña de la cuenta del Agente de autenticación, puede hacerlo en la directiva.

   - **Permitir la autenticación por certificado**. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token. De este modo, el usuario no necesitará introducir la contraseña para usar su tarjeta inteligente o token.

   - **Acceso de la cuenta a los datos cifrados**. Configure las opciones que regularán el acceso del usuario a la unidad cifrada. Puede, por ejemplo, impedir temporalmente que un usuario se autentique en lugar de eliminar su cuenta del Agente de autenticación.

   - **Comentario**. Escriba una descripción para la cuenta, de ser necesario.

8. Guarde los cambios.

9. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

   Como resultado, la tarea se completará cuando el equipo vuelva a iniciarse y el nuevo usuario podrá autenticarse, cargar el sistema operativo y acceder a la unidad cifrada.

Para modificar la contraseña u otros datos de configuración de una cuenta del Agente de autenticación, deberá agregar un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Recomendamos utilizar una tarea de grupo si, por ejemplo, necesita reemplazar el certificado del token del administrador en todos los equipos.

Cómo modificar 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 Propiedades de la tarea, seleccione la sección **Configuración**.

3. Haga clic en **Agregar** → **Comando de modificación de cuenta**.

4. En el campo **Cuenta de Windows** de la ventana que se abre, especifique el nombre de la cuenta de Microsoft Windows que desee modificar.

5. Si escribió el nombre de la cuenta de Windows manualmente, haga clic en el botón **Permitir** para que se determine el identificador de seguridad (SID) de la cuenta.

   Si opta por no determinar el identificador de seguridad (SID) haciendo clic en el botón **Permitir**, el SID será determinado al momento de ejecutar la tarea en el equipo.

   > Determinar el identificador de seguridad de una cuenta de Windows tiene la finalidad de verificar que el nombre de la cuenta se haya escrito correctamente. Si la cuenta de Windows no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con un error.

6. Seleccione la casilla **Cambiar nombre de usuario** e ingrese un nuevo nombre para la cuenta del Agente de autenticación si desea que Kaspersky Endpoint Security cambie el nombre de usuario para todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo nombre figura en el campo **Cuenta de Windows** por el nombre que se ingrese en el campo a continuación.

7. Seleccione la casilla **Modificar la configuración de la autenticación por contraseña** para hacer modificables las configuraciones de autenticación basada en contraseña.

8. Seleccione la casilla **Permitir la autenticación por contraseña** si desea que la aplicación le solicite al usuario ingresar la contraseña de la cuenta del Agente de autenticación durante la autenticación para poder acceder a discos duros cifrados. Defina una contraseña para la cuenta del Agente de autenticación.

9. Seleccione la casilla **Modificar la regla de cambio de contraseña al autenticarse en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie el valor de la configuración de cambio de contraseña correspondiente a todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo el nombre se indica en el campo **Cuenta de Windows** por el valor de configuración que se especifica a continuación.

10. Especifique el valor de la configuración de cambio de contraseña al autenticarse en el Agente de autenticación.

11. Seleccione la casilla **Modificar la configuración de la autenticación por certificado** para hacer modificables las configuraciones de autenticación basadas en un certificado electrónico de un dispositivo o tarjeta inteligente.

12. Seleccione la casilla **Permitir la autenticación por certificado** si desea que la aplicación le solicite al usuario ingresar la contraseña del token o la tarjeta inteligente conectados al equipo durante el proceso de autenticación a fin de obtener acceso a discos duros cifrados. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token.

13. Seleccione la casilla **Modificar descripción de comando** y modifique la descripción del comando si desea que Kaspersky Endpoint Security cambie la descripción del comando correspondiente a todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo nombre se indica en el campo **Cuenta de Windows**.

14. Seleccione la casilla **Modificar la regla de acceso a la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie la regla de acceso de usuarios al cuadro de diálogo de autenticación en el Agente de autenticación por el valor especificado a continuación para todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo nombre se indica en el campo **Cuenta de Windows**.

15. Especifique la regla para acceder al cuadro de diálogo de autenticación en el Agente de autenticación.

16. Guarde los cambios.

Cómo modificar 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 de propiedades de la tarea.

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

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Agregar**.

   Se abre un asistente para administrar las cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Cambiar**.

6. Seleccione una cuenta de usuario. Puede escribir el nombre de la cuenta manualmente o elegir una de las disponibles en la lista de cuentas de dominio. Vaya al siguiente paso.

   Kaspersky Endpoint Security determinará el identificador de seguridad (SID) de la cuenta. Esto se hace para verificar que la cuenta se haya especificado correctamente. Si se cometió un error al escribir el nombre de usuario, Kaspersky Endpoint Security finalizará la tarea con un error.

7. Active las casillas ubicadas junto a los parámetros que desee modificar.

8. Configure los ajustes de la cuenta del Agente de autenticación.

   - **Crear una nueva cuenta del Agente de autenticación para reemplazar la existente**. Kaspersky Endpoint Security hará un relevamiento de las cuentas del equipo. Si el id. de seguridad del usuario en el equipo coincide con el de la tarea, Kaspersky Endpoint Security modificará la configuración de la cuenta de usuario como lo indique la tarea.

   - **Nombre de usuario**. En una cuenta del Agente de autenticación, el nombre de usuario predeterminado se corresponde con el nombre del usuario en el dominio.

   - **Permitir la autenticación por contraseña**. Defina una contraseña para la cuenta del Agente de autenticación. Si lo considera necesario, puede exigir que el usuario cambie la contraseña la primera vez que se autentique. De este modo, cada usuario tendrá su propia contraseña. Si desea definir requisitos de seguridad para la contraseña de la cuenta del Agente de autenticación, puede hacerlo en la directiva.

   - **Permitir la autenticación por certificado**. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token. De este modo, el usuario no necesitará introducir la contraseña para usar su tarjeta inteligente o token.

- **Acceso de la cuenta a los datos cifrados**. Configure las opciones que regularán el acceso del usuario a la unidad cifrada. Puede, por ejemplo, impedir temporalmente que un usuario se autentique en lugar de eliminar su cuenta del Agente de autenticación.

- **Comentario**. Escriba una descripción para la cuenta, de ser necesario.

9. Guarde los cambios.

10. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Para eliminar una cuenta del Agente de autenticación, deberá agregar un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Recomendamos utilizar una tarea de grupo si, por ejemplo, necesita eliminar la cuenta de un empleado que ha renunciado.

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 Propiedades de la tarea, seleccione la sección **Configuración**.

3. Haga clic en **Agregar** → **Comando de eliminación de cuenta**.

4. En el campo **Cuenta de Windows** de la ventana que se abre, especifique el nombre de la cuenta de usuario de Microsoft Windows que se haya utilizado para crear la cuenta del Agente de autenticación que va a eliminar.

5. Si escribió el nombre de la cuenta de Windows manualmente, haga clic en el botón **Permitir** para que se determine el identificador de seguridad (SID) de la cuenta.

   Si opta por no determinar el identificador de seguridad (SID) haciendo clic en el botón **Permitir**, el SID será determinado al momento de ejecutar la tarea en el equipo.

   > Determinar el identificador de seguridad de una cuenta de Windows tiene la finalidad de verificar que el nombre de la cuenta se haya escrito correctamente. Si la cuenta de Windows no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con un 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 de propiedades de la tarea.

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

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Agregar**.

   Se abre un asistente para administrar las cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Eliminar**.

6. Seleccione una cuenta de usuario. Puede escribir el nombre de la cuenta manualmente o elegir una de las disponibles en la lista de cuentas de dominio.

7. Guarde los cambios.

8. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

   Como resultado, la tarea se completará cuando el equipo vuelva a iniciarse y el usuario no podrá autenticarse ni cargar el sistema operativo. Kaspersky Endpoint Security no permitirá que el usuario acceda a la información cifrada.

Para ver una lista de usuarios que pueden autenticarse con el Agente y cargar el sistema operativo, debe consultar 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 en un equipo para abrir su ventana de propiedades.

4. En la ventana de propiedades del equipo, elija 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 Propiedades de la tarea, seleccione la sección **Configuración**.

   Como resultado, obtendrá acceso a la lista de cuentas del Agente de autenticación presentes en el equipo. Solo los usuarios que figuren en esa lista podrán autenticarse con el Agente y cargar el sistema operativo.

Cómo ver la lista de cuentas del Agente de autenticación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.

2. Haga clic en el nombre del equipo vinculado a las cuentas del Agente de autenticación en las que esté interesado.

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 Propiedades de la tarea, seleccione la pestaña **Configuración de la aplicación**.

   Como resultado, obtendrá acceso a la lista de cuentas del Agente de autenticación presentes en el equipo. Solo los usuarios que figuren en esa lista podrán autenticarse con el Agente y cargar el sistema operativo.

Uso de un token y de una tarjeta inteligente con el Agente de autenticación

Se puede utilizar un token o una tarjeta inteligente para la autenticación cuando se está accediendo a discos duros cifrados. Para utilizar este método, es necesario agregar el archivo del certificado electrónico del token o tarjeta inteligente a la tarea *Administrar cuentas del Agente de autenticación*.

El uso de un token o de una tarjeta inteligente está disponible solo si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, se rechazará la adición del archivo de certificado electrónico al comando.

Kaspersky Endpoint Security es compatible con los siguientes dispositivos, lectores de tarjetas inteligentes y tarjetas inteligentes:

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K 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 72K Java
- Aladdin-RD JaCarta PKI

Para agregar el archivo de certificado electrónico de un token o de una tarjeta inteligente al comando para crear una cuenta del Agente de autenticación, primero deberá exportar el archivo con software de otros proveedores para la administración de certificados, y guardar el archivo.

El certificado del token o de la tarjeta inteligente debe tener las siguientes propiedades:

- El certificado debe cumplir con el estándar X.509, y el archivo del certificado debe tener el cifrado 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 inteligente no cumple con estos requisitos, el archivo del certificado no podrá incluirse en el comando con el que se crean las cuentas del Agente de autenticación.

El parámetro `KeyUsage` del certificado debe tener los valores `keyEncipherment` o `dataEncipherment`. El parámetro `KeyUsage` determina la finalidad del certificado. Si el parámetro tiene cualquier otro valor, Kaspersky Security Center descargará el archivo del certificado, pero mostrará una advertencia.

Si un usuario pierde su tarjeta inteligente o token, el administrador deberá agregar el archivo del certificado electrónico de una tarjeta inteligente o token de reemplazo al comando que se utiliza para crear las cuentas del Agente de autenticación. A continuación, el usuario debe completar el procedimiento de recibir acceso a dispositivos cifrados o restaurar datos en los dispositivos cifrados.

Descifrado de discos duros

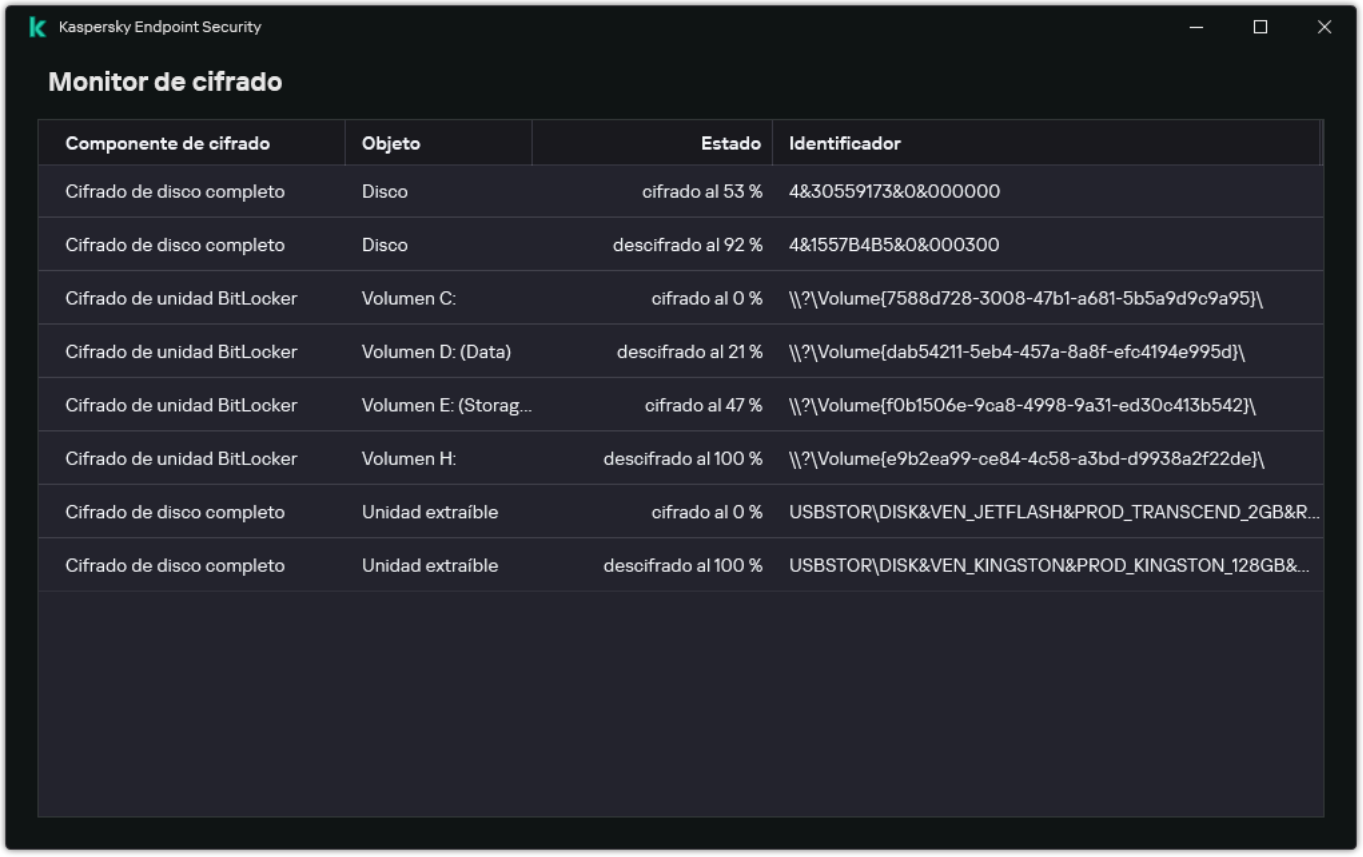
Puede descifrar discos duros aun si no hay licencia actual que permita el cifrado de datos.

Para descifrar discos duros:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 cual 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** si quiere descifrar todos los discos duros cifrados.
   - Agregue los discos duros cifrados que quiera descifrar a la tabla **No cifrar los siguientes discos duros**.

     Esta opción solo está disponible para la tecnología de Cifrado de disco de Kaspersky.
6. Guarde los cambios.

Si desea supervisar el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.



Componente de cifrado	Objeto	Estado	Identificador
Cifrado de disco completo	Disco	cifrado al 53 %	4&30559173&0&000000
Cifrado de disco completo	Disco	descifrado al 92 %	4&1557B4B5&0&000300
Cifrado de unidad BitLocker	Volumen C:	cifrado al 0 %	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
Cifrado de unidad BitLocker	Volumen D: (Data)	descifrado al 21 %	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
Cifrado de unidad BitLocker	Volumen E: (Storag...	cifrado al 47 %	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
Cifrado de unidad BitLocker	Volumen H:	descifrado al 100 %	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
Cifrado de disco completo	Unidad extraíble	cifrado al 0 %	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
Cifrado de disco completo	Unidad extraíble	descifrado al 100 %	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

Monitor de cifrado

Si el usuario apaga o reinicia el equipo durante el descifrado del disco duro cifrado con 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 de discos duros después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo.

Si el sistema operativo pasa al modo de hibernación mientas se están descifrando discos duros cifrados con 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 de discos duros después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo. Después del descifrado de discos duros, el modo de hibernación no está disponible hasta el primer reinicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el descifrado de discos duros, Kaspersky Endpoint Security reanuda el descifrado cuando el sistema operativo sale del modo de suspensión sin cargar el Agente de autenticación.

Restaurar el acceso a una unidad protegida con la tecnología Cifrado de disco de Kaspersky

Si un usuario olvida la contraseña que le permite acceder a un disco duro protegido con la tecnología de Cifrado de disco de Kaspersky, debe iniciar el procedimiento de recuperación (un procedimiento de solicitud y respuesta). También puede utilizar la cuenta del servicio para acceder al disco duro si esta característica está habilitada en la configuración de cifrado del disco.

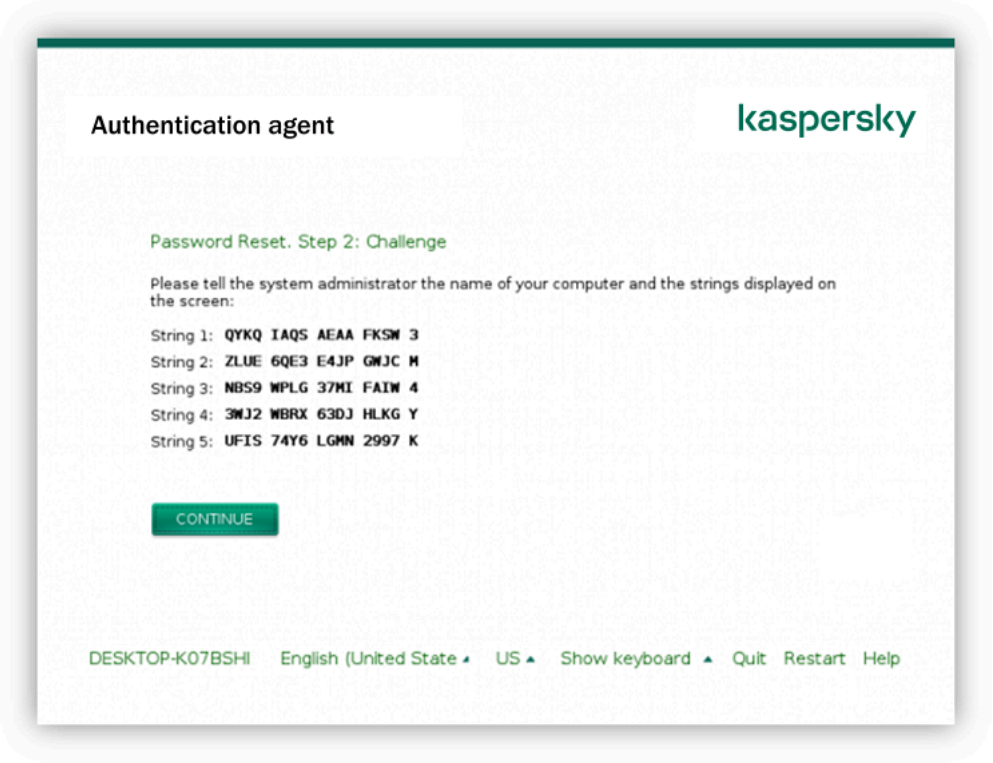
Restaurar el acceso al disco duro del sistema

El siguiente es el procedimiento para restaurar el acceso a un disco duro del sistema que se ha protegido con la tecnología de Cifrado de disco de Kaspersky:

1. El usuario le indica al administrador cuáles son los bloques de su solicitud (vea la imagen de más abajo).

2. El administrador introduce los bloques de la solicitud en Kaspersky Security Center, obtiene los bloques de respuesta y se los comunica al usuario.

3. El usuario escribe los bloques de la respuesta en la interfaz del Agente de autenticación y obtiene acceso al disco duro.



Restaurar el acceso a un disco duro del sistema protegido con Cifrado de disco de Kaspersky

Para iniciar el procedimiento de recuperación, el usuario debe hacer clic en el vínculo **Forgot your password** que se muestra en la interfaz del Agente de autenticación.

Cómo obtener, mediante la Consola de administración (MMC), los bloques de respuesta para un disco duro del sistema protegido con Cifrado de disco de Kaspersky

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 del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.

4. En el menú contextual, seleccione **Otorgar acceso en el modo sin conexión**.

5. En la ventana que se abre, seleccione la pestaña **Agente de autenticación**.

6. En el bloque **Algoritmo de cifrado en uso**, seleccione un algoritmo de cifrado: **AES56** o **AES256**.

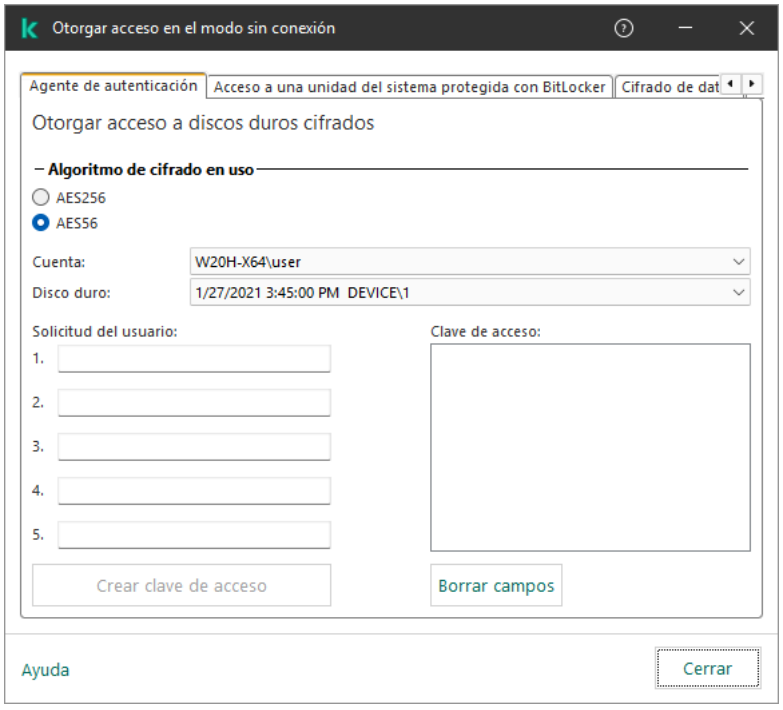
   El algoritmo de cifrado depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución. *Cifrado fuerte (AES256)* o *Cifrado ligero (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

7. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación creada para el usuario que necesita acceder al disco.

8. En la lista desplegable **Disco duro**, seleccione el disco duro cifrado para el cual tiene que recuperar el acceso.

9. En el bloque **Solicitud del usuario**, complete los bloques de solicitud según lo indica el usuario.

Como resultado, en el campo **Clave de acceso** se mostrarán los bloques generados en respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de su cuenta del Agente de autenticación. Indíquele al usuario el contenido de estos bloques.



Otorgar acceso en el modo sin conexión

Cómo obtener, mediante Web Console, los bloques de respuesta para un disco duro del sistema protegido con Cifrado de disco de Kaspersky

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.

2. Active la casilla ubicada junto al nombre del equipo en el que se encuentre la unidad a la que se necesite acceso.

3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.

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 de usuario y la contraseña de la cuenta del Agente de autenticación.

6. Escriba los bloques de solicitud que haya recibido del usuario.

Como resultado, en la parte inferior de la ventana se mostrarán los bloques generados en respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de su cuenta del Agente de autenticación. Indíquele al usuario el contenido de estos bloques.

Una vez que se complete el procedimiento de recuperación, el Agente de autenticación le pedirá al usuario que cambie la contraseña.

Restaurar el acceso a un disco duro que no sea el del sistema

El siguiente es el procedimiento para restaurar el acceso a un disco duro que no es el del sistema y que se ha protegido con la tecnología de Cifrado de disco de Kaspersky:

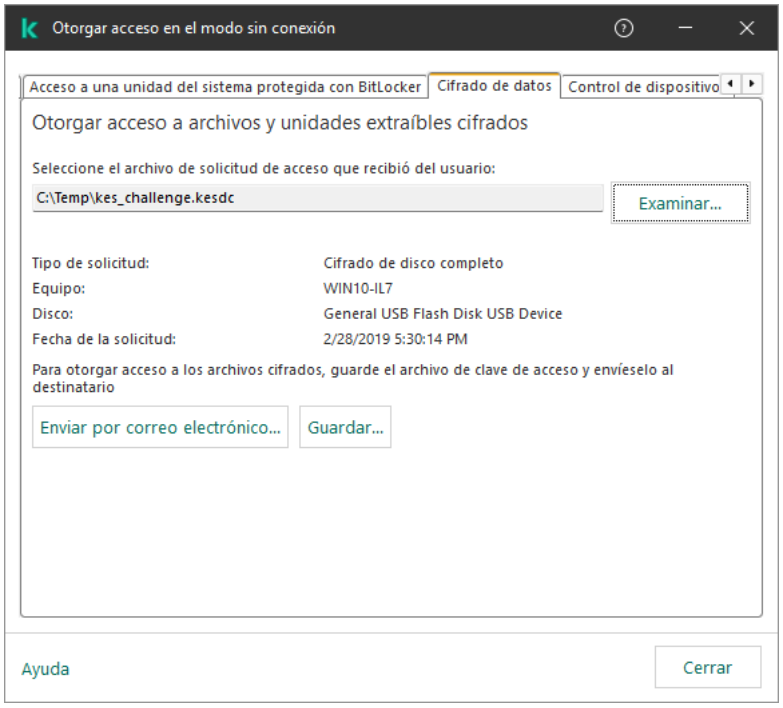
1. El usuario le envía al administrador un archivo de solicitud de acceso.
2. El administrador agrega el archivo de solicitud de acceso en Kaspersky Security Center; a continuación, crea un archivo de clave de acceso y se lo envía al usuario.
3. El usuario agrega el archivo de clave de acceso en Kaspersky Endpoint Security y obtiene acceso al disco duro.

Para iniciar el procedimiento de recuperación, el usuario debe tratar de acceder al disco duro. Cuando lo haga, Kaspersky Endpoint Security creará un archivo de solicitud de acceso, que tendrá la extensión KESDC. El usuario deberá enviarle ese archivo al administrador por correo electrónico o por cualquier otro medio.

Cómo obtener, mediante la Consola de administración (MMC), un archivo de clave de acceso para un disco duro cifrado que no sea el del sistema

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 del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
4. En el menú contextual, seleccione **Otorgar acceso en el modo sin conexión**.
5. En la ventana que se abre, seleccione la pestaña **Cifrado de datos**.
6. En la ficha **Cifrado de datos**, haga clic en el botón **Examinar**.
7. En la ventana para seleccionar el archivo de solicitud de acceso, especifique la ruta al archivo que le haya enviado el usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.



Otorgar acceso en el modo sin conexión

Cómo obtener, mediante Web Console, un archivo de clave de acceso para un disco duro cifrado que no sea el del sistema

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los archivos a los que se necesite acceso.
3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.
4. Seleccione **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión KESDC).

   Web Console le mostrará información sobre la solicitud. Encontrará, entre otros datos, el nombre del equipo que contiene los archivos a los que el usuario necesita acceder.
6. Haga clic en el botón **Guardar clave** y seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión KESDR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

Inicio de sesión con la cuenta del servicio del Agente de autenticación

Kaspersky Endpoint Security le permite agregar una cuenta del servicio de Agente de autenticación al cifrar un dispositivo. La cuenta del servicio es necesaria para acceder al equipo (por ejemplo, cuando el usuario olvida la contraseña). También puede utilizar la cuenta del servicio como cuenta de reserva. Para agregar una cuenta, seleccione una cuenta del servicio en Configuración de cifrado de disco e ingrese el nombre de la cuenta de usuario (de manera predeterminada, `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 en un equipo para abrir su ventana de propiedades.
4. En la ventana de propiedades del equipo, elija 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 del 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 **Mostrar contraseña original**.
10. Copie la contraseña de un solo uso para iniciar sesión con la cuenta del servicio.

Cómo averiguar 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 vinculado a las cuentas del Agente de autenticación en las que esté interesado.

   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 Propiedades de la tarea, seleccione la pestaña **Configuración de la aplicación**.
6. En la lista de cuentas, seleccione la cuenta del servicio del Agente de autenticación (por ejemplo, `WIN10-USER\ServiceAccount`).

7. En las propiedades de la cuenta, seleccione la casilla **Mostrar contraseña**.

8. Copie la contraseña de un solo uso para iniciar sesión con la cuenta del servicio.

Kaspersky Endpoint Security actualiza automáticamente la contraseña cada vez que un usuario se autentica con la cuenta del servicio. Después de autenticarse con el agente, debe ingresar la contraseña de la cuenta de Windows. No puede utilizar la tecnología SSO si inicia sesión con la cuenta del servicio.

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 cargador del SO no podrá acceder al disco cifrado y usted podría quedar sin acceso al equipo.

Funciones 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 una imagen 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 a una carpeta diferente. 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.14.1\reflect_drivers
     ```

> La actualización automática del sistema operativo solo está disponible si el equipo ejecuta Windows 10 1607 (RS1) o una versión superior. Para actualizar versiones anteriores del sistema operativo, se recomienda que primero descifre el disco, actualice el sistema operativo y, luego, cifre el disco.

Cuando se utiliza la tecnología Cifrado de unidad BitLocker, no es necesario descifrar los discos duros para actualizar Windows 10. Para más información sobre BitLocker, visite el sitio web de Microsoft.

Eliminación de errores de actualización de la funcionalidad de cifrado

Cuando Kaspersky Endpoint Security para Windows se actualiza a la versión 14.1, también se actualiza la característica Cifrado de disco completo.

Al iniciar la actualización de la funcionalidad Cifrado de disco completo, pueden ocurrir los siguientes errores:

- No se puede inicializar 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 funcionalidad de Cifrado de disco completo en la nueva versión de la aplicación:

1. Descifrar discos duros.
2. Cifrar discos duros una vez más.

Durante la actualización de la funcionalidad 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 completó con un error.

Para eliminar los errores que ocurrieron durante el proceso de actualización de la funcionalidad Cifrado de disco completo,

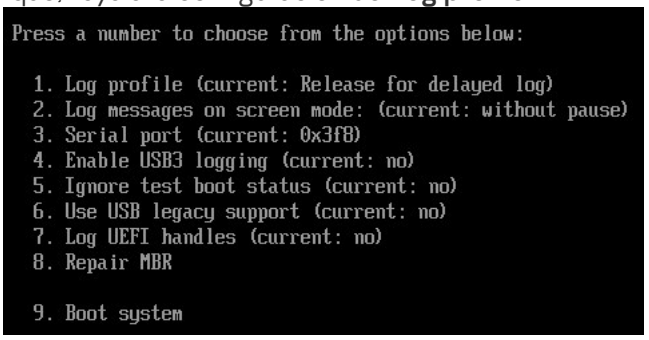
restaurar acceso a dispositivos cifrados con la Utilidad de Restauración.

Seguimiento del Agente de autenticación

La aplicación registra información de servicio sobre el funcionamiento del Agente de autenticación e información acerca de las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

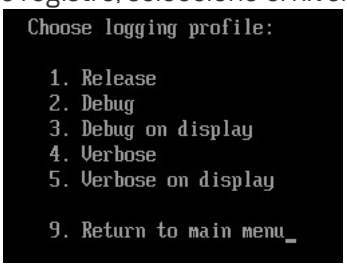
Para habilitar el seguimiento del Agente de autenticación:

1. Habilite el seguimiento de Kaspersky Endpoint Security.
2. Reinicie el equipo.
3. Tan pronto se inicie un equipo con discos duros cifrados, presione el botón **F3** para abrir una ventana para configurar los parámetros del Agente de autenticación.
4. Una vez iniciado el cargador de arranque de FDE, seleccione el gestor de arranque **KES (FDE <version>)**.
5. En el menú del gestor de arranque, vaya a la configuración de **Log profile**.



Menú del gestor de arranque

6. En la ventana de configuración del perfil de registro, seleccione el nivel de seguimiento:



Niveles de seguimiento del Agente de autenticación

- **Release**. Si se selecciona esta opción, la aplicación no registra la información sobre eventos del Agente de autenticación en el archivo de seguimiento.

- **Debug**. Si se selecciona esta opción, la aplicación registra la información sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

- **Debug on display**. Si se selecciona esta opción, la aplicación registra la información sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento, y las transmite mediante el puerto COM.

  Si se conecta un equipo con discos duros cifrados a otro equipo mediante el puerto COM, se pueden examinar los eventos del Agente de autenticación 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 realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

  El nivel de detalle de las entradas de esta opción es mayor en comparación con el nivel de la opción **Debug**. Un nivel más alto 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 registra información detallada sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento, y las transmite mediante el puerto COM.

  El nivel de detalle de las entradas de esta opción es mayor en comparación con el nivel de la opción **Debug on display**. Un nivel más alto 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 gestor de arranque muestra nuevamente el menú.

7. En el menú del gestor de arranque, seleccione **Boot system**.

   El cargador de arranque de 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, regrese a la ventana Herramientas de soporte y deshabilite el seguimiento.

Como resultado, los archivos de seguimiento de las operaciones del Agente de autenticación KES.SRV se crean en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\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 es necesario, puede enviar el archivo de seguimiento del Agente de autenticación a Kaspersky en forma manual para su análisis.

Edición de los textos de ayuda del Agente de autenticación

Antes de modificar los mensajes de ayuda del Agente de autenticación, consulte la lista de caracteres que pueden usarse en un entorno de prearranque (véase más abajo).

Para modificar 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 correspondiente 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 ficha **Autenticación** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se están ingresando las credenciales de la cuenta.
   - Seleccione la ficha **Cambiar contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se está cambiando la contraseña correspondiente a la cuenta del Agente de autenticación.
   - Seleccione la ficha **Recuperar contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se está recuperando la contraseña correspondiente a la cuenta del Agente de autenticación.
6. Modifique los mensajes de ayuda.

   Si quiere restaurar el texto original, haga clic en el botón **Predeterminado**.

   Puede ingresar texto de ayuda que contenga 16 líneas o menos. La longitud máxima de una línea es 64 caracteres.
7. Guarde los cambios.

Compatibilidad limitada de caracteres en los mensajes de ayuda del Agente de autenticación

En un entorno previo al inicio, se admiten los siguientes caracteres Unicode:

- Alfabeto latino básico (0000 - 007F)
- Caracteres latinos adicionales-1 (0080 - 00FF)

- Caracteres latinos extendidos-A (0100 - 017F)
- Caracteres latinos extendidos-B (0180 - 024F)
- Caracteres de ID extendidos sin combinar (02B0 - 02FF)
- Marcas diacríticas combinadas (0300 - 036F)
- Alfabetos griego y copto (0370 - 03FF)
- Alfabeto cirílico (0400 - 04FF)
- Hebreo (0590 - 05FF)
- Alfabeto árabe (0600 - 06FF)
- Latín extendido adicional (1E00 - 1EFF)
- Signos de puntuación (2000 - 206F)
- Símbolos de divisa (20A0 - 20CF)
- Símbolos semejantes a letras (2100 - 214F)
- Figuras geométricas (25A0 - 25FF)
- Formas de presentación del alfabeto árabe-B (FE70 - FEFF)

Los caracteres que no se especifican en esta lista no se admiten en un entorno previo al inicio. No se recomienda usar dichos caracteres en mensajes de ayuda del Agente de autenticación.

Eliminación de objetos y datos residuales tras evaluar el funcionamiento del Agente de autenticación

Durante la desinstalación de aplicación, si Kaspersky Endpoint Security detecta objetos y datos que permanecen en el disco duro del sistema después de la operación de prueba del Agente de autenticación, se interrumpe la desinstalación de aplicación y no puede reiniciarse hasta eliminar dichos objetos y datos.

Los objetos y datos pueden permanecer en el disco duro del sistema después de la operación de prueba del Agente de autenticación solo en casos excepcionales. Por ejemplo: esto puede suceder si el equipo no se ha reiniciado luego de haber aplicado una directiva de Kaspersky Security Center con configuración de cifrado, o en caso de que la aplicación no pueda iniciarse luego de una 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:

- Con la directiva de Kaspersky Security Center.
- Con la Utilidad de restauración.

Para usar una directiva de Kaspersky Security Center para eliminar objetos y datos restantes después de la operación de prueba del Agente de autenticación:

1. Aplique al equipo una directiva de Kaspersky Security Center con parámetros configurados para descifrar todos los discos duros del equipo.

2. Inicie Kaspersky Endpoint Security.

Para usar la Utilidad de restauración para eliminar objetos y datos que quedaron después de la operación de prueba del Agente de autenticación:

1. Ejecute el archivo fdert.exe (el archivo ejecutable de la Utilidad de restauración). Este archivo es creado por Kaspersky Endpoint Security.

2. En la ventana de la Utilidad de restauración, seleccione el dispositivo necesario.

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** está disponible solo si se detectan objetos y datos restantes después de la operación de prueba del Agente de autenticación.

Para quitar información sobre incompatibilidad de aplicaciones con el Agente de autenticación,

escriba el comando `avp pbatestreset` en la línea de comandos.

Administración de BitLocker

BitLocker es una tecnología de cifrado que forma parte de los sistemas operativos Windows. Kaspersky Endpoint Security le permite controlar y administrar BitLocker a través de la infraestructura de Kaspersky Next. La tecnología BitLocker está diseñada para cifrar volúmenes lógicos. No puede utilizarse para cifrar unidades extraíbles. Para más información sobre BitLocker, puede consultar la documentación de Microsoft.

Al cifrar el disco, BitLocker coloca el cargador de arranque y otros archivos auxiliares en system partition. Esta partición no está cifrada. El sistema operativo crea la partición del sistema automáticamente durante la instalación de Windows. Si todo el disco está particionado antes de instalar Windows, el sistema operativo no podrá crear una partición del sistema. En este caso, cuando inicie el cifrado de disco BitLocker, el sistema operativo le pide al usuario 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 BitLocker.

El algoritmo de cifrado BitLocker no depende de la versión de la biblioteca AES versión incluida en el paquete de distribución (AES256 o AES56). El cifrado utiliza la biblioteca de cifrado integrada del 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 han sido cifrados. Para los dispositivos que ya estaban cifrados antes de instalarse 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.

Las claves de acceso de BitLocker pueden almacenarse de manera segura utilizando un TPM (módulo de plataforma segura). Un *Trusted Platform Module (TPM)* es un microchip que proporciona funciones de seguridad básicas (entre ellas, la capacidad de almacenar claves de cifrado). Por lo general, el TPM forma parte de la placa madre del equipo e interactúa con los demás componentes del sistema a través de un bus físico. Es la opción más segura para almacenar las claves de acceso de BitLocker porque permite verificar la integridad del sistema antes del arranque. La ausencia de un TPM no es impedimento para cifrar las unidades de un equipo. En tal caso, se utiliza una contraseña para cifrar la clave de acceso. BitLocker permite emplear los siguientes métodos de autenticación:

- TPM.
- PIN y TPM.
- Contraseña.

Cuando la unidad del sistema está cifrada, el usuario debe superar la autenticación de BitLocker para iniciar el sistema operativo. Después de la autenticación, BitLocker permite que el usuario inicie sesión. BitLocker no es compatible con la tecnología de inicio de sesión único (SSO).

Cuando se cifra una unidad, BitLocker crea una clave de recuperación. Kaspersky Endpoint Security envía la clave de recuperación a Kaspersky Security Center; ello le permitirá restaurar el acceso al disco si, por ejemplo, un usuario olvida su contraseña.

Si un usuario cifra un disco con BitLocker, Kaspersky Endpoint Security enviará la clave de recuperación y la información sobre el cifrado de disco a Kaspersky Security Center.

Si utiliza directivas de grupo de Windows, deshabilite el control de BitLocker en las mismas. Las directivas de Windows pueden interferir con las de Kaspersky Security Center. Tales interferencias pueden derivar en errores de cifrado.

Activación del Cifrado de unidad BitLocker

Antes de cifrar un disco completo, recomendamos verificar que el equipo no esté infectado. Para hacerlo, inicie la tarea de Análisis completo o la de Análisis de áreas críticas. La realización del cifrado de disco completo en un equipo que está infectado con un rootkit puede hacer que el equipo se vuelva inoperable.

Para usar la tecnología Cifrado de unidad BitLocker en equipos que tengan una edición de Windows diseñada para servidores, es posible que primero necesite instalar el componente Cifrado de unidad BitLocker. Utilice para ello las herramientas que brinda el sistema operativo (el Asistente para agregar roles y características). Consulte la documentación de Microsoft para más información sobre cómo instalar Cifrado de unidad BitLocker.

Cómo activar el Cifrado de unidad 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 correspondiente 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 podrá solo cargar el sistema operativo en el cual se realizó el cifrado.

6. Configure las opciones avanzadas de Cifrado de unidad BitLocker (vea la tabla de más abajo).

7. Guarde los cambios.

Cómo activar el Cifrado de unidad BitLocker a través de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Cifrado de datos** → **Cifrado de disco completo**.

5. Seleccione la tecnología **Cifrado de disco BitLocker**.

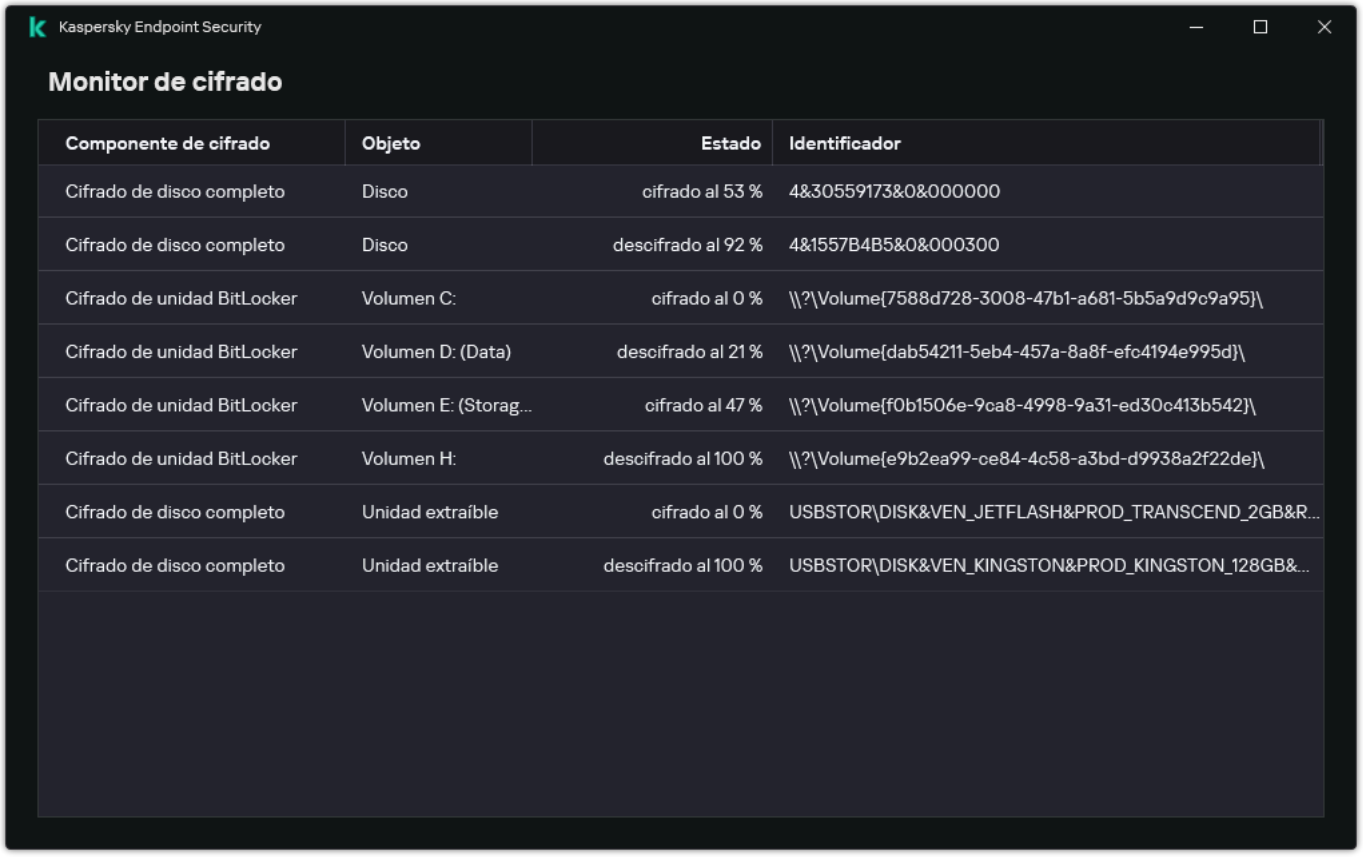
6. En el bloque **Acción en los dispositivos**, seleccione **Cifrar todos los discos duros**.

> Si el equipo tiene varios sistemas operativos instalados, después del cifrado podrá solo cargar el sistema operativo en el cual se realizó el cifrado.

7. Configure las opciones avanzadas de Cifrado de unidad BitLocker (vea la tabla de más abajo).

8. Guarde los cambios.

Si desea supervisar el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.



Componente de cifrado	Objeto	Estado	Identificador
Cifrado de disco completo	Disco	cifrado al 53 %	4&30559173&0&000000
Cifrado de disco completo	Disco	descifrado al 92 %	4&1557B4B5&0&000300
Cifrado de unidad BitLocker	Volumen C:	cifrado al 0 %	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
Cifrado de unidad BitLocker	Volumen D: (Data)	descifrado al 21 %	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
Cifrado de unidad BitLocker	Volumen E: (Storag...	cifrado al 47 %	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
Cifrado de unidad BitLocker	Volumen H:	descifrado al 100 %	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
Cifrado de disco completo	Unidad extraíble	cifrado al 0 %	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
Cifrado de disco completo	Unidad extraíble	descifrado al 100 %	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

Monitor de cifrado

Luego de aplicar la directiva, la aplicación muestra las siguientes preguntas, según la configuración de la autenticación:

- Solo TPM. No se requiere la entrada del usuario. El disco se cifrará cuando el equipo se reinicie.
- TPM + PIN / Contraseña. Si se encuentra disponible un módulo de TPM, aparece una ventana para escribir el código PIN. Si no hay disponible un módulo de TPM, se mostrará una ventana para escribir la contraseña de autenticación previa al inicio.
- Solo contraseña. Verá una ventana de solicitud de contraseña para la autenticación previa al inicio.

Si el modo de compatibilidad estándar del Procesamiento de información federal está habilitado para el sistema operativo del equipo, entonces en Windows 8 y las versiones anteriores del sistema operativo, se muestra una solicitud para conectar un dispositivo de almacenamiento para guardar el archivo de clave de recuperación. Es posible guardar varios archivos de clave de recuperación en un mismo dispositivo de almacenamiento.

Una vez que defina el PIN o la contraseña, BitLocker le pedirá que reinicie el equipo. Esto es necesario para que se complete el proceso de cifrado. El usuario deberá luego superar el procedimiento de autenticación de BitLocker. Tras autenticarse, el usuario tendrá que iniciar sesión en el sistema. El proceso de cifrado con BitLocker se completará una vez que se cargue el sistema operativo.

De no tener acceso a las claves de cifrado, el usuario puede solicitar una clave de recuperación al administrador de la red de área local (en el caso de que la clave de recuperación se haya perdido o de que no se la haya guardado en el dispositivo de antemano).

Parámetros del componente Cifrado de unidad BitLocker

Parámetro	Descripción
Habilitar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en tabletas	Usar la autenticación que requiere el ingreso de datos en un entorno previo al inicio del sistema, aun si la plataforma no tiene la capacidad de ingreso previo al inicio del sistema (por ejemplo, con teclados de pantalla táctil en tabletas). La pantalla táctil de las tabletas no está disponible en el entorno previo al inicio. Para completar la autenticación de BitLocker en tabletas, el usuario debe, por ejemplo, conectar un teclado USB. Si se selecciona la casilla de verificación, se permite el uso de la autenticación que requiere ingreso previo al inicio del sistema. Se recomienda usar esta configuración solo para dispositivos que tienen herramientas alternativas de ingreso de datos en un entorno previo al inicio del sistema, como ser, un teclado USB además de teclados de pantalla táctil. Para poder usar la tecnología Cifrado de unidad BitLocker en una tableta, esta casilla debe estar activada.
Usar cifrado de hardware (Windows 8 y versiones posteriores)	Si se selecciona la casilla de verificación, la aplicación implementa cifrado del hardware. Esto le permite aumentar la velocidad de cifrado y usar menos recursos del equipo.
Cifrar solo el espacio de disco usado (Windows 8 y versiones posteriores)	Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado. Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado. Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se agregan. Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente. Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De manera predeterminada, la casilla está desactivada.

Parámetro	Descripción
Método de autenticación	**Solo contraseña (Windows 8 y versiones posteriores)** Si se selecciona esta opción, Kaspersky Endpoint Security le solicita al usuario una contraseña cuando intenta acceder a una unidad cifrada. Esta opción se puede seleccionar cuando no se está utilizando un Módulo de plataforma segura (TPM). **Módulo de plataforma segura (TPM)** Si se selecciona esta opción, BitLocker usa un Módulo de plataforma segura (TPM). Un *Trusted Platform Module (TPM)* es un microchip que proporciona funciones de seguridad básicas (entre ellas, la capacidad de almacenar claves de cifrado). Suele haber un Módulo de plataforma segura instalado en la placa madre del equipo y este módulo interactúa con todos los demás 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 se pueden descifrar con el dispositivo. Un Módulo de plataforma segura cifra claves de cifrado con su propia clave de almacenamiento raíz. La clave de almacenamiento raíz se almacena dentro del Módulo de plataforma segura. Esto proporciona un nivel adicional de protección contra intentos de ataque a 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: • **Usar PIN para TPM**. Si activa esta casilla, los usuarios podrán usar un código PIN para obtener acceso a una clave de cifrado almacenada en un módulo de plataforma segura (TPM). Si desactiva esta casilla, los usuarios no podrán usar un código PIN. Para acceder a la clave de cifrado, deberán utilizar una contraseña. • **Módulo de plataforma segura (TPM), o contraseña si el TPM no se encuentra disponible**. Si se selecciona esta opción, el usuario puede usar una contraseña para obtener acceso a claves de cifrado cuando un módulo de plataforma segura (TPM) no está disponible. Si desactiva esta casilla y no hay un módulo TPM disponible, la función de cifrado de disco completo no se iniciará. El método de autenticación seleccionado debe configurarse mediante la especificación de requisitos de contraseña o PIN: • **Longitud mínima de PIN (caracteres)**. • **Longitud mínima de la contraseña (caracteres)**. • **Limitar el periodo de validez de la contraseña o del PIN para el TPM (días)**. • **Usar un PIN mejorado (letras y números)**. El *código PIN mejorado* permite usar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.
Recrear automáticamente clave de recuperación (días)	Actualice automáticamente la contraseña para restaurar el acceso a una unidad protegida con BitLocker. Si se selecciona la casilla de verificación, especifique el período de validez de la contraseña con clave de recuperación. Esto ayuda a prevenir la reutilización de la contraseña con clave de recuperación.

Cómo descifrar un disco duro protegido con BitLocker

Puede suceder que un usuario descifre su disco duro utilizando la función *Desactivar BitLocker* del sistema operativo. Si esto ocurre, Kaspersky Endpoint Security le pedirá al usuario repetidamente que vuelva a cifrar la unidad. Para que Kaspersky Endpoint Security deje de hacer esta solicitud, será necesario habilitar el descifrado de la unidad en la directiva.

Cómo descifrar un disco duro protegido con 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 correspondiente 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 ficha **Configuración de la aplicación**.

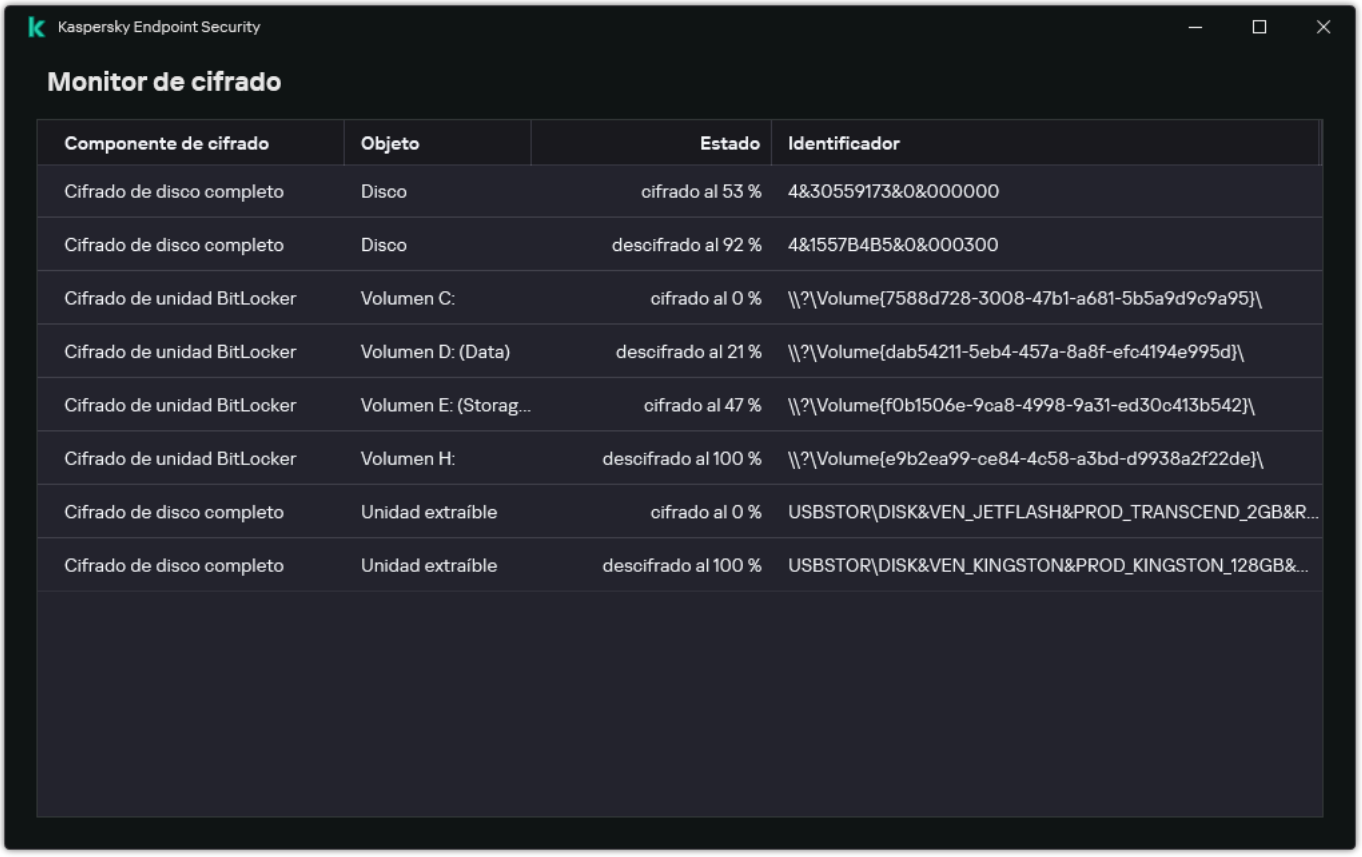
4. Vaya a **Cifrado de datos** → **Cifrado de disco completo**.

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.

Si desea supervisar el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.



Monitor de cifrado

Restaurar el acceso a una unidad protegida con BitLocker

Si un usuario olvida la contraseña para acceder a un disco duro cifrado con BitLocker, debe iniciar el procedimiento de recuperación (procedimiento de solicitud y respuesta).

> Si el sistema operativo del equipo es Windows 8 o una versión anterior y tiene habilitado el modo de compatibilidad con el Estándar federal de procesamiento de información (FIPS), habrá guardado un archivo de clave de recuperación en una unidad extraíble antes de que se aplicara el cifrado. Para volver a acceder a la unidad cifrada, conecte la unidad extraíble y siga las instrucciones en pantalla.

El siguiente es el procedimiento para restaurar el acceso a un disco duro cifrado con BitLocker:

1. El usuario le indica al administrador el id. de la clave de recuperación (vea la imagen de más abajo).
2. En Kaspersky Security Center, el administrador abre las propiedades del equipo y verifica el id. de la clave de recuperación. El id. provisto por el usuario debe ser el mismo que aparezca en las propiedades del equipo.
3. Si los id. de la clave de recuperación coinciden, el administrador le brinda al usuario una clave de recuperación o le envía un archivo de clave de recuperación.

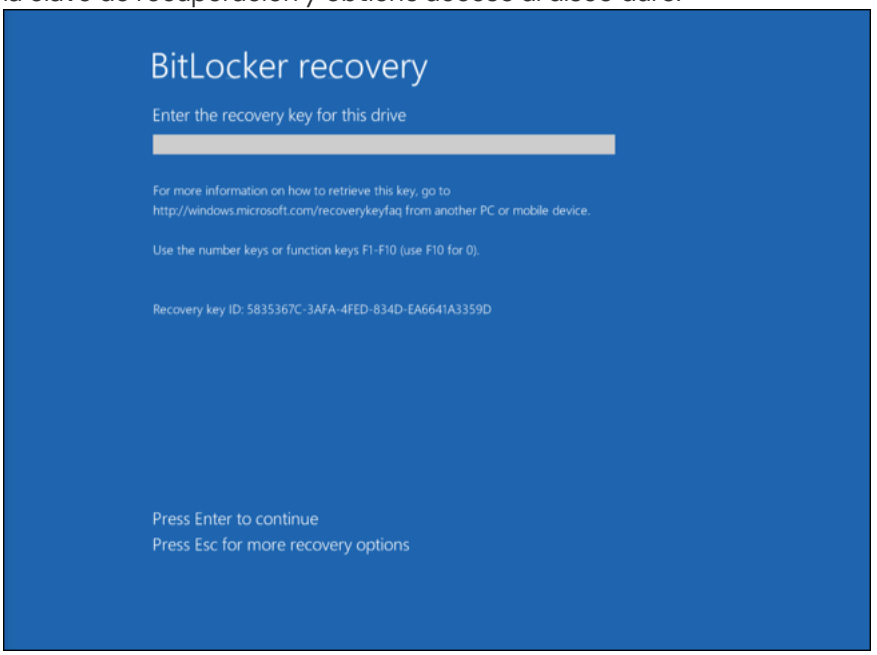
   Los archivos de clave de recuperación se utilizan para equipos con uno de estos sistemas operativos:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   Para los demás sistemas operativos, debe usarse en cambio una clave de recuperación.

   Para prevenir la reutilización de contraseñas con 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.



Restaurar el acceso a un disco duro cifrado con BitLocker

Restaurar el acceso a una unidad del sistema

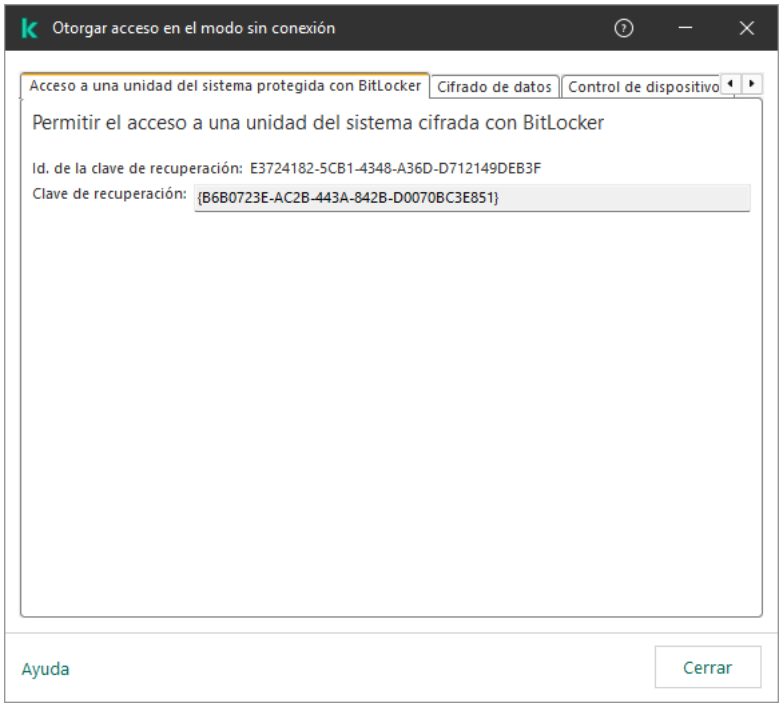
Para iniciar el procedimiento de recuperación, el usuario debe presionar la tecla **Esc** en la etapa de autenticación de prearranque.

Cómo ver la clave de recuperación para una unidad del sistema cifrada con BitLocker a través de 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 del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
4. En el menú contextual, seleccione **Otorgar acceso en el modo sin conexión**.
5. En la ventana que se abre, seleccione la pestaña **Acceso a una unidad del sistema protegida con BitLocker**.
6. Solicite al usuario que ingrese el identificador de la clave de recuperación que se indica en la ventana para ingresar la contraseña de BitLocker y compárelo con el identificador presente en el campo **Id. de la clave de recuperación**.

   Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco de sistema especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

Tras completar estos pasos, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá enviarle al usuario.



Restaurar el acceso a una unidad cifrada con la ventana BitLocker

Cómo ver la clave de recuperación para una unidad del sistema cifrada con BitLocker a través de Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentre la unidad a la que se necesite acceso.
3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.
4. En la ventana que se abre, seleccione la sección **BitLocker**.
5. Verifique el id. de la clave de recuperación. El id. provisto por el usuario debe ser el mismo que aparezca en las propiedades del equipo.

   Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco de sistema especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

6. Haga clic en **Recibir clave**.

Tras completar estos pasos, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá enviarle 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. De esta manera, se actualizarán la clave de recuperación y el archivo de clave de recuperación. Si el usuario no cambia la contraseña, será posible usar la clave de recuperación antigua la siguiente vez que se cargue el sistema operativo.

Los equipos con Windows 7 no permiten cambiar la contraseña o el código PIN. Una vez que se ingresa la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, es imposible establecer una contraseña nueva o un código PIN. Este problema se origina por las peculiaridades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.

Restaurar el acceso a una unidad que no sea la del sistema

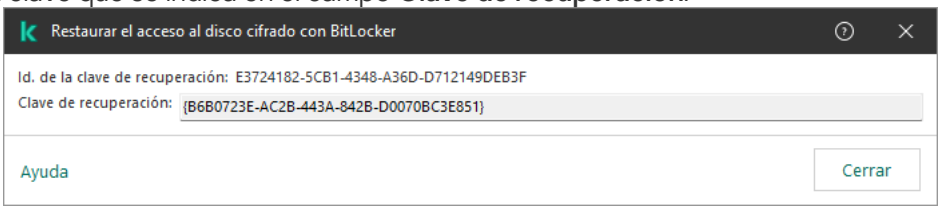
Para iniciar el procedimiento de recuperación, el usuario debe hacer clic en el vínculo **Forgot your password** de la ventana que le permite obtener acceso a la unidad. Una vez que tenga acceso a la unidad cifrada, el usuario podrá modificar la configuración de BitLocker para que, cuando se autentique en Windows, la unidad se desbloquee automáticamente.

Cómo ver la clave de recuperación para una unidad cifrada con BitLocker (que no sea la del sistema) a través de 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** → **Unidades cifradas**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que necesite crear el archivo de clave de acceso. A continuación, en el menú contextual del dispositivo, haga clic **Obtener acceso al dispositivo en Kaspersky Endpoint Security**.
4. Solicite al usuario que ingrese el identificador de la clave de recuperación que se indica en la ventana para ingresar la contraseña de BitLocker y compárelo con el identificador presente en el campo **Id. de la clave de recuperación**.

   Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso a la unidad especificada. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

5. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.



Restaurar el acceso a una unidad cifrada con la ventana BitLocker

Cómo ver la clave de recuperación para una unidad cifrada con BitLocker (que no sea la del sistema) a través de Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Operaciones** → **Protección y cifrado de datos** → **Unidades cifradas**.

2. Active la casilla ubicada junto al nombre del equipo en el que se encuentre la unidad a la que se necesite acceso.

3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.

   Se inicia un asistente para otorgar acceso al dispositivo.

4. Siga las instrucciones del asistente para otorgar acceso al dispositivo:

   a. Seleccione el complemento **Kaspersky Endpoint Security para Windows**

   b. Verifique el id. de la clave de recuperación. El id. provisto por el usuario debe ser el mismo que aparezca en las propiedades del equipo.

   > Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco de sistema especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

   c. Haga clic en **Recibir clave**.

Tras completar estos pasos, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá enviarle al usuario.

Suspensión de 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. Es posible que deba reiniciar varias veces el equipo debido a la instalación de las actualizaciones. Después de cada reinicio, el usuario debe completar la autenticación BitLocker. Para asegurarse de que las actualizaciones se instalen correctamente, puede desactivar temporalmente la autenticación 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 BitLocker, puede usar la tarea *Administración de protección de BitLocker*. Puede usar esta tarea para especificar el número de reinicios del equipo que no requieren autenticación BitLocker. De esta forma, una vez instaladas las actualizaciones y la tarea *Administración de protección de BitLocker* finaliza, la autenticación BitLocker se habilita automáticamente. Puede habilitar la autenticación 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Administración de protección de BitLocker**.

Paso 2. Administración de protección de BitLocker

Configure la autenticación BitLocker. Para pausar la protección de BitLocker, seleccione **Permitir temporalmente omitir la autenticación de BitLocker** e ingrese el número de reinicios sin autenticación BitLocker (de 1 a 15 veces). Si es necesario, ingrese 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 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 ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Nombre de la tarea

Ingrese el nombre de la tarea, por ejemplo *Actualización a Windows 10*.

Paso 5. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo pausar la protección de BitLocker a través de 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 **Agregar**.

Se inicia el Asistente de tareas. 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**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Administración de protección de BitLocker**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Actualizar a Windows 10*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

Paso 2. Administración de protección de BitLocker

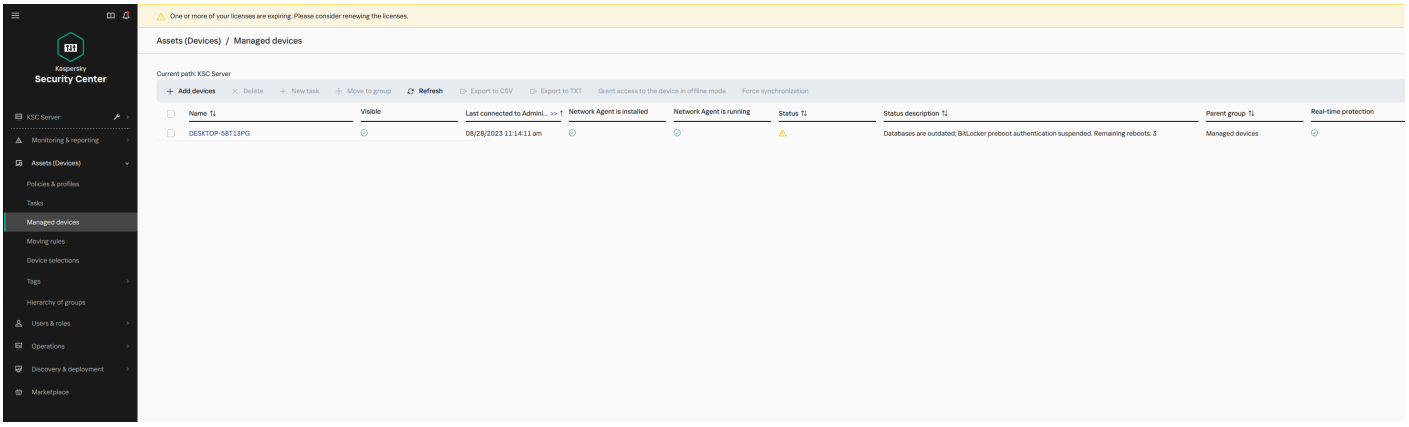
Configure la autenticación BitLocker. Para pausar la protección de BitLocker, seleccione **Permitir temporalmente omitir la autenticación de BitLocker** e ingrese el número de reinicios sin autenticación BitLocker (de 1 a 15 veces). Si es necesario, ingrese una fecha y hora de caducidad para la tarea. A la hora especificada, la tarea se desactiva automáticamente y el usuario debe completar la autenticación BitLocker cuando se reinicia el equipo.

Paso 3. Completar creación de la tarea

Salga del 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 autenticación BitLocker, Kaspersky Endpoint Security genera un evento correspondiente y registra el número de reinicios restantes. A continuación, 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 BitLocker se activa automáticamente. Para obtener acceso a los datos, el usuario debe completar la autenticación BitLocker.

En equipos que ejecutan Windows 7, BitLocker no puede contar los reinicios de equipos. El conteo de reinicios en equipos con Windows 7 es procesado por Kaspersky Endpoint Security. Por lo tanto, para activar automáticamente la autenticación BitLocker después de cada reinicio, debe iniciarse Kaspersky Endpoint Security.

Para activar la autenticación BitLocker antes de tiempo, abra las propiedades de la tarea *Administración de protección de BitLocker* y seleccione **Solicitar la autenticación cada vez en el arranque previo**.

Cifrado de archivos en discos de equipos locales.

El cifrado de archivos no es compatible con equipos basados en Arm.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

La característica de cifrado de archivos está sujeta a las siguientes consideraciones especiales:

- Kaspersky Endpoint Security cifrará o descifrará archivos en las carpetas predefinidas únicamente para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifrará ni descifrará ningún archivo que se encuentre en una carpeta redirigida o en las carpetas predefinidas de un perfil de usuario móvil, un perfil de usuario obligatorio o un perfil de usuario temporal.

- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo y las aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas están en la lista de exclusiones de cifrado:

  - %WINDIR%

  - %PROGRAMFILES% y %PROGRAMFILES(X86)%

  - Archivos de registro de Windows.

  No es posible ver ni modificar la lista de exclusiones de cifrado. Aunque los archivos y carpetas de esta lista pueden agregarse a la lista de cifrado, la característica de cifrado de archivos nunca cifrará esos objetos.

Cifrado de archivos en discos locales del equipo.

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 su nombre. Kaspersky Endpoint Security también bloquea la copia de archivos cifrados en carpetas de OneDrive si esos archivos no se agregan a la regla de descifrado.

Para cifrar archivos en discos locales:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 **Según las reglas**.
5. En la ficha **Cifrado**, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:

   a. Seleccione el elemento **Carpetas predefinidas** para agregar archivos desde carpetas de perfiles de usuarios locales sugeridos por expertos de Kaspersky a una regla de cifrado.

   - **Documentos**. Archivos que se encuentren en la carpeta *Documentos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.
   - **Favoritos**. Archivos que se encuentren en la carpeta *Favoritos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.
   - **Escritorio**. Archivos que se encuentren en la carpeta *Escritorio* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.
   - **Archivos temporales**. Archivos temporales vinculados al funcionamiento de las aplicaciones instaladas en el equipo. Aquí se incluyen, por ejemplo, las copias de seguridad temporales que se crean al trabajar con documentos en las aplicaciones de Microsoft Office.

     No se recomienda cifrar archivos temporales, ya que esto puede ocasionar pérdidas de datos. Por ejemplo, Microsoft Word crea archivos temporales al procesar un documento. Si los archivos temporales están cifrados, pero el archivo original no lo está, es posible que el usuario reciba el error *Acceso denegado* al intentar guardar el documento. Además, aunque Microsoft Word pueda guardar el archivo, es posible que no se pueda abrir el documento la próxima vez y se pierdan los datos.

   - **Archivos de Outlook**. Archivos vinculados al funcionamiento del cliente de correo electrónico Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de las libretas de direcciones sin conexión (OAB) y archivos de las libretas de direcciones personales (PAB).

   b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de carpeta introducida manualmente a una regla de cifrado.

Cuando agregue una ruta de carpeta, siga estas reglas:

- Utilice una variable de entorno (por ejemplo, `%FOLDER%\UserFolder\`). Puede usar una sola variable de entorno por ruta, y únicamente al comienzo de la ruta.
- No utilice rutas relativas.
- No utilice los caracteres `*` y `?`.
- No utilice rutas UNC.
- Utilice los caracteres `;` o `,` como separadores.

c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo individuales a una regla de cifrado. Kaspersky Endpoint Security cifrará los archivos con las extensiones especificadas en todos los discos locales del equipo.

d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones (por ejemplo, *Documentos de Microsoft Office*) a una regla de cifrado. Kaspersky Endpoint Security cifrará archivos que tengan las extensiones indicadas en los grupos de extensiones en todos los discos locales del equipo.

6. Guarde los cambios.

Tan pronto como se aplique la directiva, Kaspersky Endpoint Security cifrará los archivos incluidos en la regla de cifrado y no incluidos en la regla de descifrado.

La característica de cifrado de archivos está sujeta a las siguientes consideraciones especiales:

- Cuando un archivo aparece al mismo tiempo en una regla de cifrado y en una regla de descifrado, Kaspersky Endpoint Security hace lo siguiente:
  - si el archivo no está cifrado, lo deja sin cifrar;
  - si el archivo está cifrado, lo descifra.
- Kaspersky Endpoint Security se mantiene siempre atento a los archivos nuevos que puedan reunir los criterios de las reglas de cifrado y que, por ende, deban cifrarse. Un archivo existente que no esté cifrado puede pasar a cumplir con los criterios de una regla si, por ejemplo, sus propiedades (ruta o extensión) se modifican. Si Kaspersky Endpoint Security detecta un archivo de este tipo, lo cifrará.
- Cuando el usuario crea un archivo nuevo cuyas propiedades cumplen los criterios de la regla de cifrado, Kaspersky Endpoint Security cifra el archivo tan pronto como se abre.
- Kaspersky Endpoint Security pospone el cifrado de los archivos abiertos hasta que se los cierre.
- Si mueve un archivo cifrado a otra carpeta en el disco local, el archivo permanece cifrado sin importar si esta carpeta figura o no en la regla de cifrado.
- Si descifra un archivo y lo copia a una carpeta local que no esté incluida en una regla de descifrado, la aplicación podría cifrar la copia del archivo. Para que la copia del archivo no se cifre, deberá crear una regla de descifrado para la carpeta de destino.

Formación de reglas de acceso a archivos cifrados para aplicaciones

De forma predeterminada, todas las aplicaciones funcionan con archivos cifrados en un estado descifrado. Si usa ciertas 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 a un sitio web (por ejemplo, un 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 **Otorgar acceso a archivos cifrados solo en texto cifrado**. No es necesario crear una regla para otros navegadores (como Google Chrome).

Para formar 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 correspondiente 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 **Según las reglas**.

   Las reglas de acceso solo se aplican en el modo **Según las reglas**. Si aplica las reglas de acceso estando en el modo **Según las reglas** y luego pasa al modo **Dejar sin modificar**, Kaspersky Endpoint Security no tendrá en cuenta ninguna de las reglas de acceso. Todas las aplicaciones tendrán acceso a todos los archivos cifrados.

5. En la parte derecha de la ventana, seleccione la ficha **Reglas para aplicaciones**.
6. Si quiere seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Agregar** 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 que aparecen en la tabla. Para hacerlo, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período de adición**, y todas las casillas del bloque **Grupo**.

   b. Haga clic en **Actualizar**.

   c. En la tabla, figurarán las aplicaciones que coincidan con los filtros seleccionados.

   d. En la columna **Aplicación**, seleccione las casillas junto a las aplicaciones para las que desea formar las 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 archivos cifrados.

f. En la lista desplegable **Acciones para aplicaciones seleccionadas previamente**, seleccione la acción que realizará Kaspersky Endpoint Security sobre las reglas de acceso a archivos cifrados que se formaron previamente para dichas aplicaciones.

Los detalles de una regla de acceso a archivos cifrados para aplicaciones aparecen en la tabla en la ficha **Reglas para aplicaciones**.

7. Si quiere seleccionar aplicaciones manualmente, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

   a. En el campo de entrada de datos, escriba el nombre o una lista de nombres de archivos de aplicación ejecutables con sus extensiones.

      También puede agregar los nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center si hace clic en el botón **Agregar de la lista de Kaspersky Security Center**.

   b. Si es necesario, en el campo **Descripción**, ingrese 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 archivos cifrados.

   Los detalles de una regla de acceso a archivos cifrados para aplicaciones aparecen en la tabla en la ficha **Reglas para aplicaciones**.

8. Guarde los cambios.

Cifrado de archivos que son 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.

> No se cifrarán los archivos que fueron creados o modificados por las aplicaciones especificadas antes de aplicarse la regla del cifrado.

Para configurar el cifrado de archivos que son creados o modificados por aplicaciones específicas:

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

2. Seleccione la directiva correspondiente 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 **Según las reglas**.

> Las reglas de cifrado se aplican solo en el modo **Según las reglas**. Si aplica las reglas de cifrado estando en el modo **Según las reglas** y luego pasa al modo **Dejar sin modificar**, Kaspersky Endpoint Security no tendrá en cuenta ninguna de las reglas de cifrado. Los archivos que se cifraron anteriormente permanecerán cifrados.

5. En la parte derecha de la ventana, seleccione la ficha **Reglas para aplicaciones**.

6. Si quiere seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Agregar** 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 que aparecen en la tabla. Para hacerlo, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período de adición**, y todas las casillas del bloque **Grupo**.

   b. Haga clic en **Actualizar**.

      En la tabla, figurarán las aplicaciones que coincidan con los filtros seleccionados.

   c. En la columna **Aplicación**, active las casillas adyacentes a las aplicaciones con las que se crearán los archivos que deban cifrarse.

   d. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

   e. En la lista desplegable **Acciones para aplicaciones seleccionadas previamente**, seleccione la acción que realizará Kaspersky Endpoint Security sobre las reglas de cifrado de archivos cifrados que se formaron previamente para dichas aplicaciones.

   La información sobre la regla de cifrado para archivos creados o modificados por las aplicaciones seleccionadas se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

7. Si quiere seleccionar aplicaciones manualmente, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

   a. En el campo de entrada de datos, escriba el nombre o una lista de nombres de archivos de aplicación ejecutables con sus extensiones.

      También puede agregar los nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center si hace clic en el botón **Agregar de la lista de Kaspersky Security Center**.

   b. Si es necesario, en el campo **Descripción**, ingrese 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 las 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 correspondiente 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 **Según las reglas**.
5. En la ficha **Descifrado**, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:
   a. Seleccione el elemento **Carpetas predefinidas** para agregar archivos desde carpetas de perfiles de usuarios locales sugeridos por expertos de Kaspersky a una regla de descifrado.
   b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de carpeta introducida manualmente a una regla de descifrado.
   c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo individuales a una regla de descifrado. Kaspersky Endpoint Security no cifrará los archivos con las extensiones especificadas en todos los discos locales del equipo.
   d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones (por ejemplo, *Documentos de Microsoft Office*) a una regla de descifrado. Kaspersky Endpoint Security no cifrará los archivos almacenados en los discos locales del equipo que tengan alguna de las extensiones indicadas en los grupos de extensiones.
6. Guarde los cambios.

Si se agregó el mismo archivo a la lista de cifrado y a la regla de descifrado, Kaspersky Endpoint Security no cifrará este archivo si no está cifrado, y lo descifrará si está cifrado.

Descifrado de archivos en unidades de disco locales del equipo

Para descifrar archivos en discos locales:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 ficha **Cifrado**.

5. Elimine de la lista de cifrado los archivos y las carpetas que desea descifrar. Para ello, seleccione los archivos y el elemento **Eliminar regla y descifrar archivos** en el menú contextual del botón **Eliminar**.

   Los archivos y las carpetas que se eliminan de la lista de cifrado se agregan automáticamente a la lista de descifrado.

6. Formar una lista de descifrado de archivos.

7. Guarde los cambios.

No bien se implementa la directiva, Kaspersky Endpoint Security descifra los archivos cifrados que se agregaron a la lista de descifrado.

Kaspersky Endpoint Security descifra los archivos cifrados si sus parámetros (ruta de la carpeta, nombre de archivo, extensión de archivo) cambian para coincidir con los parámetros de objetos que se agregaron a la lista de descifrado.

Kaspersky Endpoint Security pospone el descifrado de los archivos abiertos hasta que se los cierre.

Creación de paquetes cifrados

Si necesita enviarle un archivo a alguien que está fuera de la red corporativa, puede hacerlo en forma segura utilizando un paquete cifrado. Los paquetes cifrados son útiles para compartir archivos de gran tamaño utilizando unidades extraíbles, ya que las aplicaciones de correo electrónico suelen restringir el tamaño de los adjuntos.

Cuando un usuario intente crear un paquete cifrado, Kaspersky Endpoint Security le solicitará una contraseña. Para contribuir con la protección de los datos, es posible definir (y hacer que la aplicación controle) los requisitos con los que deberán cumplir estas contraseñas para que se las considere seguras. Ello evitará que los usuarios utilicen claves simples y cortas, como `1234`.

Cómo habilitar el control de requisitos para las contraseñas definidas al crear archivos 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 correspondiente 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 contraseñas**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, seleccione la pestaña **Paquetes cifrados**.

6. Configure los requisitos de complejidad con los que deberán cumplir las contraseñas de los paquetes cifrados.

Cómo habilitar el control de requisitos para las contraseñas definidas al crear archivos cifrados 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 ficha **Configuración de la aplicación**.

4. Vaya a **Cifrado de datos** → **Cifrado de archivos**.

5. En el bloque **Configuración de contraseña para paquetes cifrados**, defina los requisitos con los que deberán cumplir las contraseñas de los paquetes cifrados que cree en el futuro.

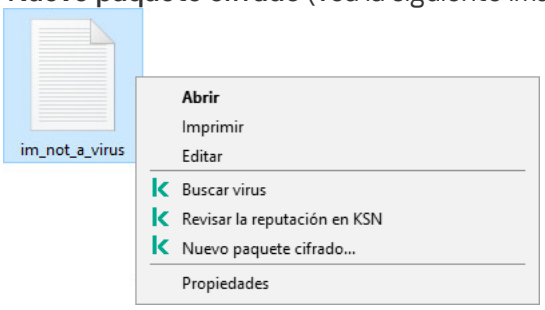
Para crear un paquete cifrado, debe utilizar un equipo con Kaspersky Endpoint Security que tenga la característica Cifrado de archivos habilitada.

> Al agregar un archivo al paquete cifrado cuyo contenido está almacenado en la nube de OneDrive, Kaspersky Endpoint Security descarga el contenido del archivo y luego lo cifra.

Para crear un paquete cifrado:

1. En cualquier administrador de archivos, seleccione los archivos o las carpetas que deban formar parte del paquete cifrado. Haga clic con el botón derecho del mouse para abrir su menú contextual.

2. En el menú contextual, seleccione **Nuevo paquete cifrado** (vea la siguiente imagen).



Creación de un paquete cifrado

3. En la ventana que se abre, defina y confirme la contraseña.

   La contraseña deberá ajustarse a los requisitos de seguridad que se hayan definido en la directiva.

4. Haga clic en **Crear**.

   Se inicia el proceso de creación del paquete cifrado. Kaspersky Endpoint Security no realiza la compresión de archivos cuando crea un paquete cifrado. Cuando el proceso finalice, se creará un paquete cifrado autoextraíble en la carpeta de destino. El paquete será un archivo ejecutable (de extensión exe) con el icono y estará protegido con la contraseña que haya definido.

Para acceder a los archivos de un paquete cifrado, haga doble clic en el paquete y, luego de que se inicie el asistente de desempaquetamiento, escriba la contraseña. Si ha olvidado la contraseña, no podrá recuperarla; quedará, en ese caso, sin acceso a los archivos del paquete. Si lo desea, podrá volver a crear el paquete cifrado.

Procedimiento para recuperar el acceso a archivos cifrados

Cuando un grupo de archivos se cifra, Kaspersky Endpoint Security recibe una clave de cifrado que permite acceder a ellos en forma directa. Si utiliza esta clave de cifrado, un usuario que esté trabajando con cualquier cuenta de usuario de Windows que esté activa durante el cifrado de archivos podrá acceder directamente a los archivos cifrados. Los usuarios que trabajen con las cuentas de Windows que estaban activas durante el cifrado de archivos deben conectarse a Kaspersky Security Center para acceder a los archivos cifrados.

Los archivos cifrados pueden ser inaccesibles en las siguientes circunstancias:

- El equipo del usuario almacena claves de cifrado, pero no hay 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 LAN.

  Si el acceso a Kaspersky Security Center no existe, debe:

  - solicitar una clave de acceso para el acceso a archivos cifrados en los discos duros del equipo;
  - para acceder a los archivos cifrados almacenados en unidades extraíbles, solicite otra clave de acceso para los archivos cifrados de cada disco extraíble.

- Los componentes del cifrado se eliminan desde el equipo del usuario. En este caso, el usuario puede abrir los archivos cifrados en discos locales y extraíbles, pero los contenidos de esos archivos aparecerán cifrados.

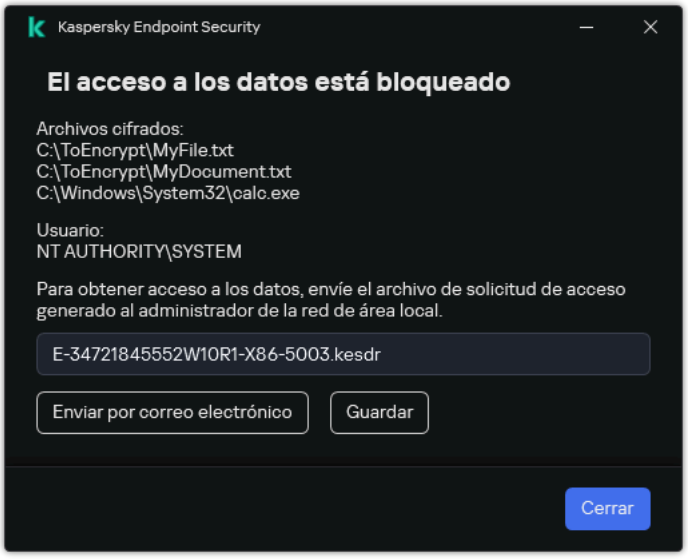
  El usuario puede trabajar con archivos cifrados en las siguientes circunstancias:

  - Los archivos se encuentran dentro de paquetes cifrados creados en un equipo con Kaspersky Endpoint Security instalado.
  - Los archivos están almacenados en unidades extraíbles en las cuales se ha autorizado el modo portátil.

El usuario que necesite acceder a los archivos cifrados deberá iniciar un procedimiento de recuperación (un procedimiento de solicitud y respuesta).

El procedimiento para recuperar acceso a los archivos cifrados consiste en lo siguiente:

1. El usuario le envía al administrador un archivo de solicitud de acceso (vea la imagen de abajo).
2. El administrador agrega el archivo de solicitud de acceso en Kaspersky Security Center; a continuación, crea un archivo de clave de acceso y se lo envía al usuario.
3. El usuario agrega el archivo de clave de acceso en Kaspersky Endpoint Security y obtiene acceso a los archivos.



Procedimiento para recuperar el acceso a archivos cifrados

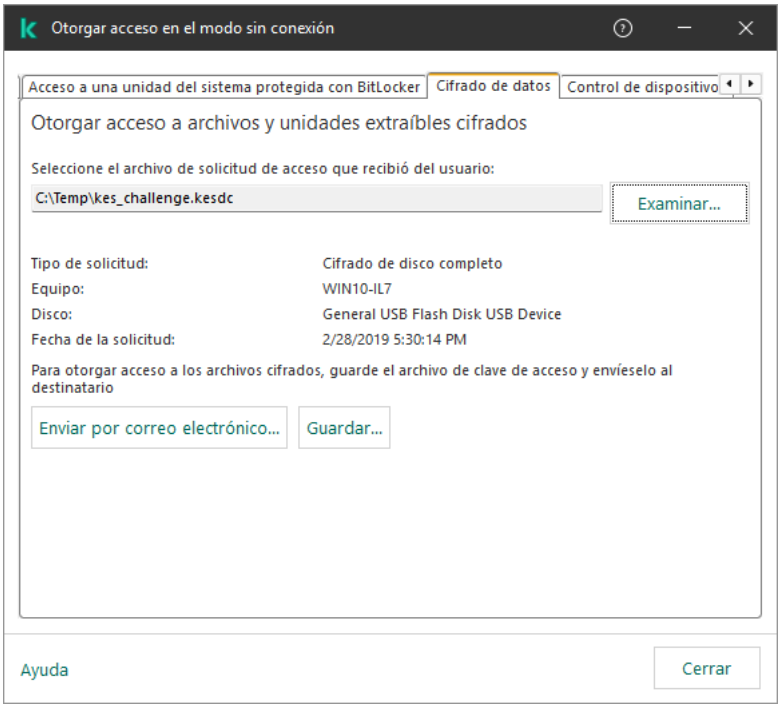
Para iniciar el procedimiento de recuperación, el usuario debe tratar de acceder a un archivo. Cuando lo haga, Kaspersky Endpoint Security creará un archivo de solicitud de acceso, que tendrá la extensión KESDC. El usuario deberá enviarle ese archivo al administrador por correo electrónico o por cualquier otro medio.

Kaspersky Endpoint Security genera archivos de solicitud de acceso que permiten acceder a todos los archivos cifrados almacenados en la unidad (disco local o unidad extraíble) del equipo.

Cómo obtener un archivo de clave de acceso para archivos cifrados 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. En la pestaña **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
4. En el menú contextual, seleccione **Otorgar acceso en el modo sin conexión**.
5. En la ventana que se abre, seleccione la pestaña **Cifrado de datos**.
6. En la ficha **Cifrado de datos**, haga clic en el botón **Examinar**.
7. En la ventana para seleccionar el archivo de solicitud de acceso, especifique la ruta al archivo que le haya enviado el usuario.

   Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.



Otorgar acceso en el modo sin conexión

Cómo obtener un archivo de clave de acceso para archivos cifrados mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.

2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los archivos a los que se necesite acceso.

3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.

4. Seleccione **Cifrado de datos**.

5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión KESDC).

   Web Console le mostrará información sobre la solicitud. Encontrará, entre otros datos, el nombre del equipo que contiene los archivos a los que el usuario necesita acceder.

6. Haga clic en el botón **Guardar clave** y seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión KESDR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

Una vez que lo reciba, el usuario deberá hacer doble clic en el archivo de clave de acceso para ejecutarlo. Kaspersky Endpoint Security le permitirá entonces acceder a todos los archivos cifrados de la unidad. Si el usuario necesita acceso a los archivos cifrados de una unidad diferente, deberá obtener un nuevo archivo de clave de acceso, exclusivo para esa unidad.

Restauración del acceso a datos cifrados después de una falla del sistema operativo

Ante un problema con el sistema operativo, únicamente podrá recuperar el acceso a la información que se haya cifrado con la tecnología de cifrado de archivos (FLE). La información para la que se haya usado el cifrado de disco completo (FDE) no podrá restaurarse.

Para recuperar el acceso a sus datos cifrados después de una falla del sistema operativo:

1. Reinstale 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 controlaba el equipo al momento de cifrarse los datos.

Los datos cifrados volverán a estar disponibles bajo las mismas condiciones de acceso que hayan estado vigentes antes del problema con el sistema operativo.

Modificación de plantillas de mensajes de acceso a archivos cifrados

Para modificar plantillas de 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 correspondiente 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 quiere modificar la plantilla del mensaje del usuario, seleccione la ficha **Mensaje del usuario**. Cuando un usuario intenta acceder a un archivo cifrado sin que haya en su equipo una clave que le permita hacerlo (ver la figura a continuación), se abrirá la siguiente ventana. Hacer clic en el botón **Enviar por correo electrónico** crea automáticamente un mensaje de usuario. Este mensaje se envía al administrador de la red de área local corporativa junto con el archivo para solicitar acceso a archivos cifrados.

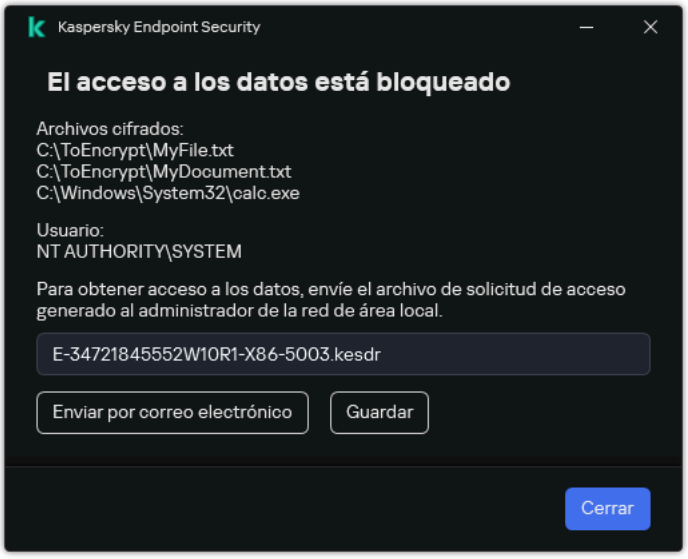
   - Si quiere modificar la plantilla del mensaje del administrador, seleccione la ficha **Mensaje del administrador**. El usuario recibe este mensaje después de que se otorga acceso a los archivos cifrados.

6. Modifique las plantillas de mensaje.

   Para agregar una variable al texto de la plantilla, coloque el cursor en la posición deseada, haga clic en **Variable** y seleccione la variable requerida de la lista de opciones disponibles.

   También puede restaurar el texto de la plantilla predeterminada utilizando el botón **Predeterminado**.

7. Guarde los cambios.



Procedimiento para recuperar el acceso a archivos cifrados

Cifrado de unidades extraíbles

El cifrado de unidades extraíbles no es compatible con equipos basados en Arm.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha 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 se conecta una unidad extraíble con un sistema de archivos no compatible 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 la información almacenada en una unidad extraíble, puede usar los siguientes tipos de cifrado:

- Full Disk Encryption (FDE).

  Cifrado de la unidad extraíble completa, incluido su sistema de archivos.

  Tenga en cuenta que no se podrá acceder a la información cifrada fuera de la red corporativa. Aun dentro de la red corporativa, tampoco será posible acceder a esta información si el equipo no está conectado a Kaspersky Security Center (es decir, si se utiliza un equipo invitado).

- File Level Encryption (FLE).

  Cifrado únicamente de los archivos almacenados en la unidad extraíble. El sistema de archivos no se modifica.

  Si cifra los archivos de una unidad extraíble, podrá utilizar un modo especial —llamado *modo portátil*— para acceder a la información fuera de la red corporativa.

Kaspersky Endpoint Security crea una clave maestra como parte del proceso de cifrado. La clave maestra se guarda en los siguientes repositorios:

- Kaspersky Security Center
- El equipo del usuario

  La clave maestra se cifra con la clave secreta del usuario.

- Unidad extraíble

  La clave maestra se cifra con la clave pública de Kaspersky Security Center.

Una vez que haya cifrado una unidad extraíble, mientras se encuentre dentro de la red corporativa, podrá acceder a sus datos como si estuviera utilizando una unidad convencional sin cifrado.

Acceso a datos cifrados

Cuando se conecta una unidad extraíble con información cifrada, Kaspersky Endpoint Security hace lo siguiente:

1. Busca una clave maestra en el repositorio local del equipo del usuario.

   Si encuentra la clave maestra pertinente, el usuario puede acceder a la información de la unidad extraíble.

   Si no encuentra la clave maestra, Kaspersky Endpoint Security hace lo siguiente:

   a. Envía una solicitud a Kaspersky Security Center.

      Tras recibir la solicitud, Kaspersky Security Center envía una respuesta con la clave maestra.

   b. Kaspersky Endpoint Security guarda la clave maestra en el repositorio local del equipo para poder operar con la unidad extraíble cifrada.

2. Descifra la información.

Consideraciones especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles está sujeto a las siguientes consideraciones especiales:

- La directiva con los ajustes preestablecidos para el cifrado de unidades extraíbles se crea para un grupo específico de equipos administrados. Por lo tanto, el resultado de la aplicación de la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al cual está conectada la unidad extraíble.

- Kaspersky Endpoint Security no cifra ni descifra los archivos de solo lectura que puedan encontrarse en las unidades extraíbles.

- Los siguientes tipos de dispositivo se admiten como unidad extraíble:

  - Medios de datos conectados por medio de un bus USB

  - Discos duros conectados por medio de buses USB y FireWire

  - Unidades SSD conectadas por medio de buses USB y FireWire

Inicio del cifrado de unidades extraíbles

Para descifrar una unidad extraíble, puede utilizarse una directiva. Las directivas en las que se definen los ajustes de cifrado de unidades extraíbles se crean para grupos de administración específicos. Por lo tanto, el resultado del descifrado de datos en unidades extraíbles depende del equipo al cual esté conectada la unidad extraíble.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si se conecta una unidad extraíble con un sistema de archivos no compatible 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 correspondiente 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 la unidad extraíble completa** (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. Los sistemas de archivos no se cifrarán, con lo cual los nombres de los archivos y las estructuras de carpetas quedarán sin cambios.
   - **Solo cifrar archivos nuevos** (FLE). De los archivos de las unidades extraíbles, Kaspersky Endpoint Security cifrará únicamente aquellos que se hayan agregado 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 **Modo portátil**.

   El *modo portátil* es un modo de funcionamiento de la característica de cifrado de archivos (FLE). Brinda la capacidad de acceder a la información de una unidad extraíble cifrada cuando se está fuera de la red corporativa. También permite trabajar con información cifrada en equipos que no tienen Kaspersky Endpoint Security instalado.

6. Para cifrar unidades extraíbles nuevas, recomendamos activar la casilla **Solo cifrar el espacio de disco usado**. Si se cancela la selección de la casilla, 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, seleccione la casilla **Permitir cifrado de unidades extraíbles en el modo sin conexión**.

   El *modo de cifrado sin conexión* se utiliza para cifrar unidades extraíbles, mediante la tecnología de 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 **Permitir cifrado de unidades extraíbles en el modo sin conexión** está desactivada y no hay conexión con Kaspersky Security Center, las unidades extraíbles no se podrán cifrar.

9. Guarde los cambios.

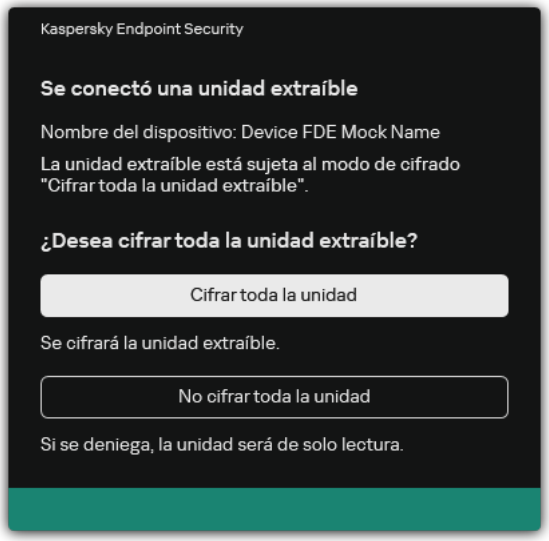
Cuando se conecte una unidad extraíble (o cuando ya haya una unidad extraíble conectada) después de que se aplique la directiva, Kaspersky Endpoint Security le solicitará al usuario que confirme la operación de cifrado (vea la imagen de más abajo).

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 solicitud se repetirá la siguiente vez que se aplique una directiva de Kaspersky Security Center o cuando se vuelva a conectar la misma unidad extraíble.

Si el usuario intenta expulsar una unidad extraíble en forma segura mientras su información se está cifrando, Kaspersky Endpoint Security interrumpirá el proceso de cifrado antes de que se complete y permitirá extraer la unidad. El proceso de cifrado se reanudará cuando el usuario conecte la unidad nuevamente al equipo.

Si tiene problemas para cifrar una unidad extraíble, consulte el informe de **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Puede ocurrir que otra aplicación impida el acceso a los archivos. En tal caso, desconecte la unidad extraíble y vuelva a conectarla.



Solicitud de cifrado para una unidad extraíble

Agregar una regla de cifrado para unidades extraíbles

Para añadir una regla de cifrado para unidades extraíbles:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 sobre el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:
   - Si quiere agregar reglas de cifrado para unidades extraíbles que están en la lista de dispositivos de confianza del componente Control de dispositivos, seleccione **De la lista de dispositivos de confianza de esta directiva**.
   - Si quiere agregar reglas de cifrado para 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 realizará Kaspersky Endpoint Security en los archivos almacenados en las unidades extraíbles seleccionadas.

6. Seleccione la casilla **Modo portátil** si desea que Kaspersky Endpoint Security prepare las unidades extraíbles antes del cifrado, lo que permite que sea posible utilizar los archivos cifrados almacenados en esas unidades en modo portátil.

   El modo portátil le permite usar archivos cifrados almacenados en unidades extraíbles conectadas a equipos sin funcionalidad de cifrado.

7. Seleccione la casilla **Solo cifrar el espacio de disco usado** si quiere que Kaspersky Endpoint Security cifre solo los sectores del disco que estén ocupados por archivos.

   Si está aplicando el cifrado a un disco que ya está en uso, le recomendamos que cifre todo el disco. De esta manera, se asegurará de que toda la información —incluida la información eliminada, que podría contener datos recuperables— esté protegida. Se recomienda usar la función **Solo cifrar el espacio de disco usado** en el caso de discos nuevos sin uso previo.

   Si un dispositivo ya se cifró con la función **Solo cifrar el espacio de disco usado**, después de aplicar una directiva en el modo **Cifrar la unidad extraíble completa**, no se cifrarán los sectores no ocupados por archivos.

8. En la lista desplegable **Acciones para dispositivos seleccionados previamente**, seleccione la acción que realizará Kaspersky Endpoint Security de acuerdo con las reglas de cifrado previamente definidas para las unidades extraíbles:

   - Si quiere que la regla de cifrado creada anteriormente para el disco extraíble permanezca sin cambios, seleccione **Omitir**.
   - Si quiere que la regla de cifrado creada anteriormente para la unidad extraíble sea reemplazada por la regla nueva, seleccione **Actualizar**.

9. Guarde los cambios.

Las nuevas reglas de cifrado se aplicarán a todas las unidades extraíbles conectadas a los equipos de la organización.

Exportar e importar una lista de reglas de cifrado para unidades extraíbles

Puede exportar la lista de reglas de cifrado de unidades extraíbles a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar 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 otro servidor.

Cómo exportar e importar una lista de reglas de cifrado de unidades extraíbles a 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 ficha **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 vínculo **<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 la regla de acceso que desea exportar.

   b. Haga clic en **Exportar**.

   c. Confirme que desea exportar solo las reglas seleccionadas, o bien exporte 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 vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del 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 correspondiente 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 la regla de acceso que desea 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 vínculo **Exportar**.

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.

5. Para importar una lista de reglas de cifrado para unidades extraíbles:

   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

b. Abra el archivo.

Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

6. Guarde los cambios.

Modo portátil para acceder a unidades extraíbles con archivos cifrados

El *modo portátil* es un modo de funcionamiento de la característica de cifrado de archivos (FLE). Brinda la capacidad de acceder a la información de una unidad extraíble cifrada cuando se está fuera de la red corporativa. También permite trabajar con información cifrada en equipos que no tienen Kaspersky Endpoint Security instalado.

El modo portátil es útil en los siguientes casos:

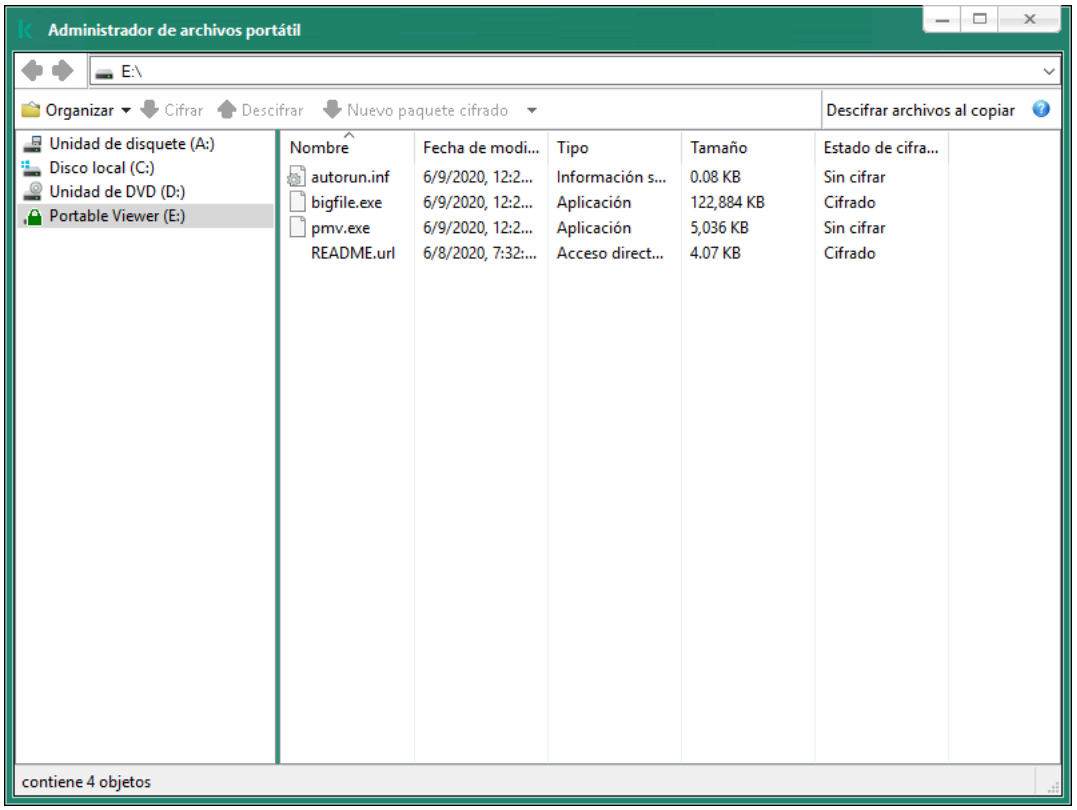
- cuando no hay conexión entre el equipo y el Servidor de administración de Kaspersky Security Center,
- cuando la infraestructura se ha modificado debido a un cambio de Servidor de administración de Kaspersky Security Center,
- cuando Kaspersky Endpoint Security no está instalado en el equipo.

Administrador de archivos portátiles

Para que una unidad extraíble pueda utilizarse en modo portátil, Kaspersky Endpoint Security instala en ella un módulo de cifrado especial, llamado *Administrador de archivos portátil*. A través de su interfaz, el Administrador de archivos portátil permite operar con información cifrada cuando Kaspersky Endpoint Security no está instalado en un equipo (vea la imagen de más abajo). Cuando Kaspersky Endpoint Security está instalado en un equipo, la información de una unidad extraíble cifrada puede manipularse con cualquier administrador de archivos (por ejemplo, el Explorador de Windows).

El Administrador de archivos portátil almacena una clave que se utiliza para cifrar los archivos de la unidad extraíble. Esta clave, a su vez, está cifrada con una contraseña que define el usuario. El usuario establece la contraseña antes de que se cifren los archivos de la unidad.

Cuando conecte una unidad extraíble a un equipo que no tenga Kaspersky Endpoint Security instalado, el Administrador de archivos portátil se ejecutará automáticamente. Si la autoejecución de aplicaciones está deshabilitada en el equipo, deberá abrir el Administrador de archivos portátil en forma manual. Para hacer esto, ejecute el archivo pmv.exe, que encontrará en la unidad extraíble.



Administrador de archivos portátiles

Habilitar el modo portátil para operar con archivos cifrados

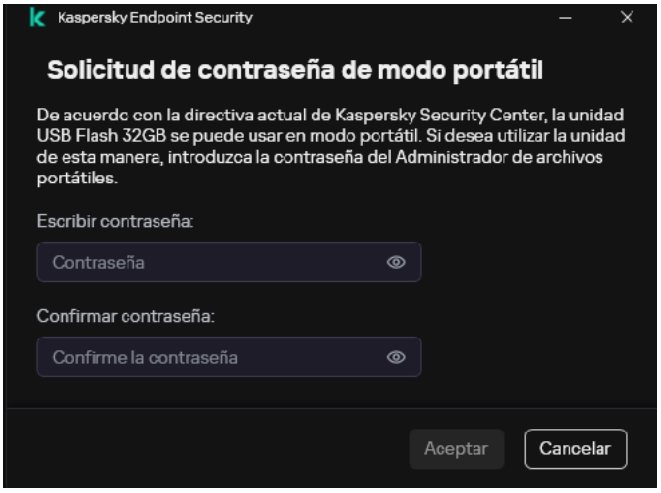
Cómo habilitar, mediante la Consola de administración (MMC), el uso del modo portátil para operar con los archivos cifrados de una unidad extraíble

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 **Solo cifrar archivos nuevos**.

   El modo portátil solo es compatible con la tecnología de cifrado de archivos (FLE). No podrá utilizar el modo portátil con la tecnología de cifrado de disco completo (FDE).

5. Seleccione la casilla de verificación **Modo portátil**.
6. De ser necesario, agregue reglas de cifrado para unidades extraíbles específicas.
7. Guarde los cambios.
8. Aplique la directiva y conecte la unidad extraíble al equipo.
9. Confirme la operación de cifrado del disco extraíble.

Se abre una ventana en la que puede crear una contraseña para el Administrador de archivos portátil.



Solicitud de contraseña para el modo portátil

10. Especifique una contraseña que cumpla con los requisitos de seguridad y confírmela.

11. Guarde los cambios.

Cómo habilitar, mediante Web Console, el uso del modo portátil para operar con los archivos cifrados de una unidad extraíble

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 ficha **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 **Solo cifrar archivos nuevos**.

   El modo portátil solo es compatible con la tecnología de cifrado de archivos (FLE). No podrá utilizar el modo portátil con la tecnología de cifrado de disco completo (FDE).

6. Seleccione la casilla de verificación **Modo portátil**.

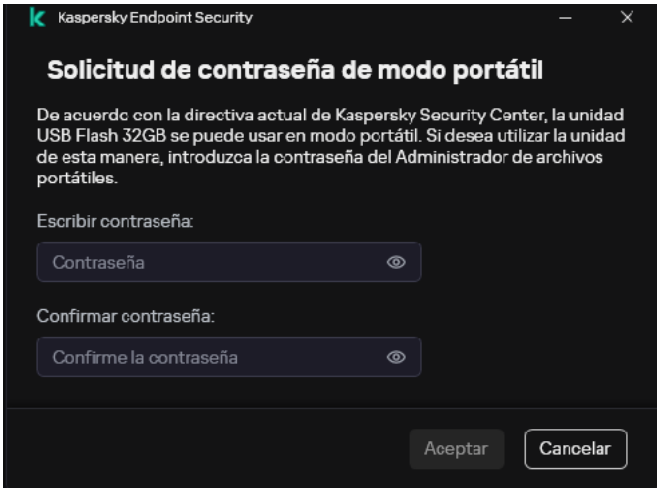
7. De ser necesario, agregue reglas de cifrado para unidades extraíbles específicas.

8. Guarde los cambios.

9. Aplique la directiva y conecte la unidad extraíble al equipo.

10. Confirme la operación de cifrado del disco extraíble.

Se abre una ventana en la que puede crear una contraseña para el Administrador de archivos portátil.



Solicitud de contraseña para el modo portátil

11. Especifique una contraseña que cumpla con los requisitos de seguridad y confírmela.

12. Guarde los cambios.

Kaspersky Endpoint Security cifrará los archivos de la unidad extraíble. El Administrador de archivos portátil se copiará a la unidad extraíble para que pueda trabajar con los archivos cifrados. Si la unidad ya contiene archivos cifrados, Kaspersky Endpoint Security los volverá a cifrar con su propia clave. De este modo, el usuario podrá acceder a todos los archivos de la unidad cuando utilice el modo portátil.

Acceder a los archivos cifrados de una unidad extraíble

Tras cifrar los archivos de una unidad extraíble que permita usar el modo portátil, podrá acceder al contenido de las siguientes maneras:

- Si Kaspersky Endpoint Security no está instalado en el equipo, el Administrador de archivos portátil le pedirá una contraseña. Deberá introducir esta contraseña cada vez que reinicie el equipo o reconecte la unidad extraíble.

- Si el equipo tiene Kaspersky Endpoint Security instalado, pero se encuentra fuera de la red corporativa, la aplicación le pedirá que introduzca una contraseña o que le envíe al administrador una solicitud para acceder a los archivos. Una vez que tenga acceso a los archivos de la unidad extraíble, Kaspersky Endpoint Security guardará la clave secreta en el repositorio de claves del equipo. De esta manera, podrá acceder a los archivos cuando lo necesite sin tener que escribir la contraseña o pedirle autorización al administrador (consulte la figura a continuación).

- Si el equipo tiene Kaspersky Endpoint Security instalado y se encuentra dentro de la red corporativa, podrá acceder al dispositivo sin introducir ninguna contraseña. Kaspersky Endpoint Security obtendrá la clave secreta del Servidor de administración de Kaspersky Security Center al que se encuentre conectado el equipo.

Acceder a los archivos cifrados de una unidad extraíble

Recuperar la contraseña definida para el modo portátil

Si olvida la contraseña que definió para usar el modo portátil, conecte la unidad extraíble a un equipo que tenga Kaspersky Endpoint Security instalado y que se encuentre conectado a la red corporativa. Se le permitirá acceder a los archivos de la unidad puesto que la clave secreta estará almacenada en el repositorio de claves del equipo o en el Servidor de administración. Descifre los archivos y vuelva a cifrarlos con una nueva contraseña.

Propiedades del modo portátil cuando una unidad extraíble se conecta a un equipo vinculado a otra red

Si su equipo tiene Kaspersky Endpoint Security instalado, pero se encuentra fuera de la red corporativa, dispone de las siguientes alternativas para acceder a los archivos:

- **Acceder a los archivos con una contraseña**

  Una vez que introduzca la contraseña, tendrá la capacidad de ver, modificar y guardar archivos en la unidad extraíble (tendrá *acceso transparente*). Kaspersky Endpoint Security podría otorgarle acceso de solo lectura a la unidad si el cifrado de unidades extraíbles está configurado del siguiente modo en la directiva:

  - El modo portátil está deshabilitado.
  - Se selecciona el modo **Cifrar todos los archivos** o **Solo cifrar archivos nuevos**.

  En los demás casos, tendrá acceso completo (de lectura y escritura) a la unidad extraíble. Podrá agregar y eliminar archivos.

  Los permisos de acceso a una unidad pueden modificarse en cualquier momento, incluso mientras la unidad está conectada al equipo. Si los permisos se modifican, Kaspersky Endpoint Security bloqueará el acceso a los archivos y le pedirá la contraseña nuevamente.

  Una vez que introduzca la contraseña, no podrá aplicar ajustes de directiva de cifrado para la unidad extraíble. En tal caso, no podrá descifrar los archivos de la unidad ni volver a cifrarlos.

- **Solicitarle al administrador que le brinde acceso a los archivos**

Si ha olvidado la contraseña que definió para utilizar el modo portátil, comuníquese con el administrador para que le brinde acceso a los archivos. Para realizar el pedido, deberá enviarle al administrador un archivo de solicitud de acceso, que tendrá la extensión KESDC. El archivo puede enviarse por correo electrónico o por cualquier otro medio. El administrador le enviará a usted un archivo de acceso (un archivo de extensión KESDR), que le permitirá acceder a los archivos cifrados.

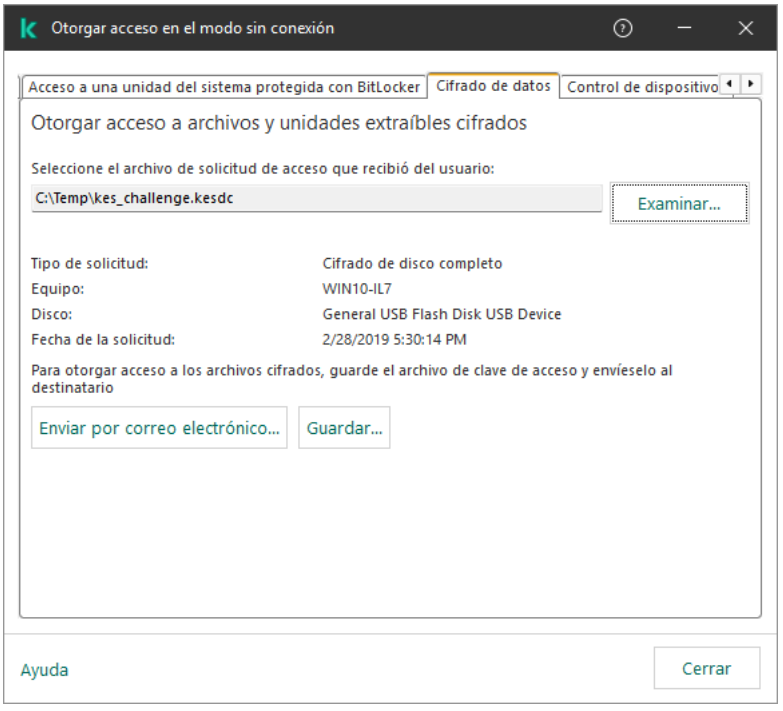
Tras completar el procedimiento de solicitud y respuesta para recuperar la contraseña, tendrá acceso total (de lectura y escritura) a la unidad extraíble y acceso transparente a los archivos que contenga.

Podrá aplicar una directiva de cifrado de unidades extraíbles y, con ello, descifrar archivos o realizar otras acciones. Una vez que haya recuperado 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 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. En la pestaña **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
4. En el menú contextual, seleccione **Otorgar acceso en el modo sin conexión**.
5. En la ventana que se abre, seleccione la pestaña **Cifrado de datos**.
6. En la ficha **Cifrado de datos**, haga clic en el botón **Examinar**.
7. En la ventana para seleccionar el archivo de solicitud de acceso, especifique la ruta al archivo que le haya enviado el usuario.

   Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.



Otorgar acceso en el modo sin conexión

Cómo obtener un archivo de acceso a datos cifrados mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Activos (dispositivos)**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los archivos a los que se necesite acceso.
3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.
4. Seleccione **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión KESDC).

   Web Console le mostrará información sobre la solicitud. Encontrará, entre otros datos, el nombre del equipo que contiene los archivos a los que el usuario necesita acceder.
6. Haga clic en el botón **Guardar clave** y seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión KESDR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

Descifrado de unidades extraíbles

Para descifrar una unidad extraíble, puede utilizarse una directiva. Las directivas en las que se definen los ajustes de cifrado de unidades extraíbles se crean para grupos de administración específicos. Por lo tanto, el resultado del descifrado de datos en unidades extraíbles depende del equipo al cual esté conectada la unidad extraíble.

Para descifrar unidades extraíbles:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
2. Seleccione la directiva correspondiente 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 quiere descifrar todos los archivos cifrados almacenados en las unidades extraíbles, en la lista desplegable **Modo de cifrado**, seleccione **Descifrar la unidad extraíble completa**.

5. Para descifrar datos almacenados en unidades extraíbles individuales, modifique las reglas de cifrado para las unidades extraíbles que contienen los datos que quiera descifrar. Para hacerlo:

   a. En la lista de unidades extraíbles para las que se configuraron reglas de cifrado, seleccione una entrada correspondiente a la unidad extraíble que necesita.

   b. Haga clic en el botón **Establecer una regla** para modificar la regla de cifrado para la unidad extraíble seleccionada.

   c. En el menú contextual del botón **Establecer una regla**, seleccione el elemento **Descifrar la unidad extraíble completa**.

6. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security descifra las unidades extraíbles que ya se encuentren conectadas al equipo o que el usuario conecte. La aplicación le advierte al usuario que el proceso de descifrado puede durar algunos minutos. Si el usuario inicia la extracción segura de un disco extraíble durante el descifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de descifrado de datos y permite la extracción del disco extraíble antes de que finalice la operación de descifrado. El proceso de descifrado se reanudará cuando el usuario conecte la unidad al equipo nuevamente.

Si no consigue descifrar una unidad extraíble, consulte el informe de **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Puede ocurrir que otra aplicación impida el acceso a los archivos. En tal caso, desconecte la unidad extraíble y vuelva a conectarla.

Visualización de detalles del cifrado de datos

En el transcurso del cifrado o descifrado, Kaspersky Endpoint Security envía información sobre el estado de los parámetros de cifrado correspondientes a los equipos cliente de Kaspersky Security Center.

Visualización del 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 canceló el cifrado de datos.
- **No cumple con la directiva debido a un error**. Error de cifrado de datos, por ejemplo, falta una licencia.
- **Aplicación de la directiva; se debe reiniciar el equipo**. El cifrado de datos está en curso en el equipo. Reinicie el equipo para completar el cifrado de datos.
- **Directiva de cifrado no especificada**. El cifrado de datos está desactivado en la configuración de la directiva.
- **No admitido**. Los componentes de cifrado de datos no están instalados en el equipo.
- **Aplicación de directiva**. El cifrado/descifrado de datos está en curso en el equipo.

Para ver el estado de 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 ficha **Dispositivos** del espacio de trabajo, deslice la barra de desplazamiento hasta el extremo derecho. Si la columna de **Estado de cifrado** no se muestra, agregue esta columna en la configuración de la consola de Kaspersky Security Center.

   La columna **Estado de cifrado** muestra el estado de cifrado de los datos de los equipos del grupo de administración seleccionado. Este estado se forma en base a la información sobre el cifrado de archivos en los discos locales del equipo y sobre el cifrado de disco completo.

4. Si el estado del cifrado de datos del equipo es **Aplicación de la directiva**, puede supervisar el panel de progreso del cifrado:

   a. Abra las propiedades del equipo con el estado de **Aplicación de la directiva** haciendo doble clic en él.

   b. En la ventana de propiedades del equipo, elija 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 los dispositivos** puede ver el progreso actual del cifrado de datos como un porcentaje.

Cómo ver las estadísticas de cifrado en los paneles de Kaspersky Security Center

Para ver el estado de 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 que se encuentra a la derecha del árbol de la Consola de administración, seleccione la ficha **Estadísticas**.

4. Cree una página nueva con paneles de detalles que contengan estadísticas de cifrado de datos. Para hacerlo:

   a. En la ficha **Estadísticas**, haga clic en el botón **Personalizar vista**.

   b. En la ventana que se abre, haga clic en el botón **Agregar**.

   c. Esto abre una ventana: allí ingrese el nombre de la página en la sección **General**.

   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 protección**, seleccione el elemento **Cifrado de los dispositivos**.

   f. Haga clic en **Aceptar**.

g. Si es necesario, edite la configuración del panel de detalles. Para ello, use las secciones **View** y **Dispositivos**.

h. Haga clic en **Aceptar**.

i. Repita los pasos d al h de las instrucciones: seleccione el elemento **Cifrado de unidades extraíbles** en la sección **Estado de protección**.

Los paneles de detalles agregados aparecerán en la lista **Paneles de información**.

j. Haga clic en **Aceptar**.

El nombre de la página con los paneles de detalles que creó en los pasos anteriores aparecerá en la lista **Páginas**.

k. Haga clic en el botón **Cerrar**.

5. En la ficha **Estadísticas**, abra la página que se creó en los pasos anteriores de las instrucciones.

Aparecen los paneles de detalles, que muestran el estado de cifrado de los equipos y unidades extraíbles.

Visualización de errores de cifrado en unidades de disco locales del equipo

Para visualizar errores de cifrado en unidades de disco locales 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**, 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 los destalles de los errores de cifrado de archivos que se produjeron en las unidades locales del equipo. Cuando se corrige un error, Kaspersky Security Center elimina los detalles del error de la ventana **Errores de cifrado de datos**.

Visualización del informe de cifrado de datos

Kaspersky Security Center le permite crear informes de cifrado de datos:

- **Informe sobre el estado de cifrado de los dispositivos administrados**. El informe incluye información sobre si el estado de cifrado de la computadora cumple con la directiva de cifrado.

- **Informe sobre el estado de 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 derechos de acceso a unidades cifradas**. El informe incluye información sobre el estado de las cuentas que tienen acceso a unidades cifradas.

- **Informe sobre los errores de cifrado de archivos**. El informe incluye información sobre los errores que ocurrieron durante la ejecución de tareas de cifrado o descifrado de datos en los equipos.

- **Informe sobre el bloqueo de acceso a los archivos cifrados**. El informe incluye información sobre aplicaciones bloqueadas para que no obtengan acceso a archivos cifrados.

Para ver el informe de cifrado de datos:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **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 las instrucciones del Asistente de plantilla de informe. En la ventana **Selección del tipo de plantilla de informe** en la sección **Otro**, seleccione uno de los informes de cifrado de datos.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de 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 del informe. El informe se muestra en una ventana nueva.

Trabajar con dispositivos cifrados cuando no tenemos acceso a ellos

Obtención de acceso a dispositivos cifrados

Se puede requerir a un usuario que solicite 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 aun si no hay conexión con Kaspersky Security Center.

El acceso a dispositivos cifrados se puede obtener de las siguientes maneras:

1. Desde la interfaz de Kaspersky Endpoint Security, el usuario crea un archivo de solicitud de acceso (que tendrá la extensión kesdc) y se lo envía al administrador de la LAN corporativa.

2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso (que tendrá la extensión kesdr) y se lo envía al usuario.

3. El usuario aplica la clave de acceso.

Restaurar datos de dispositivos cifrados

Un usuario puede usar la Utilidad de restauración de dispositivos cifrados (en adelante también llamada Utilidad de restauración) para trabajar con dispositivos cifrados. Esto puede resultar necesario en los siguientes casos:

- El procedimiento de usar una clave de acceso para obtener acceso falló.

- No se han instalado los componentes de cifrado en el equipo con el dispositivo cifrado.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración residen en la memoria del equipo del usuario de forma no cifrada desde hace algún tiempo. Para reducir el riesgo de acceso no autorizado a tales datos, se le aconseja restaurar el acceso a los dispositivos cifrados en equipos de confianza.

Los datos en dispositivos cifrados se pueden restaurar de la siguiente forma:

1. Mediante la Utilidad de restauración, el usuario crea un archivo de solicitud de acceso (que tendrá la extensión fdertc) y se lo envía al administrador de la LAN corporativa.

2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso (que tendrá la extensión fdertr) y se lo envía al usuario.

3. El usuario aplica la clave de acceso.

Para restaurar datos en discos duros del sistema 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 se han dañado, el usuario debe completar el procedimiento de restauración usando un archivo de solicitud de acceso.

Antes de restaurar datos de dispositivos cifrados, se recomienda cancelar la directiva de Kaspersky Security Center o deshabilitar el cifrado en la configuración de la directiva de Kaspersky Security Center en el equipo donde se realizará el procedimiento. Ello evitará que el dispositivo vuelva a cifrarse.

Recuperación de datos con la Utilidad de restauración FDERT

Cuando un disco duro sufre un daño, su sistema de archivos puede presentar irregularidades. Ante esta situación, la información que se haya protegido con la tecnología Cifrado de disco de Kaspersky quedará inaccesible. En tal caso, puede descifrar la información y copiarla a un nuevo disco duro.

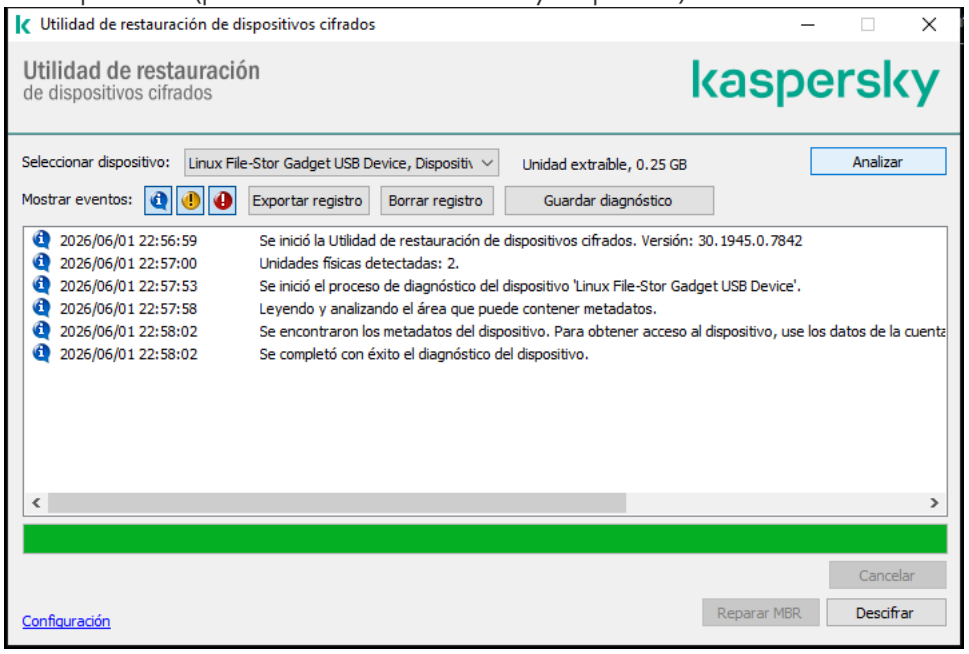
Para recuperar los datos de una unidad protegida con Cifrado de disco de Kaspersky, siga estos pasos:

1. Cree una Utilidad de restauración independiente (vea la imagen de más abajo).

2. Conecte el disco a un equipo en el que no se hayan instalado los componentes de cifrado de Kaspersky Endpoint Security.

3. Ejecute la Utilidad de restauración y realice un diagnóstico del disco duro.

4. Acceda a los datos del disco. Para ello, introduzca las credenciales del Agente de autenticación o realice el procedimiento de recuperación (procedimiento de solicitud y 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 principal de la aplicación haga clic en el botón .

2. En la ventana que se abre, haga clic en el botón **Restaurar dispositivo cifrado**.

   Se inicia la Utilidad de restauración de dispositivos cifrados.

3. Haga clic en el botón **Crear Utilidad de restauración independiente** en la ventana de la Utilidad de Restauración.

4. Guarde la Utilidad de restauración independiente en el equipo.

El archivo ejecutable de la Utilidad de restauración (fdert.exe) se guardará en la carpeta que haya seleccionado. Copie la Utilidad de restauración a un equipo en el que no se hayan instalado 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 residen en la memoria del equipo del usuario de forma no cifrada desde hace algún tiempo. Para reducir el riesgo de acceso no autorizado a tales datos, se le aconseja restaurar el acceso a los dispositivos cifrados en equipos de confianza.

Recuperación de los datos almacenados en el disco duro

Para restaurar el acceso a dispositivos cifrados con la Utilidad de Restauración:

1. Ejecute el archivo fdert.exe (el archivo ejecutable de la Utilidad de restauración). Este archivo es creado por Kaspersky Endpoint Security.

2. En la ventana Utilidad de restauración, seleccione el dispositivo cifrado al que desee restaurar el acceso.

3. Haga clic en el botón **Analizar** para permitir que la utilidad defina cuál de las acciones debe realizar en el dispositivo: si se lo debe desbloquear o descifrar.

   Si el equipo tiene acceso a la funcionalidad del cifrado de Kaspersky Endpoint Security, la utilidad de restauración le solicita desbloquear el dispositivo. Si bien desbloquear el dispositivo no lo descifra, el dispositivo queda accesible directamente por estar desbloqueado. Si el equipo no tiene acceso a la funcionalidad del cifrado de Kaspersky Endpoint Security, la utilidad de restauración le solicita descifrar el dispositivo.

4. Si desea importar la información de diagnóstico, haga clic en el botón **Guardar diagnóstico**.

   La utilidad guardará un archivo comprimido, que contendrá los archivos con la información de diagnóstico.

5. Haga clic en el botón **Reparar MBR** si el diagnóstico del disco duro cifrado del sistema ha generado un mensaje sobre problemas relacionados con el registro de arranque maestro (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 **Desbloquear** o **Descifrar** según los resultados de diagnóstico.

7. Si desea utilizar una cuenta del Agente de autenticación para restaurar los datos, seleccione la opción **Usar 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 de un disco duro del sistema. Si el disco duro del sistema está dañado y se han perdido los datos de la cuenta del Agente de autenticación, debe obtener una clave de acceso del administrador de la red de área local corporativa para restaurar los datos de un dispositivo cifrado.

8. Si desea iniciar el procedimiento de recuperación, haga lo siguiente:

   a. Seleccione la opción **Especificar clave de acceso manualmente**.

   b. Haga clic en el botón **Recibir clave de acceso** y guarde el archivo de solicitud de acceso (un archivo de extensión FDERTC) en el equipo.

   c. Envíe el archivo de solicitud de acceso al administrador de la red LAN corporativa.

   > No cierre la ventana **Recibir clave de acceso al dispositivo** hasta que haya recibido la clave de acceso. Cuando esta ventana se abra nuevamente, no podrá aplicar la clave de acceso creada anteriormente por el administrador.

   d. El administrador de la LAN corporativa creará y le enviará un archivo de acceso, cuya extensión será FDERTR. Guarde este archivo (consulte las instrucciones a continuación).

   e. Descargue el archivo de acceso a través de la ventana **Recibir clave de acceso al dispositivo**.

9. Si necesita descifrar el dispositivo, deberá configurar algunas opciones adicionales:

   - Especifique el área para descifrar:

     - Si desea descifrar todo el dispositivo, seleccione la opción **Descifrar todo el dispositivo**.

     - Si desea descifrar solo parte de los datos del dispositivo, seleccione la opción **Descifrar áreas individuales del dispositivo** y especifique los límites del área para 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 **Guardar datos descifrados 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 **Guardar datos descifrados 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**.

    Se inicia el proceso de desbloqueo o descifrado del dispositivo.

Cómo crear un archivo de clave de acceso para archivos 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** → **Unidades cifradas**.

3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que necesite crear el archivo de clave de acceso. A continuación, en el menú contextual del dispositivo, haga clic **Obtener acceso al dispositivo en Kaspersky Endpoint Security**.

   Si no sabe con seguridad a qué equipo corresponde 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 **Obtener clave de cifrado del dispositivo en Kaspersky Endpoint Security**.

4. En la ventana que se abre, seleccione el algoritmo de cifrado que se deba usar: AES256 o AES56.

   El algoritmo de cifrado 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 le haya enviado el usuario.

6. Haga clic en **Desbloquear**.

Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.

Cómo crear un archivo de clave de acceso para archivos cifrados en Web Console

1. En la ventana principal de Web Console, seleccione **Operaciones** → **Protección y cifrado de datos** → **Unidades cifradas**.

2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los datos a los que se necesite acceso.

3. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.

   Se inicia un asistente para otorgar acceso al dispositivo.

4. Siga las instrucciones del asistente para otorgar acceso al dispositivo:

   a. Seleccione el complemento de Kaspersky Endpoint Security para Windows.

   b. Seleccione el algoritmo de cifrado que se deba usar: AES256 o AES56.

      El algoritmo de cifrado 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 le haya enviado el usuario (el archivo tendrá la extensión FDERTC).

   d. Seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión FDERTR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle 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 al disco duro cifrado por algún motivo y no se puede cargar el sistema operativo.

Puede cargar una imagen del sistema operativo Windows con el disco de rescate y restaurar el acceso al disco duro cifrado mediante 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 previo al arranque de Windows. Al crear la imagen personalizada del entorno previo al arranque de Windows, agregue el archivo ejecutable de la Utilidad de Restauración a la imagen.

3. Guarde la imagen personalizada del entorno previo a la instalación de Windows en un medio de inicio, como ser un CD o un disco extraíble.

   Consulte los archivos de ayuda de Microsoft si desea conocer las instrucciones para crear una imagen personalizada del entorno previo al arranque de Windows (por ejemplo, en el recurso Microsoft TechNet).

Soluciones Detection and Response

Las soluciones 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 Detection and Response brindan información sobre la amenaza detectada y permiten administrar las acciones de Respuesta ante amenazas.

Por lo tanto, la solución Detection and Response hace lo siguiente:

- Recibe información sobre la operación de una computadora, servidor u otros dispositivos (telemetría).
- Analiza automáticamente la información para detectar amenazas.
- Genera detalles de alerta como columnas de la cadena de desarrollo de amenazas para el análisis y la elección de acciones de respuesta ante amenazas.
- Lleva a cabo acciones de respuesta ante amenazas (por ejemplo, aislamiento de la red de la computadora).

Kaspersky Endpoint Security es compatible con las soluciones Detection and Response a través de un agente integrado. El agente incorporado envía telemetría a los servidores de soluciones y lleva a cabo acciones de respuesta ante amenazas. El agente integrado admite lo siguiente:

- 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 utilizar Kaspersky Endpoint Security con la solución de 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 adquirir una licencia para cada una de las soluciones. La licencia puede incluir el derecho a utilizar una única solución (por ejemplo, solo el complemento de MDR) o varias soluciones, el complemento [EDR Optimum+MDR].

MDR y EDR Optimum admiten los siguientes métodos de licencia:

- La funcionalidad MDR o EDR Optimum está incluida en la licencia de Kaspersky Endpoint Security para Windows.

  La funcionalidad está disponible inmediatamente después de activar Kaspersky Endpoint Security para Windows. Solo necesita agregar una clave.

- Licencias independientes para MDR o EDR Optimum (MDR Add-on, EDR Optimum Add-on o [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 agregan 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 agregarse.

Kaspersky Endpoint Security permite agregar solo una *clave activa* para licencias MDR y EDR Optimum. Por lo tanto, si necesita activar ambas soluciones, debe agregar una clave de complemento [EDR Optimum+MDR] Add-on en lugar de una clave separada para cada solución. También puede agregar una *clave de reserva*.

Si usó un archivo BLOB al implementar MDR, no necesita una clave separada para activar MDR. El archivo BLOB ya contiene información de licencia.

Licencia inicial 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. Si desea agregar una clave, use la tarea *Agregar clave* o utilice la funcionalidad de distribución automática de claves. La clave de licencia se agrega a la aplicación como una segunda clave activa o como una 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 agregó 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 agrega la nueva clave a la aplicación, sino que reemplaza la clave actual con la nueva clave. La razón de esto es la restricción que le permite a la aplicación agregar una sola clave para activar MDR y EDR Optimum.

Por ejemplo, supongamos 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 usar 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 incluyen la misma cantidad de soluciones. Es decir, si agregó una clave de complemento EDR Optimum, no puede reemplazar esta clave con una clave de complemento MDR. Sin embargo, puede reemplazar la clave de complemento EDR Optimum con una clave de complemento [EDR Optimum + MDR]. La aplicación también rechaza las claves si intenta reemplazar una clave de complemento MDR con una clave de complemento EDR. Para reemplazar una clave, puede ejecutar la tarea *Agregar clave*. La tarea *Agregar clave* permite reemplazar las claves de licencia por las soluciones que se deseen.

Si agregó una clave de reserva de [EDR Optimum+MDR] Add-on, para agregar una clave activa de complemento EDR Optimum o MDR correctamente, primero debe sustituir la clave de reserva por una clave de complemento EDR Optimum o MDR, o bien eliminar la clave de reserva y, a continuación, sustituir la clave activa.

Compatibilidad con soluciones EDR de terceros

Puede usar Kaspersky Endpoint Security para proteger estaciones de trabajo y servidores junto con soluciones EDR de terceros. Para eliminar los falsos positivos, recomendamos agregar 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.14.1.0`	`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 permite que la aplicación interactúe con otras soluciones de Kaspersky para detectar amenazas avanzadas (p. ej., Kaspersky Sandbox). Cada solución de Kaspersky es compatible con una versión específica de Kaspersky Endpoint Agent.

Para usar Kaspersky Endpoint Agent como parte de las soluciones de Kaspersky, debe activar dichas soluciones con la clave de licencia correspondiente.

Si necesita información más detallada sobre la versión de Kaspersky Endpoint Agent incluida en su solución de software, o para más detalles sobre la solución independiente, consulte la guía de ayuda del producto que corresponda:

- 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 las versiones 11.2.0 a 11.8.0 de Kaspersky Endpoint Security incluye Kaspersky Endpoint Agent. Puede seleccionar Kaspersky Endpoint Agent al instalar Kaspersky Endpoint Security para Windows. De este modo, 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) a 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 toda la Detection and Response para trabajar con el agente incorporado 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 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)	Kaspersky Anti Targeted Attack Platform (componente Network Detection and Response)
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 incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	Kaspersky Endpoint Agent
12.6	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**	**Agente incorporado**

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. Cuando despliegue Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, las soluciones de Detection and Response seguirán funcionando con Kaspersky Endpoint Security. Además, se eliminará Kaspersky Endpoint Agent del equipo.

El kit de distribución para las versiones 11.2.0 a 11.8.0 de Kaspersky Endpoint Security incluye Kaspersky Endpoint Agent. Puede seleccionar Kaspersky Endpoint Agent al instalar Kaspersky Endpoint Security para Windows. De este modo, 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.

Migrar la configuración [KES+KEA] a [KES+agente incorporado] incluye los siguientes pasos:

1. **Actualizar Kaspersky Security Center**

   Actualice todos los componentes de Kaspersky Security Center a la versión 13.2 o superior, incluido el Agente de red en las computadoras de los usuarios y en Web Console.

2. **Actualizar el complemento web de Kaspersky Endpoint Security**

En Kaspersky Security Center Web Console, actualice 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 nueva directiva 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 licencia**

   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 luego de actualizar la aplicación a la versión 11.7.0. No necesita realizar ninguna otra acción.

   Si utiliza una licencia independiente de complemento Kaspersky Endpoint Detection and Response Optimum para activar la funcionalidad EDR Optimum, debe asegurarse de que la clave de complemento EDR Optimum se agregue al repositorio de Kaspersky Security Center y de que la funcionalidad de distribución automática de claves de licencia esté habilitada. Luego 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 *Agregar clave*.

   No necesita activar la funcionalidad de Kaspersky Sandbox. Kaspersky Sandbox estará disponible de forma inmediata luego de la actualización y activación de 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. Luego 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 la funcionalidad de Kaspersky Sandbox y EDR Optimum, 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 para 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, escriba la contraseña de desinstalación en la configuración de la tarea *Instalar aplicación de forma remota*. Puede ingresar la contraseña de desinstalación a partir de Kaspersky Security Center Linux 15.1.

También puede actualizar la aplicación utilizando los siguientes métodos:

- Utilizando el servicio de actualización de Kaspersky (Seamless Update - SMU).
- De manera 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 usar 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 mediante Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tiene 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. Después de esto, Kaspersky Endpoint Security pasa a usar el agente incorporado y elimina Kaspersky Endpoint Agent.

6. **Reinicio del equipo**

   Reinicie el equipo para terminar de actualizar la aplicación con el agente integrado. Al actualizar la aplicación, el instalador elimina Kaspersky Endpoint Agent antes de que se reinicie el equipo. Después de reiniciar el equipo, el instalador agrega el agente incorporado. Esto significa que Kaspersky Endpoint Security no realiza las funciones de EDR ni Kaspersky Sandbox hasta que se reinicia el equipo.

7. **Revisar el estado de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox**

Luego de la actualización, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.
- El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes 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 de EDR Optimum esté activada mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de 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 la tarea y la directiva de 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 estándar de tareas y directivas de Kaspersky Security Center.

Se recomienda comenzar con la migración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en un solo equipo, luego hacerlo en un grupo de equipos, y finalmente completar la migración en todos los equipos de la organización.

Para migrar la configuración de la tarea y la directiva de Kaspersky Endpoint Agent a Kaspersky Endpoint Security, siga los siguientes pasos:

en la ventana principal de Web Console, seleccione **Operaciones** → **Migración de Kaspersky Endpoint Agent**.

Esto ejecuta el Asistente de migración de tareas y directivas. Siga las instrucciones del Asistente.

Paso 1. Migración de la directiva

El Asistente de migración crea una nueva directiva que fusiona la configuración de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuya configuración desee fusionar 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 fusionar la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de la tarea

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desea crear para la directiva de Kaspersky Endpoint Security. El asistente es compatible con las tareas de la solución Kaspersky Endpoint Detection and Response y Kaspersky Sandbox. Vaya al siguiente paso.

Paso 3. Fin del Asistente

Salga del Asistente. Como resultado, el asistente hace lo siguiente:

- Cree una nueva directiva de Kaspersky Endpoint Security.

  La directiva fusiona 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 nueva directiva 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 nueva directiva combinada.

  > Luego de realizar la migración de Kaspersky Endpoint Agent a 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 surjan errores al conectar el equipo a los servidores de Central Node. Esto se debe a que el asistente de migración de Web Console omite la siguiente configuración de directiva y no la migra:

  - Prohibición de modificación de configuración **Conexión a servidores KATA** ("candado").

    De forma predeterminada, la configuración se puede modificar (el "candado" está abierto). Por lo tanto, la configuración no se aplica al equipo. Debe prohibir la modificación de la configuración y cerrar el "candado".

  - Contenedor cifrado.

    Si utiliza autenticación de dos factores para conectarse a los servidores de Central Node, debe volver a agregar el contenedor cifrado. El asistente de migración migra correctamente el certificado TLS del servidor.

El Asistente de migración de la tarea y la directiva de la Consola de administración (MMC) migra toda la configuración de la solución Kaspersky Anti Targeted Attack Platform (EDR).

- Cree nuevas tareas de Kaspersky Endpoint Security.

  Las nuevas tareas son copias de las tareas de Kaspersky Endpoint Agent para las soluciones 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, seleccione 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. Seleccionar la aplicación para la que desea convertir directivas y tareas

En este paso, debe seleccionar Kaspersky Endpoint Security para Windows. Vaya al siguiente paso.

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 cuya configuración desee transferir a la directiva de Kaspersky Endpoint Security. Vaya al siguiente paso.

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. Se nombrarán nuevas directivas como *<nombre de la directiva> (convertido)*.

Paso 3. Conversión de tareas

Omita este paso. El asistente es compatible solo con las tareas de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox. La administración de estos componentes solo está disponible en Web Console. Vaya al siguiente paso.

Paso 4. Fin del Asistente

Salga del Asistente. Al finalizar el 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 admitir las soluciones Kaspersky Managed Detection and Response:

- 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 monitorea 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 el equipo debe estar agregado en la consola de Kaspersky Security Center. Para habilitar la interacción de EDR Agent con Kaspersky Security Center, debe instalar el complemento de administración para 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 adecuada.

Se deben instalar las siguientes aplicaciones de Kaspersky en la infraestructura para admitir las soluciones de Kaspersky Detection and Response:

	• Agente de red • EDR Agent
Endpoint	
	Complemento de administración para Kaspersky Endpoint Security para Windows
Kaspersky Security Center	
Soluciones Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Instalar EDR Agent

Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent (EDR Agent) para las soluciones Kaspersky Detection and Response se instala de la misma manera.

EDR Agent se puede instalar en el equipo de varias maneras:

- De manera remota, a través de Kaspersky Security Center.
- De manera local con el Asistente de instalación.
- De manera local con la línea de comandos (solo para KATA (EDR) y EDR Expert (on-premises)).

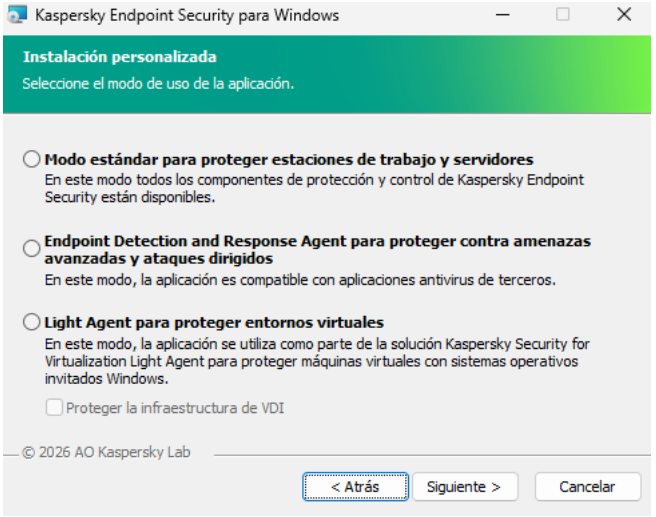
Para instalar EDR Agent, debe seleccionar la configuración adecuada en la configuración del paquete de instalación o en el Asistente de instalación.

Cómo instalar EDR Agent con el Asistente de configuración

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

   Se inicia el Asistente de instalación.

Configuración de Kaspersky Endpoint Security



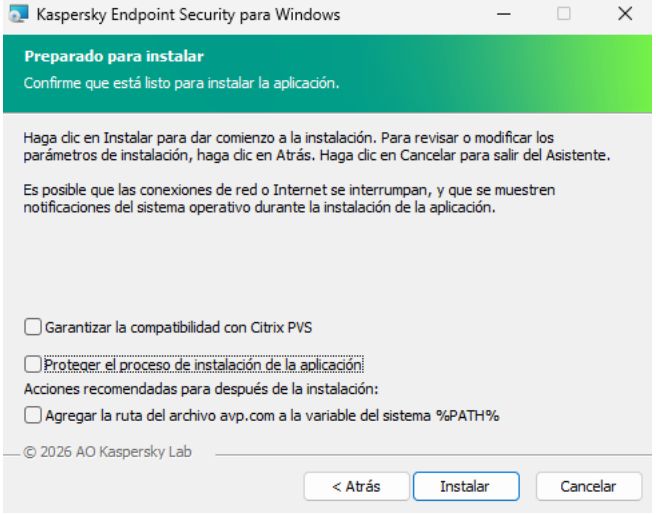
Elegir la configuración de la aplicación

Seleccione la configuración de **Endpoint Detection and Response Agent**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros.

Componentes de Kaspersky Endpoint Security

Seleccione los componentes que desea instalar. Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles. Para ello, deberá ejecutar el Asistente de instalación nuevamente y seleccionar la opción que permite cambiar los componentes disponibles.

La configuración avanzada



Configuración avanzada de la instalación de la aplicación

Proteger el proceso de instalación de la aplicación. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda deshabilitar 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.

Agregar la ruta del archivo avp.com a la variable del sistema %PATH%. Puede agregar la ruta de instalación a la variable %PATH% para facilitar el uso de la interfaz de línea de comandos.

Cómo instalar EDR Agent desde la línea de comandos (solo para KATA (EDR) y EDR Expert (on-premises))

1. Abra el símbolo del sistema (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

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

De esta manera, 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 esté instalada y comprobar su configuración, ejecute el comando `status`.

Cómo instalar EDR Agent con 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**.

   Se abre una lista con los paquetes de instalación que se han descargado a Kaspersky Security Center.

3. Abra las propiedades del paquete de instalación.

   Si es 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 proteger contra amenazas avanzadas y ataques dirigidos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros.

6. Seleccione los componentes que desea instalar.

   Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles.

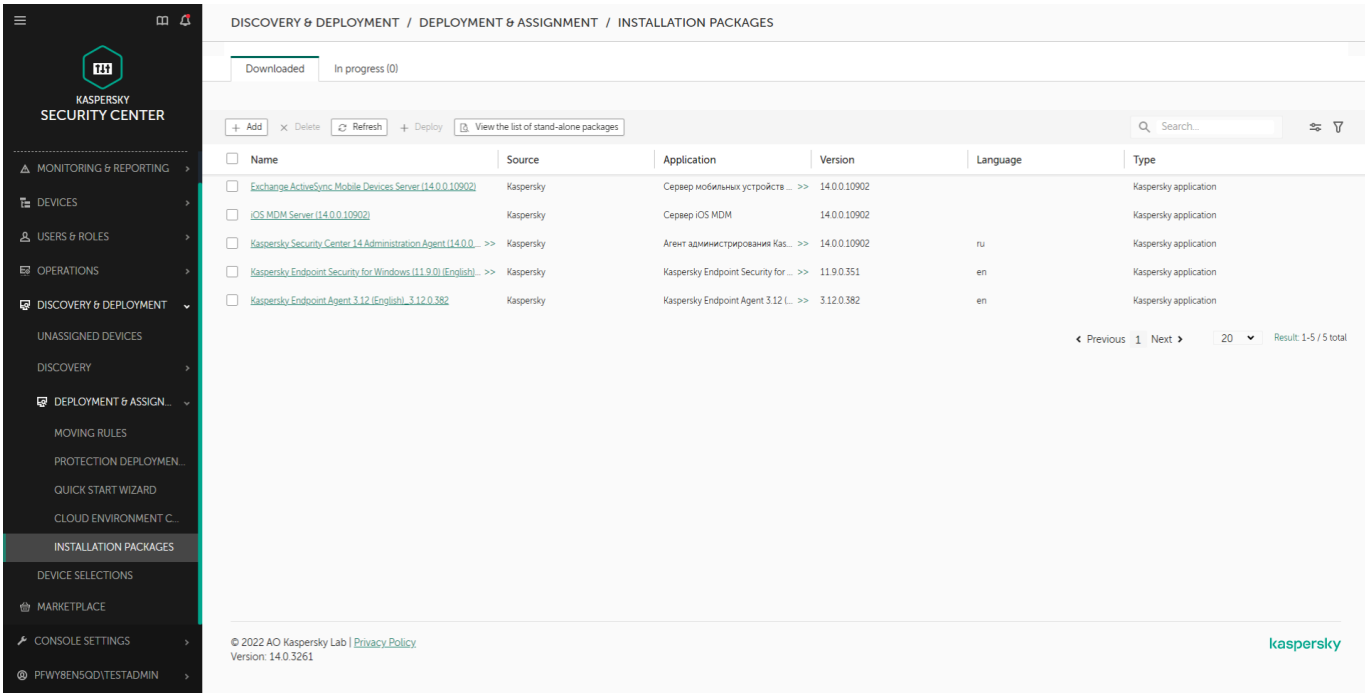
7. Guarde los cambios.

8. Crear una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que creó.

Cómo instalar EDR Agent con Web Console

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

Se abre una lista con los paquetes de instalación que se han descargado a Kaspersky Security Center.



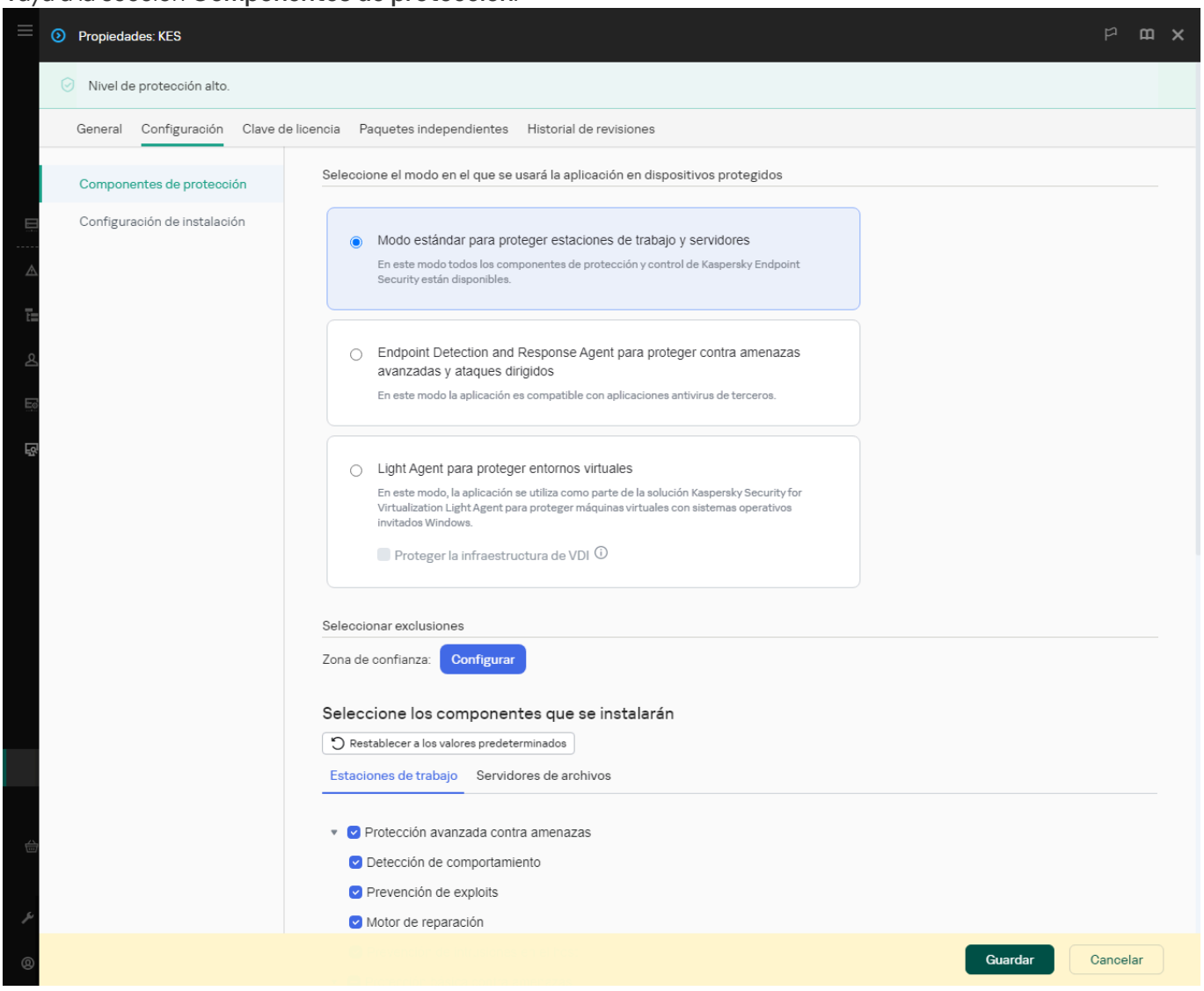
Lista de paquetes de instalación

2. Abra las propiedades del paquete de instalación.

   Si es necesario, cree un nuevo paquete de instalación.

3. Seleccione la ficha **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 para proteger contra amenazas avanzadas y ataques dirigidos**. En esta configuración, solo puede instalar los componentes que brindan soporte para las soluciones de Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) y KUMA. Esta configuración es necesaria si se implementa una 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 de EPP de terceros.

6. Seleccione los componentes que desea instalar.

   Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles.

7. Guarde los cambios.

8. Crear una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que creó.

Como consecuencia, EDR Agent se instala en el equipo del usuario. Puede utilizar la interfaz de la aplicación, y se muestra un ícono 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 contra archivos peligrosos. No es necesario realizar ninguna acción.

Si no pudo 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 la configuración avanzada de la aplicación y, por ejemplo, crear una zona de confianza u ocultar la interfaz de la aplicación. La configuración en las siguientes secciones está disponible:

- Kaspersky Security Network
- Configuración de la aplicación
- Configuración de red
- Exclusiones
- Informes

- Interfaz
- Administrar configuración

Integrar 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 secuencias 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 nueva conexión 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 el interruptor de **Conexión en segundo plano para la integración Habilitada**.
4. Guarde los cambios.

El proceso de integración con Kaspersky Managed Detection and Response se divide en los siguientes pasos:

1. **Instalación del componente Managed Detection and Response**

   Puede seleccionar el componente MDR durante la instalación o la actualización, además de usar 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 deshabilitar la opción **Comprobar si hay aplicaciones incompatibles de terceros** en la configuración de la tarea.

2. **Configuración de Kaspersky Private Security Network**

   > Omita este paso si está usando 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). A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky.

   En las propiedades del Servidor de administración, cargue el archivo de configuración de Kaspersky Security Network. Encontrará el archivo de configuración de Kaspersky Security Network dentro del archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre cómo configurar Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center. Si lo prefiere, puede cargar el archivo de configuración de Kaspersky Security Network al equipo utilizando la línea de comandos (consulte las instrucciones a continuación).

Cómo configurar Kaspersky Private Security Network mediante la línea de comandos

1. Abra el símbolo del sistema (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 contenga 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 los archivos, las aplicaciones y los sitios web. La sección **Kaspersky Security Network** de la configuración de la directiva mostrará el siguiente estado operativo: *Infraestructura: Kaspersky Private Security Network*.

Debe habilitar el modo KSN extendido para que Managed Detection and Response funcione.

3 **Activar Kaspersky Managed Detection and Response**

A partir de Kaspersky Endpoint Security 12.10 para Windows, para activar la funcionalidad Managed Detection and Response, además de una código de activación, puede utilizar un archivo de clave.

Tiene que comprar una licencia por separado para MDR (complemento de Kaspersky Managed Detection and Response).

La funcionalidad se vuelve disponible después de agregar una clave diferente para el complemento de Kaspersky Managed Detection and Response. La licencia para la funcionalidad independiente Managed Detection and Response es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad de MDR esté incluida en la licencia y de que esté en funcionamiento en la interfaz local de la aplicación.

4 **Habilitar los componentes de Managed Detection and Response**

Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (consulte las instrucciones más abajo). El archivo BLOB contiene la ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. Encontrará el archivo BLOB en el archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre el archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

A partir de Kaspersky Endpoint Security 12.6 para Windows, la adición de un archivo BLOB es opcional para Kaspersky Managed Detection and Response sin inquilinos si tiene una licencia actual.

Cómo habilitar 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 correspondiente 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 de verificación **Managed Detection and Response (Industrial CyberSecurity)**.

5. En el bloque **Configuración**, haga clic en **Cargar** y seleccione el archivo BLOB que obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tendrá la extensión P7.

   De manera predeterminada, el usuario puede administrar la configuración de la aplicación (el "candado" está abierto). Para aplicar la directiva en los equipos, cierre los candados .

6. Guarde los cambios.

Cómo habilitar 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.

5. Active el interruptor de **Managed Detection and Response HABILITADA**.

6. Haga clic en **Cargar** y seleccione el archivo BLOB que obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tendrá la extensión P7.

   De manera predeterminada, el usuario puede administrar la configuración de la directiva (el "candado" está abierto). Para aplicar la directiva en los equipos, cierre los candados .

7. Guarde los cambios.

Cómo habilitar Managed Detection and Response desde la línea de comandos

1. Abra el símbolo del sistema (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 habilitada. El usuario debe tener el permiso **Configurar la aplicación**.

Como resultado, Kaspersky Endpoint Security verificará el archivo BLOB. Durante la verificación del archivo BLOB, se controlarán la firma digital y el plazo de la licencia. De no ocurrir errores en este proceso, Kaspersky Endpoint Security descargará el archivo y lo enviará al equipo cuando se realice la siguiente sincronización con Kaspersky Security Center. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Managed Detection and Response** se agregará a la lista de componentes de Kaspersky Endpoint Security.

5. **Configuración de otros componentes de la aplicación para recibir telemetría**

   Debe habilitar los siguientes componentes para que Managed Detection and Response funcione:

   - Kaspersky Security Network (modo ampliado).
   - Detección de comportamiento.
   - Prevención de exploits.
   - Protección contra amenazas web.
   - Protección contra amenazas de correo.
   - Protección contra archivos peligrosos.
   - Protección contra amenazas de red.
   - Firewall.
   - Protección vía 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 ficha **Configuración de la aplicación**.
   4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.
   5. Active el interruptor de **Managed Detection and Response HABILITADA**.
   6. Guarde los cambios.

   1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
   2. Seleccione la directiva correspondiente 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 de verificación **Managed Detection and Response (Industrial CyberSecurity)**.
   5. Guarde los cambios.

Integrar KATA Agent con EDR (EDR)

EDR Agent se instala en estaciones de trabajo y servidores en la infraestructura de TI de la organización. En estos equipos, EDR Agent monitorea continuamente procesos, conexiones de red abiertas y archivos que se modifican, y envía datos de monitoreo al servidor con el componente Central Node.

Para la integración con EDR (KATA), debe habilitar 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)**

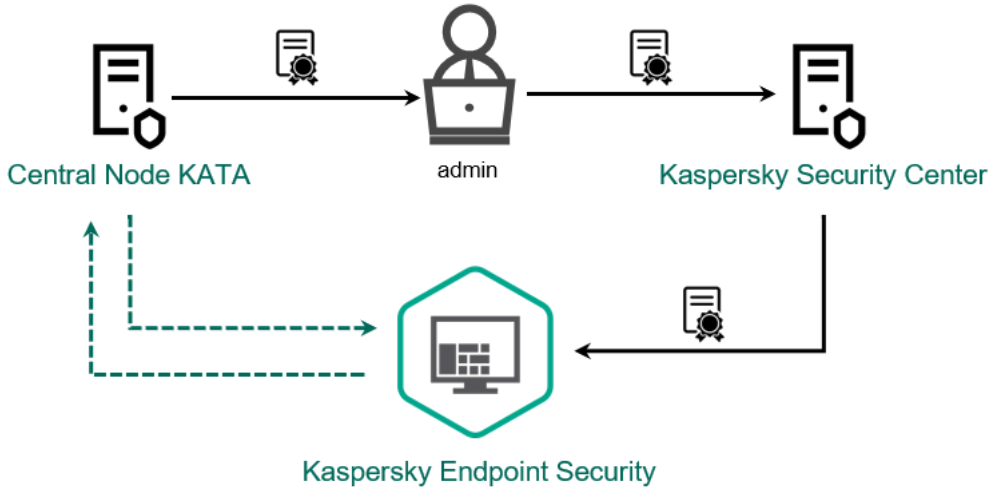
   Tiene que comprar una licencia por separado para EDR (KATA) (complemento de Kaspersky Endpoint Detection and Response [KATA]).

   La funcionalidad se vuelve disponible después de agregar 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 que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad de EDR (KATA) esté incluida en la licencia y de que esté en ejecución en la interfaz local de la aplicación.

2. **Conexión a Central Node**

Kaspersky Anti Targeted Attack Platform exige 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). Luego, 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 habilitar esta verificación, debe activar la autenticación bidireccional en la configuración de Central Node y Kaspersky Endpoint Security. Para usar autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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 a 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 correspondiente 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 de verificación **Endpoint Detection and Response Expert (on-premises)**.
6. Haga clic en **Configuración de conexión del servidor**.
7. Configure la conexión del servidor:
   - **Tiempo de espera (s)**. 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).

- **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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

  El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

8. Haga clic en **Aceptar**.

9. Agregue servidores de Central Node. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

   Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 íconos de candado y guarde los cambios.

Cómo conectar un equipo con Kaspersky Endpoint Security a 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premise)**.

5. Active el interruptor de **Endpoint Detection and Response Expert (on-premise) HABILITADO**.

6. Para configurar EDR (KATA), seleccione **Endpoint Detection and Response Expert (versión 7.1 o anterior)** de la lista de soluciones.

7. Haga clic en **Configuración de conexión**.

8. Configure la conexión del servidor:

   - **Tiempo de espera (s)**. 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

  El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

9. Haga clic en **Aceptar**.

10. Agregue servidores de Central Node. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

    Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 íconos de candado y guarde los cambios.

Como resultado, se agrega el equipo a la consola de Kaspersky Anti Targeted Attack Platform. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (on-premises)** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Integrar KATA Agent con NDR (EDR)

EDR Agent se instala en estaciones de trabajo y servidores en la infraestructura de TI de la organización. En estos equipos, EDR Agent monitorea continuamente procesos, conexiones de red abiertas y archivos que se modifican, y envía datos de monitoreo al servidor con el componente Central Node.

Para la integración con NDR (KATA), debe habilitar 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 posterior.
- 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)**

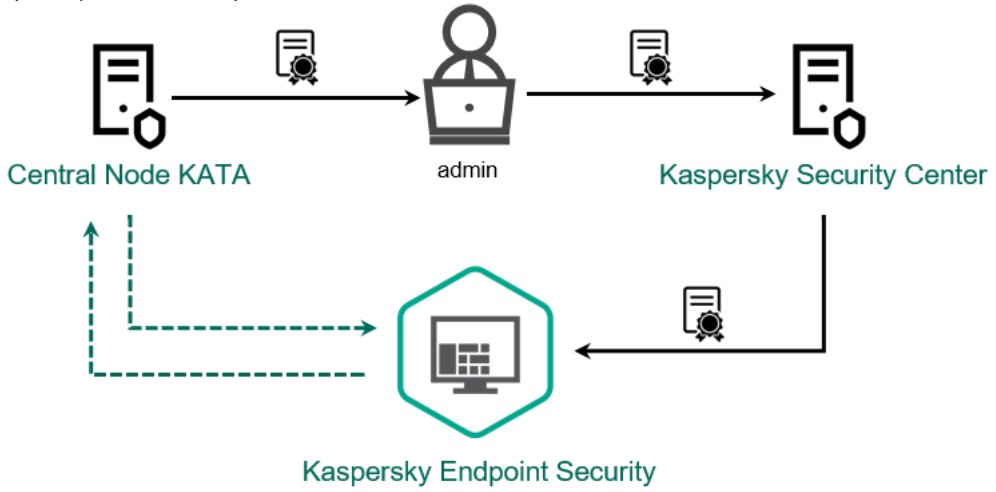
   Tiene que comprar una licencia por separado para NDR (KATA) (complemento de Kaspersky Network Detection and Response [KATA]).

   La funcionalidad se vuelve disponible después de agregar 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 que la de Kaspersky Endpoint Security.

   Asegúrese de que la funcionalidad de NDR (KATA) esté incluida en la licencia y de que esté en ejecución en la interfaz local de la aplicación.

2. **Conexión a Central Node**

   Kaspersky Anti Targeted Attack Platform exige 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). Luego, 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 habilitar esta verificación, debe activar la autenticación bidireccional en la configuración de Central Node y Kaspersky Endpoint Security. Para usar autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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 a 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 correspondiente 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 de verificación **Network Detection and Response (KATA)**.
5. Haga clic en **Configuración de conexión**.
6. Configure la conexión del servidor:
   - **Tiempo de espera (s)**. 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
7. Haga clic en **Aceptar**.
8. Agregue servidores de Central Node. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.
9. Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 a 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Network Detection and Response (KATA)**.

5. Active el interruptor de **Network Detection and Response (KATA) HABILITADO**.

6. Haga clic en **Configuración de conexión**.

7. Configure la conexión del servidor:

   - **Tiempo de espera (s)**. 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

8. Haga clic en **Aceptar**.

9. Agregue servidores de Central Node. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

10. Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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, se agrega el equipo a la consola de Kaspersky Anti Targeted Attack Platform. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Network Detection and Response (KATA)** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Integración del 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 de forma continua procesos, conexiones de red abiertas y archivos que se modifican, y envía datos de monitoreo al servidor de EDR Expert (on-premise).

Para la integración con EDR, debe habilitar 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. **Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Tiene que comprar una licencia por separado para EDR Expert (on-premises) (complemento de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La funcionalidad se vuelve disponible después de agregar 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 de EDR Expert (on-premises) esté incluida en la licencia y de que esté en ejecución en la interfaz local de la aplicación.

2. **Conexión a servidores de recopilación de telemetría y al servidor de respuesta**

   Kaspersky Endpoint Detection and Response Expert (on-premises) exige una conexión de confianza entre Kaspersky Endpoint Security y dos servidores:

   - Un *servidor de recopilación de telemetría* es un servidor que forma parte de una solución SIEM y que recopila, normaliza, correlaciona, analiza y almacena información sobre los eventos que ocurren en el equipo.

   - Un *servidor de respuesta* es un servidor que recibe y analiza datos, estudia el comportamiento de los objetos y publica los resultados de dichos estudios.

   Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Luego, 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 habilitar esta verificación, debe activar la autenticación bidireccional en la configuración del servidor y de Kaspersky Endpoint Security. Para usar autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premise)**.

5. Active el interruptor de **Endpoint Detection and Response Expert (on-premise) HABILITADO**.

6. Para configurar EDR Expert (on-premises), seleccione **Endpoint Detection and Response Expert (versión 8.0 o posterior)** de la lista de soluciones.

7. Configure la conexión de los *servidores de colección de telemetría*:

   a. En el bloque **Conexión a servidores de recopilación de telemetría**, haga clic en el vínculo **Configuración de conexión**.

   b. Configure la conexión de los servidores de colección de telemetría:

      - **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor.

      - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en Open Single Management Platform (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 habilitarla en la configuración del servidor y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Después de configurar el servidor, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña.

        El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

d. Agregue servidores de colección de telemetría. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

   Puede agregar varias direcciones de servidores de colección de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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**, establezca la configuración de **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 a amenazas y envía los resultados de la tarea.

   b. Haga clic en el vínculo **Configuración de conexión**.

   c. Configure la conexión de los servidores de respuesta:

      - **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor.

      - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en Open Single Management Platform (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 habilitarla en la configuración del servidor y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Después de configurar el servidor, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña.

        El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   d. Haga clic en **Aceptar**.

   e. Agregue los servidores de respuesta. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

      Puede agregar varias direcciones de servidores de respuestas. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 íconos de candado y guarde los cambios.

De esta forma, el equipo se agrega a Open Single Management Platform (OSMP). El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (on-premises)** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Compatibilidad con aplicaciones de EPP de terceros

EDR Agent admite la funcionalidad de las soluciones 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 admite trabajar con Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform (EDR) y Kaspersky Anti Targeted Attack Platform (NDR).

EDR Agent es compatible con aplicaciones EPP de los siguientes proveedores:

- **Dr.Web**

  EDR Agent es compatible con el agente Dr.Web para Windows, versión 13.0.1 o una posterior y Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent es compatible con Dallas Lock 8.0-C, versión 11.4.2.843 o posterior.

  > Para que el EDR Agent se ejecute en un equipo que tenga instalado el software Dallas Lock, debe habilitar 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 o posterior.

  > La aplicación no se puede instalar en un equipo en el que 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 Apex One, versión 14.0.12994 o posterior (incluido Security Agent).

  EDR Agent es compatible con Trend Micro Deep Security, versión 20.0.2-4960 o posterior (incluido Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent es compatible con Sophos Intercept X versión 2024.1.2 o posterior (incluido Endpoint Agent) y Sophos Core Agent versión 2024.3.2.3.

- **Bitdefender**

  EDR Agent es compatible con Bitdefender Endpoint Security Tools, versión 7.9.21.523 o posterior.

- **ESET**

  EDR Agent es compatible con ESET Endpoint Security versión 12.0.2049.0 o posterior y ESET Management Agent versión 12.0 o posterior.

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, luego el Agente de red 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 porque su instalador puede volver a analizar el equipo en busca de software incompatible y eliminar las aplicaciones.

Si no pudo 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 usa datos de telemetría recibidos de puntos de conexión y aprendizaje automático. MDR envía los datos de los incidentes a los expertos de Kaspersky. A continuación, los expertos pueden procesar el incidente y, por ejemplo, agregar una nueva entrada a las bases de datos antivirus. Alternativamente, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener más detalles sobre el funcionamiento de la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Configuración de Kaspersky Endpoint Security para la integración con MDR

Se puede utilizar la siguiente configuración para trabajar con MDR:

- **[KES+Agente incorporado]**. En esta configuración, Kaspersky Endpoint Security actúa como la aplicación que garantiza la seguridad del equipo y como la aplicación para trabajar con MDR. El agente incorporado está disponible en Kaspersky Endpoint Security 11.6.0 para Windows o versiones posteriores.

- **[EPP de terceros+EDR Agent]**. En esta configuración, la seguridad de la infraestructura de TI la proporciona la Plataforma de protección de endpoints (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. EDR Agent está disponible en Kaspersky Endpoint Security 12.3 para Windows o posterior.

Compatibilidad con versiones anteriores de Kaspersky Endpoint Security

Kaspersky Endpoint Security es compatible, desde la versión 11, con la solución MDR. Kaspersky Endpoint Security versiones 11-11.5.0 solo envían datos de telemetría a Kaspersky Managed Detection and Response para habilitar la detección de amenazas. Kaspersky Endpoint Security versión 11.6.0 tiene todas las funcionalidades del agente integrado (Kaspersky Endpoint Agent).

Si utiliza Kaspersky Endpoint Security versiones 11-11.5.0, deberá actualizar las bases de datos a las más recientes para trabajar con la solución MDR. También deberá instalar Kaspersky Endpoint Agent.

Si usa Kaspersky Endpoint Security 11.6.0 o posterior, no necesita instalar Kaspersky Endpoint Agent para usar la solución MDR.

> Si la directiva de Kaspersky Endpoint Security también aplica a los equipos que no tengan Kaspersky Endpoint Security 11-11.5.0 instalados, primero debe crear una directiva de Kaspersky Endpoint Agent independiente para esos equipos. En la directiva nueva, configure la integración con Kaspersky Managed Detection and Response.

Integración del agente incorporado con MDR

Para configurar la integración con Kaspersky Managed Detection and Response, debe habilitar 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 nueva conexión 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 el interruptor de **Conexión en segundo plano para la integración Habilitada**.
4. Guarde los cambios.

El proceso de integración con Kaspersky Managed Detection and Response se divide en los siguientes pasos:

1. **Instalación del componente Managed Detection and Response**

   Puede seleccionar el componente MDR durante la instalación o la actualización, además de usar 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 deshabilitar la opción **Comprobar si hay aplicaciones incompatibles de terceros** en la configuración de la tarea.

2. **Configuración de Kaspersky Private Security Network**

Omita este paso si está usando 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). A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky.

En las propiedades del Servidor de administración, cargue el archivo de configuración de Kaspersky Security Network. Encontrará el archivo de configuración de Kaspersky Security Network dentro del archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre cómo configurar Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center. Si lo prefiere, puede cargar el archivo de configuración de Kaspersky Security Network al equipo utilizando la línea de comandos (consulte las instrucciones a continuación).

Cómo configurar Kaspersky Private Security Network mediante la línea de comandos

1. Abra el símbolo del sistema (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 contenga 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 los archivos, las aplicaciones y los sitios web. La sección **Kaspersky Security Network** de la configuración de la directiva mostrará el siguiente estado operativo: *Infraestructura: Kaspersky Private Security Network*.

Debe habilitar el modo KSN extendido para que Managed Detection and Response funcione.

3 Activar Kaspersky Managed Detection and Response

A partir de Kaspersky Endpoint Security 12.10 para Windows, para activar la funcionalidad Managed Detection and Response, además de una código de activación, puede utilizar un archivo de clave.

Kaspersky Managed Detection and Response admite los siguientes métodos de licencia:

- La funcionalidad Managed Detection and Response está incluida en la licencia de Kaspersky Endpoint Security para Windows.

  La funcionalidad está disponible inmediatamente después de activar Kaspersky Endpoint Security para Windows.

- Se utiliza una licencia independiente para MDR (complemento Kaspersky Managed Detection and Response).

  La funcionalidad se vuelve disponible después de agregar una clave diferente para el complemento de Kaspersky Managed Detection and Response. Como resultado, se agregan dos claves en el equipo: una para Kaspersky Endpoint Security y otra para Kaspersky Managed Detection and Response.

  La licencia para la funcionalidad independiente Managed Detection and Response es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad de MDR esté incluida en la licencia y de que esté en funcionamiento en la interfaz local de la aplicación.

4. **Habilitar los componentes de Managed Detection and Response**

Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (consulte las instrucciones más abajo). El archivo BLOB contiene la ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. Encontrará el archivo BLOB en el archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre el archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

A partir de Kaspersky Endpoint Security 12.6 para Windows, la adición de un archivo BLOB es opcional para Kaspersky Managed Detection and Response sin inquilinos si tiene una licencia actual.

Cómo habilitar 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 correspondiente 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 de verificación **Managed Detection and Response (Industrial CyberSecurity)**.
5. En el bloque **Configuración**, haga clic en **Cargar** y seleccione el archivo BLOB que obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tendrá la extensión P7.

   De manera predeterminada, el usuario puede administrar la configuración de la aplicación (el "candado" está abierto). Para aplicar la directiva en los equipos, cierre los candados .

6. Guarde los cambios.

Cómo habilitar 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.
5. Active el interruptor de **Managed Detection and Response HABILITADA**.

6. Haga clic en **Cargar** y seleccione el archivo BLOB que obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tendrá la extensión P7.

> De manera predeterminada, el usuario puede administrar la configuración de la directiva (el "candado" está abierto). Para aplicar la directiva en los equipos, cierre los candados .

7. Guarde los cambios.

Cómo habilitar Managed Detection and Response desde la línea de comandos

1. Abra el símbolo del sistema (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 habilitada. El usuario debe tener el permiso **Configurar la aplicación**.

Como resultado, Kaspersky Endpoint Security verificará el archivo BLOB. Durante la verificación del archivo BLOB, se controlarán la firma digital y el plazo de la licencia. De no ocurrir errores en este proceso, Kaspersky Endpoint Security descargará el archivo y lo enviará al equipo cuando se realice la siguiente sincronización con Kaspersky Security Center. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Managed Detection and Response** se agregará a la lista de componentes de Kaspersky Endpoint Security.

5. **Configuración de otros componentes de la aplicación para recibir telemetría**

Debe habilitar los siguientes componentes para que Managed Detection and Response funcione:

- Kaspersky Security Network (modo ampliado).
- Detección de comportamiento.
- Prevención de exploits.
- Protección contra amenazas web.
- Protección contra amenazas de correo.
- Protección contra archivos peligrosos.
- Protección contra amenazas de red.
- Firewall.
- Protección vía 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 ficha **Configuración de la aplicación**.
  4. Vaya a **Configuración de agentes integrados** → **Managed Detection and Response**.
  5. Active el interruptor de **Managed Detection and Response HABILITADA**.
  6. Guarde los cambios.

  1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Directivas**.
  2. Seleccione la directiva correspondiente 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 de verificación **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 incorporado 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 llevará a cabo todas las funciones de Kaspersky Endpoint Agent.

Cuando despliegue Kaspersky Endpoint Security en computadoras que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Managed Detection and Response seguirá funcionando con Kaspersky Endpoint Security. Además, se eliminará Kaspersky Endpoint Agent del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 11.6.0 o posterior.

> Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar estas dos aplicaciones en el mismo equipo.

Se deben cumplir las siguientes condiciones para que Kaspersky Endpoint Security funcione como parte de Kaspersky Managed Detection and Response:

- Kaspersky Security Center versión 13.2 o posterior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la función 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 a través de 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 incorporado] 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 posterior. Según el tipo de consola de Kaspersky Security Center que esté utilizando, actualice el complemento de administración en la Consola de administración (MMC) o en el complemento web de la Web Console.

2. **Migrar directivas y tareas**

   Transfiera la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows. Las siguientes opciones están disponibles:

   - 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 la tarea y la directiva de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console.

En la ventana principal de Web Console, seleccione **Operaciones** → **Migración de Kaspersky Endpoint Agent**.

Esto ejecuta el Asistente de migración de tareas y directivas. Siga las instrucciones del Asistente.

Paso 1. Migración de la directiva

El Asistente de migración crea una nueva directiva que fusiona la configuración de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuya configuración desee fusionar 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 fusionar la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de la tarea

El Asistente de migración no admite tareas de MDR. Omita este paso.

Paso 3. Fin del Asistente

Salga del Asistente. Al finalizar el asistente, se creará una nueva directiva de Kaspersky Endpoint Security. La directiva fusiona 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 nueva directiva 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 nueva directiva combinada.

- Un Asistente estándar de conversión por lotes de directivas y tareas. 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 de 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 agregar la clave con la tarea *Agregar clave*. Como resultado, se agregarán dos claves a la aplicación: *Kaspersky Endpoint Security* y *Kaspersky Managed Detection and Response*.

4. **Instalar/actualizar la aplicación de Kaspersky Endpoint Security**

   Para migrar la funcionalidad de 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 utilizando los siguientes métodos:

- Mediante el servicio de actualización de Kaspersky.
- De manera 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 usar 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 mediante Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tiene acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes en función de un conjunto de componentes de Kaspersky Endpoint Agent. Después de esto, Kaspersky Endpoint Security pasa a usar el agente incorporado 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**

Luego de la instalación o actualización de la aplicación, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.
- El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de haber activado la funcionalidad de agente incorporado.
- 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 lo sucesivo, también denominada "EDR Optimum"). A partir de la versión 11.8.0, Kaspersky Endpoint Security para Windows incluye un agente incorporado para la solución Kaspersky Endpoint Detection and Response Expert (en lo sucesivo, también denominada "EDR Expert"). *Kaspersky Endpoint Detection and Response* es una variedad de soluciones para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. Las funcionalidades de las soluciones combinan la detección automática de las amenazas con la capacidad para reaccionar a estas amenazas para contrarrestar los 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 antes 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 de amenazas

Kaspersky Endpoint Detection and Response usa las siguientes herramientas de 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 en la 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 los datos de Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan con mayor velocidad a las amenazas, que el rendimiento de algunos componentes de protección aumente y que la posibilidad de encontrarse con falsos positivos disminuya.
- Tecnología Cloud Sandbox que le permite ejecutar archivos detectados en un entorno aislado y comprobar su reputación.

Principio de operación de la solución

Kaspersky Endpoint Detection and Response revisa y analiza el desarrollo de las amenazas y proporciona al *personal de seguridad* o al *Administrador* la información sobre el posible ataque necesaria para una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana independiente. Una *alerta* es un evento en la infraestructura de TI corporativa que la aplicación identificó como inusual o sospechoso y que puede representar una amenaza para la seguridad de la infraestructura de TI corporativa. *Detalles de la alerta* es una herramienta para ver la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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 está usando 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 durante la instalación de 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 incorporado con EDR Optimum/EDR Expert

Para configurar la integración con Kaspersky Endpoint Detection and Response, debe agregar 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 las alertas se movió 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, cuando trabaja con EDR Optimum, necesitará el complemento de administración de Kaspersky Endpoint Security para crear tareas de respuesta ante amenazas y el complemento de administración de EDR para ver los detalles de las alertas.
- El componente Endpoint Detection and Response Optimum incluido en Kaspersky Endpoint Security, es compatible 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 las características están cubiertas por la licencia.
- El componente Endpoint Detection and Response está activado.
- Los componentes de la aplicación de los que depende Endpoint Detection and Response están habilitados y funcionan. Endpoint Detection and Response depende de los siguientes componentes:
  - Protección contra archivos peligrosos.
  - Protección contra amenazas web.
  - Protección contra amenazas de 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, así como mediante la tarea *Cambiar componentes de la aplicación*.

   > Debe reiniciar el equipo para terminar de actualizar la aplicación con los nuevos componentes.

2. **Activar Kaspersky Endpoint Detection and Response**

   Puede comprar una licencia para utilizar 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 está disponible inmediatamente después de activar Kaspersky Endpoint Security para Windows.

   - Compra de una licencia por separado para EDR Optimum o EDR Expert (complemento de Kaspersky Endpoint Detection and Response).

     La funcionalidad se vuelve disponible después de agregar una clave diferente para Kaspersky Endpoint Detection and Response. Como resultado, se agregan 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 de EDR Optimum o EDR Expert esté incluida en la licencia y de que esté 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. **Habilitar los componentes de Endpoint Detection and Response**

   Puede habilitar o deshabilitar el componente en la configuración de directivas de Kaspersky Endpoint Security para Windows.

   Cómo habilitar o deshabilitar el componente Endpoint 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 ficha **Configuración de la aplicación**.
   4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
   5. Active el interruptor de **Endpoint Detection and Response HABILITADO**.
   6. Guarde los cambios.

El componente Kaspersky Endpoint Detection and Response está habilitado. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Optimum** o **Endpoint Detection and Response Expert (cloud)** se agrega a la lista de componentes de Kaspersky Endpoint Security.

4. **Habilitar la transferencia de datos al Servidor de administración**

   Para habilitar todas las funcionalidades de Endpoint Detection and Response, se debe habilitar la transferencia de datos de los siguientes tipos de datos:

   - Datos de archivos en cuarentena.

     Estos datos se requieren para obtener información acerca de los archivos en cuarentena en un equipo a través de Web Console y Cloud Console. Por ejemplo, puede descargar un archivo de la cuarentena para analizarlo en Web Console y Cloud Console.

   - Datos de la cadena de desarrollo de la amenaza.

     Estos datos se requieren para obtener información acerca de las amenazas detectadas en un equipo en Web Console y Cloud Console. Puede ver los detalles de la alerta y llevar a cabo acciones de respuesta en Web Console y Cloud Console.

   Cómo habilitar la transferencia de datos al Servidor de administración 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 ficha **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 vínculo **Configuración avanzada**.
   6. En la ventana que se abre, seleccione las siguientes casillas:
      - **Acerca de los archivos en Cuarentena**.
      - **Acerca de la cadena de desarrollo de la amenaza**.
   7. Para aplicar la directiva a los equipos, cierre los íconos 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 una actividad que indica 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 *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta ante amenazas.

Kaspersky Endpoint Security busca indicadores de compromiso mediante el uso de archivos de IOC. Los *Archivos de IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos de IOC deben cumplir con el estándar OpenIOC.

Modo de ejecución de la tarea de Análisis de IOC

Kaspersky Endpoint Detection and Response le permite crear tareas de análisis de IOC estándar para detectar datos en peligro. *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 el uso de archivos de IOC preparados por el usuario. Si desea agregar un indicador de compromiso de forma manual, lea los requisitos para archivos de IOC.

El archivo que puede descargar haciendo clic en el siguiente vínculo, contiene una tabla con la lista completa de términos IOC del estándar 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 un 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 que contenga una lista de indicadores de compromiso. Puede agregar listas de los siguientes objetos como indicadores de compromiso:

- Hashes de archivos (MD5/SHA256).

  La aplicación elabora un archivo de IOC con un alcance de análisis FileItem/Md5sum o FileItem/Sha256sum.

- Direcciones IP (IPv4 o IPv6).

  La aplicación elabora un archivo de IOC con un alcance de análisis PortItem/RemoteIP.

- Nombres DNS.

  La aplicación elabora un archivo de IOC con un alcance 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 de propiedades de la tarea. Si es necesario, cree la tarea **Análisis de IOC**.

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

4. Vaya a la sección **Análisis de amenazas**.

5. Haga clic en **Redefinir archivos de IOC**.

6. Se abrirá el formulario para crear un archivo de IOC:

   a. En **Fuente de archivos de IOC**, seleccione **Generar a partir de archivo**.

   b. Ingrese el nombre para el archivo de IOC.

   c. Seleccione el archivo TXT que contiene una lista de indicadores de compromiso.

   d. Seleccione el tipo de archivo de IOC: **Nombres de DNS**, **Hashes de archivos**, **Direcciones IP**.

   e. Haga clic en **Generar**.

   Kaspersky Endpoint Security agrega archivos de IOC a la colección IOC. Si es necesario, puede excluir de forma temporal los archivos de IOC del alcance de la tarea.

7. Guarde los cambios.

Crear una tarea de 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 la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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.

- Mediante el Asistente de tareas.

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 de Análisis de IOC:

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar la tarea. Vaya al siguiente paso.

   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 las tareas 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 dicha unidad.

   En el caso de las tareas independientes de análisis de IOC en unidades de red, es necesario seleccionar manualmente la cuenta de usuario que tiene acceso a esta unidad en las propiedades de la tarea.

6. Finalice el asistente.

   La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **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 un resumen de la información sobre el archivo, incluida la lista de indicadores que no aprobaron la verificación. Después de cargar los archivos de IOC, puede editarlos de forma manual en el editor incorporado 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 de IOC que son compatibles con la versión 1.0 de OpenIOC.

    Kaspersky Endpoint Security agrega archivos de IOC a la colección IOC. Si es necesario, puede excluir de forma temporal los archivos de IOC del alcance de la tarea.

    No se recomienda agregar o eliminar archivos de IOC después de ejecutar la tarea. Esto puede hacer que los resultados del análisis de IOC se muestren de manera incorrecta para ejecuciones anteriores de la tarea. Para buscar indicadores de compromiso en archivos IOC nuevos, se recomienda agregar nuevas tareas.

11. Si es necesario, seleccione la casilla **Análisis retrospectivo de IOC**. En el modo *Análisis retrospectivo de IOC* de la tarea *Análisis de IOC*, Kaspersky Endpoint Security analiza los indicadores de vulneración mediante el uso de datos durante un período determinado. Este modo está diseñado para buscar indicadores de compromiso según la telemetría del equipo protegido, como la actividad de la red, los procesos, los archivos y otros tipos de telemetría. Kaspersky Endpoint Security analiza los datos de los registros del sistema operativo y del navegador del equipo. El Análisis retrospectivo de IOC examina los registros de los siguientes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versión 79 o posterior).

12. Configure las acciones al detectar un IOC:

- **Aislar el dispositivo de la red**. Si esta opción está seleccionada, Kaspersky Endpoint Security aísla el equipo de la red para evitar que la amenaza se propague. Puede configurar la duración del aislamiento en Configuración del componente Endpoint Detection and Response.

  Si esta casilla está desactivada, puede aislar el equipo de la red después de ejecutar la tarea de forma manual. 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 de Análisis de IOC**). Kaspersky Endpoint Security también permite administrar configuraciones adicionales de inmediato: Período de deshabilitación del aislamiento de la red y exclusiones del aislamiento de la red.

- **Mover la copia a la Cuarentena, eliminar objeto**. Si esta opción está seleccionada, 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 Cuarentena.

  Si esta casilla está desactivada, puede poner el archivo en cuarentena después de ejecutar la tarea de forma manual. Si la tarea *Análisis de IOC* detecta un archivo que puede poner en riesgo los datos, puede poner este archivo en cuarentena directamente desde los resultados del análisis de IOC (**Configuración de la aplicación** → **Resultados de Análisis de IOC**). Entonces, Kaspersky Endpoint Security inicia el asistente de creación de tareas e incluye los datos del archivo detectado. Solo necesita administrar configuraciones de tareas adicionales, por ejemplo, configurar la programación de tareas.

- **Ejecutar análisis de áreas críticas**. Si esta opción está seleccionada, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del kernel, los procesos en ejecución y los sectores de inicio del disco.

13. Vaya a la sección **Avanzado**.

14. Seleccione los tipos de datos (documentos IOC) que deben analizarse como parte de la tarea.

> Kaspersky Endpoint Security selecciona automáticamente los tipos de datos (documentos de IOC) para la tarea de *Análisis de IOC* de acuerdo con el contenido de los archivos de IOC cargados. No se recomienda anular la selección de los tipos de datos.

Además, puede configurar los alcances del análisis de los siguientes tipos de datos:

- **Archivos: FileItem**. Configure un alcance del análisis de IOC en el equipo mediante el uso de los alcances predefinidos.

  De manera predeterminada, Kaspersky Endpoint Security analiza IOC solo en áreas importantes del equipo, como la carpeta de descargas, el escritorio, la carpeta con archivos temporales del sistema operativo, etc. También se puede agregar manualmente al alcance del análisis.

- **Registros de eventos de Windows: EventLogItem**. Ingrese el período de tiempo en el que se registraron los eventos. También puede seleccionar 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.

- **Registro de Windows: RegistryItem**. Configure el alcance del Análisis de IOC en el registro.

  De forma predeterminada, Kaspersky Endpoint Security analiza un conjunto de claves de registro.

15. En la ventana de propiedades de la tarea, seleccione 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**.

De esta manera, 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 en la sección **Resultados**. Puede ver la información sobre los indicadores de compromiso detectados en las propiedades de la tarea: **Configuración de la aplicación** → **Resultados de Análisis de IOC**. Desde los resultados del Análisis de IOC, también puede poner en cuarentena el archivo detectado o aislar el equipo de la red de forma manual.

Kaspersky Endpoint Security busca duplicados entre los registros creados para el mismo archivo de IOC y, en los resultados de la tarea, solo conserva los registros únicos. Los duplicados son registros del mismo tipo con los mismos valores en todos los campos comparados. La aplicación tampoco puede crear un registro si este 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	• Faltan los valores de los campos FullPath, Md5sum o Sha256sum. • Falta el valor del campo FullPath y hay valores idénticos en los campos Md5sum y Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Falta el valor de al menos uno de los siguientes campos: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Faltan los valores de los campos startTime o PID.

> Es posible que la ventana **Detalles de alerta** muestre los registros RegistryItem que tengan los mismos valores de campos. Dichos registros no son duplicados, ya que los valores del campo Texto, que no se muestran en la interfaz, son diferentes.

> Los resultados del análisis de IOC se mantienen durante 30 días. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

Telemetría extendida de Análisis de IOC

Recomendamos habilitar la telemetría extendida en el equipo para realizar el análisis retrospectivo de IOC. La telemetría extendida mejora la precisión en la detección de IOC, pero utiliza más recursos del equipo.

La telemetría extendida también admite los siguientes términos:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Si la telemetría extendida está deshabilitada, Kaspersky Endpoint Security puede rotar la información sobre los indicadores de vulneración detectados.

Para habilitar la telemetría extendida:

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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la casilla de verificación **Habilitar el registro avanzado de la actividad del sistema**.
6. Guarde los cambios.

Mover el archivo a cuarentena

Al reaccionar a las amenazas, Kaspersky Endpoint Detection and Response puede crear tareas *Poner archivo en 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 Cuarentena solo cuando se integra con la solución 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 *Poner archivo en cuarentena* de las siguientes formas:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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.

- Mediante el Asistente de tareas.

  Debe ingresar la ruta del archivo o el hash (SHA256 o MD5), o la ruta del archivo y 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 riesgo los datos, puede poner este archivo en cuarentena directamente desde los resultados del análisis de IOC (**Configuración de la aplicación** → **Resultados de Análisis de IOC**). Entonces, Kaspersky Endpoint Security inicia el asistente de creación de tareas e incluye los datos del archivo detectado. Solo necesita administrar configuraciones de tareas adicionales, por ejemplo, configurar la programación de tareas.

La tarea *Poner archivo en cuarentena* tiene las siguientes limitaciones:

1. El tamaño del archivo no debe exceder los 100 MB.
2. Los objetos críticos del sistema (SCO) no se pueden poner en cuarentena. Los SCO son archivos que el sistema operativo y la aplicación Kaspersky Endpoint Security para Windows requieren para poder ejecutarse.
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 en cuarentena como resultado de la tarea *Poner archivo en cuarentena*.

Para crear una tarea de Poner archivo en cuarentena:

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Poner archivo en 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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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 la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. En la lista de archivos, haga clic en **Agregar**.

   Se inicia el asistente de adición de archivos.

10. Para agregar el archivo, debe ingresar la ruta completa al archivo o la ruta y el hash de archivo.

    Si el archivo está ubicado en una unidad de red, ingrese la ruta del archivo que comienza con `\\` y no la letra de la unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede recibir un error *No se encuentra el archivo*.

11. En la ventana de propiedades de la tarea, seleccione 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**.

De esta manera, Kaspersky Endpoint Security mueve el archivo a cuarentena.

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 *Poner archivo en cuarentena* puede finalizar con el error *Acceso denegado* si está intentando mover a cuarentena un archivo ejecutable que se está ejecutando actualmente. Cree una tarea de proceso de finalización para el archivo y vuelva a intentarlo.

La tarea *Poner archivo en cuarentena* puede finalizar con el error *No hay suficiente espacio en el almacenamiento en la cuarentena* si se intenta poner en cuarentena un archivo muy grande. Vacíe la cuarentena o aumente el espacio de la cuarentena. A continuación, vuelva a intentarlo.

Puede restaurar un archivo en cuarentena o vaciar la cuarentena mediante Web Console. Puede restaurar objetos localmente en el equipo mediante el uso de 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, el archivo se guarda en Cuarentena. *Cuarentena* es un almacenamiento local especial en el equipo. Puede descargar este archivo de Cuarentena a su equipo a través de Web Console (**Operaciones** → **Almacenamientos** → **Cuarentena**). En equipo del usuario, el archivo permanece en su carpeta original.

El tamaño del archivo no debe exceder los 100 MB.

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 de Obtener archivo:

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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 la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. En la lista de archivos, haga clic en **Agregar**.

   Se inicia el asistente de adición de archivos.

10. Para agregar el archivo, debe ingresar la ruta completa al archivo o la ruta y el hash de archivo.

    > Si el archivo está ubicado en una unidad de red, ingrese la ruta del archivo que comienza con `\\` y no la letra de la unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede recibir un error *No se encuentra el archivo*.

11. En la ventana de propiedades de la tarea, seleccione 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 en Cuarentena en Web Console.

Eliminar archivo

Puede eliminar archivos de forma remota mediante la tarea *Eliminación de archivo*. Por ejemplo, puede eliminar un archivo de forma remota al responder a amenazas.

La tarea *Eliminación de archivo* tiene las siguientes limitaciones:

- System Critical Object (SCO) no se puede eliminar. Los SCO son archivos que el sistema operativo y la aplicación Kaspersky Endpoint Security para Windows requieren para poder ejecutarse.

- 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 de Eliminación de archivo:

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Eliminación de 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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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 la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. En la lista de archivos, haga clic en **Agregar**.

   Se inicia el asistente de adición de archivos.

10. Para agregar el archivo, debe ingresar la ruta completa al archivo o la ruta y el hash de archivo.

    > Si el archivo está ubicado en una unidad de red, ingrese la ruta del archivo que comienza con `\\` y no la letra de la unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede recibir un error *No se encuentra el archivo*.

11. En la ventana de propiedades de la tarea, seleccione 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**.

De esta manera, 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 *Eliminación de archivo* puede finalizar con el error *Acceso denegado o archivo no encontrado* si está intentando eliminar un archivo ejecutable que se está ejecutando actualmente. Cree una tarea de proceso de finalización para el archivo y vuelva a intentarlo.

Inicio de proceso

Puede ejecutar archivos de forma remota mediante la tarea *Inicio de proceso*. Por ejemplo, puede ejecutar de forma remota una utilidad que crea el archivo de configuración del equipo. A continuación, puede usar la tarea *Recibir archivo del dispositivo* 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 de Inicio de proceso:

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Inicio de 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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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 la tarea nueva.

8. Se abre la ventana de propiedades de la tarea.

9. Seleccione la ficha **Configuración de la aplicación**.

10. Ingrese el comando de inicio de proceso.

    Supongamos 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 (de manera predeterminada). La utilidad se ubica en la carpeta `C:\Users\admin\Diagnostic\`. Debe guardar el archivo de configuración en la carpeta `C:\Users\admin\Documents\Configuration`. Ingrese 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, seleccione 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 en la sección **Resultados de la ejecución**.

Terminar proceso

Puede finalizar procesos de forma remota mediante la tarea *Finalizar 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 quiere prohibir la ejecución de un archivo, puede configurar el componente Prevención de la ejecución. Puede prohibir la ejecución de archivos ejecutables, scripts, archivos con formato de Office.

La tarea *Finalizar proceso* tiene las siguientes limitaciones:

- Los procesos de objetos críticos del sistema (SCO) no se pueden finalizar. Los SCO son archivos que el sistema operativo y la aplicación Kaspersky Endpoint Security para Windows requieren para poder ejecutarse.
- 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 de Finalizar proceso:

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

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Finalizar 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**, seleccione el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Ingrese las credenciales de la cuenta del usuario cuyos derechos desea usar 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 la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

8. Seleccione la ficha **Configuración de la aplicación**.

9. Para completar el proceso, debe seleccionar el archivo que desea finalizar. Puede seleccionar un archivo de las siguientes maneras:

   - Ingrese el nombre completo del archivo.
   - Ingrese el hash y la ruta de archivo.
   - Ingrese el PID del proceso (solo para tareas locales).

   > Si el archivo está ubicado en una unidad de red, ingrese la ruta del archivo que comienza con `\\` y no la letra de la unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede recibir un error *No se encuentra el archivo*.

10. En la ventana de propiedades de la tarea, seleccione la pestaña **Programación**.

11. 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.

12. Haga clic en **Guardar**.

13. Active la casilla ubicada junto a la tarea.

14. Haga clic en **Iniciar**.

    De esta manera, Kaspersky Endpoint Security finaliza el proceso en el equipo. Por ejemplo, si se está ejecutando una aplicación GAME e interrumpe 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 en la sección **Resultados**.

Prevención de la ejecución

La prevención de la ejecución permite administrar la ejecución de archivos ejecutables y scripts, así como la apertura de archivos en formato de Office. De este modo, puede, por ejemplo, impedir la ejecución de aplicaciones que considere inseguras. De esta manera, se puede detener la propagación de la amenaza. La prevención de la ejecución es compatible con un conjunto de extensiones de archivos de Office y un conjunto de intérpretes de script.

Regla de prevención de la ejecución

La prevención de la ejecución administra el acceso de los usuarios a los archivos con reglas de prevención de la ejecución. La opción *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 los algoritmos hash MD5 y SHA256.

Puede crear reglas de prevención de la ejecución:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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.

- Mediante el uso de una directiva de grupo o de la configuración de la aplicación local.

  Debe ingresar la ruta del archivo o el hash (SHA256 o MD5), o la ruta del archivo y el hash del archivo.

También puede administrar la prevención de la ejecución localmente mediante el uso de la línea de comandos.

Prevención de la ejecución tiene las siguientes limitaciones:

1. Las reglas de prevención no cubren los archivos en CD o en imágenes ISO. La aplicación no bloquea la ejecución o apertura de estos archivos.

2. Es imposible bloquear el inicio de objetos críticos del sistema (SCO). Los SCO son archivos que el sistema operativo y la aplicación Kaspersky Endpoint Security para Windows requieren para poder ejecutarse.

3. No se recomienda crear más de 5000 reglas de prevención de la ejecución, ya que pueden generar inestabilidad en el sistema.

Modos de reglas de prevención de la ejecución

El componente Prevención de la ejecución puede funcionar de dos modos:

- Solo estadísticas

  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.

- **Activa**

  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 de Kaspersky Security Center.

Administrar la prevención de la ejecución

La configuración de los componentes solo se puede modificar en Web Console.

Para impedir la ejecución:

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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la ficha **Prevención de ejecución**.
6. Active el interruptor de **Prevención de ejecución HABILITADA**.
7. En el bloque **Acción ante operaciones de ejecución o apertura de un objeto prohibido**, seleccione el modo de funcionamiento del componente:

   - **Bloquear y agregar al 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 de Kaspersky Security Center.

   - **Agregar a registros 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. Cree una lista de reglas de prevención de la ejecución:

   a. Haga clic en **Agregar**.

   b. Esto abre una ventana; en esta ventana, ingrese el nombre de la regla de prevención de la ejecución (por ejemplo, *Aplicación A*).

   c. En la lista desplegable **Tipo**, seleccione el objeto que desea bloquear: **Archivo ejecutable**, **Script**, **Documento de Microsoft Office**.

      Si selecciona un tipo de objeto incorrecto, Kaspersky Endpoint Security no bloquea el archivo o el script.

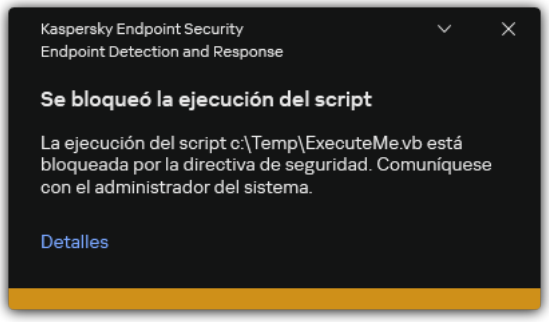
   d. Para agregar el archivo, debe ingresar el hash del archivo (SHA256 o MD5), la ruta completa al archivo, o el hash y la ruta.

      > Si el archivo está ubicado en una unidad de red, ingrese la ruta del archivo que comienza con `\\` y no la letra de la unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de la unidad de la red, Kaspersky Endpoint Security no bloquea el archivo o el script.

      La prevención de la ejecución es compatible con un conjunto de extensiones de archivos de Office y un conjunto de intérpretes de script.

9. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security bloquea la ejecución de objetos: la ejecución de archivos ejecutables y scripts, la apertura de archivos con formato de Office. Sin embargo, puede, por ejemplo, abrir un archivo de script en un editor de texto aunque se impida la ejecución del script. Cuando se bloquea la ejecución de un objeto, Kaspersky Endpoint Security muestra una notificación estándar (vea la figura siguiente) si las notificaciones están activadas en la configuración de la aplicación.



Notificación de la prevención de la ejecución

Aislamiento de la red del equipo

El aislamiento de la red del equipo permite aislar automáticamente un equipo de la red en respuesta a la detección de un indicador de compromiso (IOC): *modo automático*. Puede activar manualmente el aislamiento de la red mientras investiga la amenaza detectada: *modo manual*.

Cuando el aislamiento de la red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones de red TCP/IP nuevas en el equipo, a excepción de las siguientes conexiones.

- Conexiones enumeradas en Exclusiones de aislamiento de la 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 el modo de Light Agent.
- Conexiones a KSN al integrar la aplicación con Kaspersky Managed Detection and Response.

La configuración de los componentes solo se puede modificar en Web Console.

Modo de aislamiento de la red automático

Puede configurar el aislamiento de la red para que se active automáticamente en respuesta a una detección de IOC. Puede configurar el modo de aislamiento de la red automático con una directiva de grupo.

Cómo configurar el aislamiento de la red para que se active automáticamente 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 de propiedades de la tarea.

   Si es necesario, cree la tarea *Análisis de IOC*.

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

4. En el bloque **Acción al detectar un IOC**, seleccione las casillas **Tomar medidas de respuesta después de que se encuentra un IOC** y **Aislar el equipo de la red**.

5. Guarde los cambios.

Como resultado, cuando se detecta un IOC, la aplicación aísla el equipo de la red para evitar que la amenaza se propague.

Puede configurar el Aislamiento de la red automático para que se deshabilite tras un determinado período de tiempo. De forma predeterminada, la aplicación desactiva el aislamiento de la red una vez transcurridas 8 horas desde su activación. También puede desactivar el aislamiento de la red manualmente (consulte las instrucciones a continuación). Después de desactivar el aislamiento de red, el equipo puede utilizar la red sin restricciones.

Cómo configurar la demora en la desactivación del aislamiento de la red de un equipo 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la ficha **Aislamiento de la red**.
6. Seleccione el retraso para desactivar el aislamiento de la red.
7. Guarde los cambios.

Modo de aislamiento de la red manual

Puede activar o desactivar manualmente el aislamiento de la red. Puede configurar el modo de aislamiento de la red manual usando las propiedades del equipo en la consola de Kaspersky Security Center.

Puede activar el aislamiento de la red:

- En detalles de la alerta (solo para EDR Optimum).

  Detalles de la alerta es una herramienta para ver la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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.
- Mediante la configuración local 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 de Análisis de IOC**). Kaspersky Endpoint Security también permite administrar configuraciones adicionales de inmediato: Período de deshabilitación del aislamiento de la red y exclusiones del aislamiento de la red.

Cómo activar manualmente el aislamiento de red de un equipo

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 ficha **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.

5. Seleccione la ficha **Configuración de la aplicación**.

6. Vaya a **Detection and Response** → **Endpoint Detection and Response**.

7. En el bloque **Aislamiento de la red**, haga clic en **Aislar el equipo de la red**.

Puede configurar el Aislamiento de la red automático para que se deshabilite tras un determinado período de tiempo. De forma predeterminada, la aplicación desactiva el aislamiento de la red una vez transcurridas 8 horas desde su activación. Después de desactivar el aislamiento de red, el equipo puede utilizar la red sin restricciones.

Cómo configurar la demora en la desactivación del aislamiento de la 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 ficha **Tareas**.

   Esto muestra la lista de tareas disponibles en el equipo.

4. Seleccione la tarea **Aislamiento de la red**.

5. Seleccione la ficha **Configuración de la aplicación**.

6. En la ventana que se abre, seleccione la demora para desactivar el aislamiento de la red.

7. Guarde los cambios.

Cómo desactivar manualmente el aislamiento de red de un equipo

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 ficha **Aplicaciones**.

4. Haga clic en **Kaspersky Endpoint Security para Windows**.

   Se abre la configuración local de la aplicación.

5. Seleccione la ficha **Configuración de la aplicación**.

6. Vaya a **Detection and Response** → **Endpoint Detection and Response**.

7. En el bloque **Aislamiento de la red**, haga clic en **Desbloquear el equipo aislado de la red**.

También puede deshabilitar el aislamiento de la red localmente mediante el uso de la línea de comandos.

A partir de Kaspersky Endpoint Security 12.10 para Windows, puede administrar el aislamiento de la red desde los detalles de la alerta. Además, en los detalles de la alerta, puede especificar el período del 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 la red

Puede configurar las exclusiones de aislamiento de la red. Las conexiones de red que coinciden con las reglas no se bloquean en el equipo cuando el aislamiento de la red está activado.

Para configurar las exclusiones de aislamiento de la red, puede utilizar una lista de *perfiles de la red estándar*. De forma predeterminada, las exclusiones incluyen perfiles de red que contienen reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles del cliente DNS/DHCP. También puede modificar la configuración de los perfiles de la red estándar o definir las exclusiones manualmente (vea las instrucciones más abajo).

Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de la 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 la 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 impide aplicar las exclusiones del aislamiento de la red configurado en las propiedades del equipo porque estos parámetros tienen situaciones de uso diferentes.

Cómo agregar una exclusión de aislamiento de la 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la ficha **Aislamiento de la red**.
6. En el bloque **Exclusiones de aislamiento de la red**, haga clic en **<N> exclusiones**.
7. Esto abre una ventana. En la ventana, haga clic en **Agregar** → **Agregar del perfil** y seleccione los perfiles de la red estándar para configurar las exclusiones.

   Las exclusiones de aislamiento de la red del perfil se agregan a la lista de exclusiones de aislamiento de la red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de la conexión de la red.
8. Si es necesario, agregue una exclusión de aislamiento de la red manualmente. Para hacerlo, en la ventana con la lista de exclusiones, haga clic en **Agregar** → **Agregar** y modifique de forma manual la configuración de la conexión de la red.
9. Guarde los cambios.

Cómo agregar una exclusión de aislamiento de la 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 ficha **Tareas**.

   Esto muestra la lista de tareas disponibles en el equipo.
4. Seleccione la tarea **Aislamiento de la red**.
5. Seleccione la ficha **Configuración de la aplicación**.
6. En la ventana que se abre, haga clic en **Exclusiones**.
7. Esto abre una ventana; en esta ventana, haga clic en **Agregar del perfil** y seleccione los perfiles de la red estándar para configurar las exclusiones.

   Las exclusiones de aislamiento de la red del perfil se agregan a la lista de exclusiones de aislamiento de la red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de la conexión de la red.
8. Si es necesario, agregue una exclusión de aislamiento de la red manualmente. Para hacerlo, en la ventana con la lista de exclusiones, haga clic en **Agregar** y modifique manualmente la configuración de la conexión de la red.
9. Guarde los cambios.

También puede ver la lista de exclusiones de aislamiento de la red localmente mediante el uso de 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 exclusiones de aislamiento de la red desde 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.

Cloud Sandbox

Cloud Sandbox es una tecnología que le permite detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Cloud Sandbox para su análisis. Cloud Sandbox ejecuta estos archivos en un entorno aislado para identificar actividades maliciosas y decide sobre su reputación. Luego, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Cloud Sandbox detectó un archivo malicioso, Kaspersky Endpoint Security realiza la acción adecuada para eliminar esta amenaza en todos los equipos donde se detecte este archivo.

Para que Cloud Sandbox funcione, debe habilitar el uso de Kaspersky Security Network.

Si está utilizando Kaspersky Private Security Network, la tecnología Cloud Sandbox no está disponible.

La tecnología Cloud Sandbox está habilitada de forma permanente y está disponible para todos los usuarios de Kaspersky Security Network, independientemente del tipo de licencia que utilicen. Si ya implementó la solución Endpoint Detection and Response Optimum, puede habilitar un contador independiente para las amenazas que detecte Cloud Sandbox. Puede utilizar este contador para recopilar estadísticas al analizar las amenazas detectadas. Kaspersky Endpoint Security indica la tecnología de detección de amenazas Cloud Sandbox en *Informe de amenazas* en la consola de Kaspersky Security Center.

Contadores de amenazas

Para habilitar el contador de Cloud Sandbox, realice 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la ficha **Cloud Sandbox**.
6. Active el interruptor de **Cloud Sandbox HABILITADO**.
7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Siempre que hay una amenaza, Kaspersky Endpoint Security activa el contador de amenazas detectadas mediante Cloud Sandbox en la ventana principal de la aplicación, en **Tecnologías de detección de amenazas**. Kaspersky Endpoint Security también indicará la tecnología de detección de amenazas Cloud Sandbox en *Informe de amenazas* en la consola de Kaspersky Security Center.

Guía de migración de KEA a KES para EDR Optimum

Kaspersky Endpoint Security para Windows incluye un agente incorporado 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 llevará a cabo todas las funciones de Kaspersky Endpoint Agent.

Cuando despliegue Kaspersky Endpoint Security en computadoras que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Endpoint Detection and Response Optimum seguirá funcionando con Kaspersky Endpoint Security. Además, se eliminará Kaspersky Endpoint Agent del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 11.7.0 o posterior.

Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar estas dos 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 versión 2.0 o superior.
- Kaspersky Security Center versión 13.2 o posterior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la función de EDR Optimum.
- EDR Optimum solo se puede administrar mediante Kaspersky Security Center Web Console.
- La transferencia de datos al Servidor de administración está habilitada. Estos 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 funcione con el Servidor de administración a través de 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 incorporado] para EDR Optimum

1. **Actualizar el complemento web de Kaspersky Endpoint Security**

   El componente EDR Optimum se puede administrar con el complemento web de Kaspersky Endpoint Security, versión 11.7.0 o posterior.

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 migrar desde Kaspersky Endpoint Agent en Web Console.

   Cómo migrar la configuración de la tarea y la directiva de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console.

   En la ventana principal de Web Console, seleccione **Operaciones** → **Migración de Kaspersky Endpoint Agent**.

Esto ejecuta el Asistente de migración de tareas y directivas. Siga las instrucciones del Asistente.

Paso 1. Migración de la directiva

El Asistente de migración crea una nueva directiva que fusiona la configuración de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuya configuración desee fusionar 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 fusionar la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de la tarea

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desea crear para la directiva de Kaspersky Endpoint Security. Vaya al siguiente paso.

Paso 3. Fin del Asistente

Salga del Asistente. Como resultado, el asistente hace lo siguiente:

- Cree una nueva directiva de Kaspersky Endpoint Security.

  La directiva fusiona 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 nueva directiva 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 nueva directiva combinada.

  > Luego de realizar la migración de Kaspersky Endpoint Agent a 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.

- Cree nuevas tareas 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 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 automáticamente luego de actualizar la aplicación a la versión 11.7.0 o posterior. 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 agregue al repositorio de Kaspersky Security Center y de que la funcionalidad de distribución automática de claves de licencia esté habilitada. Luego de actualizar la aplicación a la versión 11.7.0 o posterior, la funcionalidad EDR Optimum se activa automáticamente.

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 *Agregar clave*.

4. **Instalar/actualizar la aplicación de Kaspersky Endpoint Security**

Para migrar la funcionalidad de 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 utilizando los siguientes métodos:

- Mediante el servicio de actualización de Kaspersky.
- De manera 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 usar 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 mediante Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tiene 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. Después de esto, Kaspersky Endpoint Security pasa a usar el agente incorporado 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**

Luego de la instalación o actualización de la aplicación, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.
- El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de haber activado la funcionalidad de agente incorporado.
- 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 incluye un agente incorporado para la integración con la solución 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 los objetos en servidores especiales con imágenes virtuales implementadas de los sistemas operativos Microsoft Windows (servidores de Sandbox). Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Sandbox y la Ayuda de Kaspersky Anti Targeted Attack Platform.

Integración del agente incorporado con Kaspersky Sandbox

Es necesario agregar el componente Sandbox para la integración con Kaspersky Sandbox. Puede seleccionar el componente Sandbox durante la instalación o la actualización, además de usar la tarea *Cambiar componentes de la aplicación*.

Para usar el componente, se deben cumplir las siguientes condiciones:

- Kaspersky Security Center 13.2. Las versiones anteriores de Kaspersky Security Center no permiten la creación de tareas independientes de análisis de IOC para la respuesta ante amenazas.
- El componente se puede administrar solo mediante el uso de Web Console. No puede administrar este componente mediante el uso de la Consola de administración (MMC).
- La aplicación está activada y las características están cubiertas por la licencia.
- La transferencia de datos al Servidor de administración está habilitada.

  Para utilizar todas las funciones de Kaspersky Sandbox, asegúrese de que la transferencia de datos de archivos en cuarentena esté habilitada. Estos 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 de la cuarentena para analizarlo en Web Console.

  Cómo habilitar 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 ficha **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 **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 funcione con el Servidor de administración a través de Kaspersky Security Center Web Console, debe establecer una nueva conexión segura, una *conexión en segundo plano*. Para obtener más información sobre 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 el interruptor de **Conexión en segundo plano para la integración Habilitada**.
4. Guarde los cambios.

Si no se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de Administración, no se pueden crear tareas de análisis de IOC independientes como parte de la Respuesta ante amenazas.

- Para configurar una conexión de confianza con el servidor de Sandbox, tiene que preparar un certificado TLS. Luego, debe agregar el certificado al equipo mediante una directiva. Además, debe agregar el certificado al servidor Sandbox.

  La autenticación bidireccional mediante un contenedor criptográfico no está disponible para Kaspersky Sandbox.

  Puede agregar un certificado TLS en Web Console o de manera local mediante el uso de la línea de comandos.

- El componente Kaspersky Sandbox está habilitado.
- Los componentes de la aplicación que garantizan el funcionamiento de Sandbox están habilitados y funcionan. Los siguientes componentes garantizan el funcionamiento de Sandbox:
  - Protección contra archivos peligrosos.
  - Prevención de intrusiones en el host.
  - Firewall.
  - Protección vía AMSI.
  - Análisis en segundo plano.

Para habilitar o deshabilitar la integración con Kaspersky Sandbox:

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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Sandbox**.
5. Use el interruptor **Integración con Sandbox HABILITADA** para habilitar o deshabilitar el componente.

6. En el bloque **Modo de integración**, seleccione el modo de funcionamiento del componente: **Kaspersky Sandbox**.

7. Haga clic en el vínculo **Configuración de conexión**.

   Se 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 agregó un certificado TLS anteriormente, ese certificado se revoca. Solo se utiliza el último certificado agregado.

9. Establezca la configuración avanzada de las conexiones para los servidores de Sandbox:

   - **Tiempo de espera (ms)**. Tiempo de conexión agotado para el servidor de Sandbox. Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de conexión agotado para el 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 solicitudes**. 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 la cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Sandbox deja de agregar 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 de Sandbox**, haga clic en el botón **Agregar**.

11. Se abre una ventana. En la ventana, ingrese la dirección del servidor de Sandbox (IPv4, IPv6, DNS) y el puerto.

    Para obtener más información sobre el despliegue 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. De no ocurrir errores en este proceso, Kaspersky Endpoint Security carga el archivo del certificado en el equipo cuando se realiza la siguiente sincronización con Kaspersky Security Center. Si agregó dos certificados TLS, Kaspersky Sandbox utilizará el último certificado agregado para establecer una conexión de confianza. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Sandbox** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Puede habilitar o deshabilitar la integración con Kaspersky Sandbox en Web Console o de manera local mediante 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 obtiene un error con una descripción que se ajusta al formato `Error code: XXX` (por ejemplo, `0xa67b01f4`), comuníquese con el Servicio de 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 una actividad que indica 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 *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta ante amenazas.

Kaspersky Endpoint Security busca indicadores de compromiso mediante el uso de archivos de IOC. Los *Archivos de IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos de IOC deben cumplir con el estándar OpenIOC. Kaspersky Endpoint Security genera automáticamente archivos de IOC para Kaspersky Sandbox.

Modo de ejecución de la tarea de Análisis de IOC

La aplicación crea tareas de análisis de IOC independientes para Kaspersky Sandbox. *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. No se admiten archivos de IOC personalizados. Las tareas se eliminan automáticamente 30 días después de la hora de creación. Para obtener más información 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 ajustar la configuración solo en Web Console.

Debe contar con 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 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 de propiedades de la tarea.

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

4. Vaya a la sección **Configuración de Análisis de IOC**.

5. Configure las acciones al detectar un IOC:

- **Mover la copia a la Cuarentena, eliminar objeto**. Si esta opción está seleccionada, 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 Cuarentena.

- **Ejecutar análisis de áreas críticas**. Si esta opción está seleccionada, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del kernel, los procesos en ejecución y los sectores de inicio del disco.

- **Ejecutar solo cuando el equipo esté inactivo**. Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. Si interrumpió la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta automáticamente la tarea, y continúa desde el punto donde se interrumpió. Esta opción de programación le permite conservar los recursos del equipo cuando el equipo está en uso.

6. Guarde los cambios.

Puede ver los resultados de la tarea en las propiedades de la tarea en la sección **Resultados**. Puede ver la información sobre los indicadores de compromiso detectados en las propiedades de la tarea: **Configuración de la aplicación** → **Resultados de Análisis de IOC**.

Los resultados del análisis de IOC se mantienen durante 30 días. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

Guía de migración de KEA a KES para Kaspersky Sandbox

Kaspersky Endpoint Security para Windows incluye un agente incorporado para la solución Kaspersky Sandbox. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con Kaspersky Sandbox. Kaspersky Endpoint Security llevará a cabo todas las funciones de Kaspersky Endpoint Agent.

Cuando despliegue Kaspersky Endpoint Security en equipos que tienen Kaspersky Endpoint Agent instalado, la solución Kaspersky Sandbox seguirá funcionando con Kaspersky Endpoint Security. Además, se eliminará Kaspersky Endpoint Agent del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 11.7.0 o posterior.

Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar estas dos 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 posterior.

- Kaspersky Security Center versión 13.2 o posterior (incluido el Agente de red). En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Kaspersky Sandbox.

- Kaspersky Sandbox se puede administrar solo mediante el uso de Kaspersky Security Center Web Console.

- La transferencia de datos al Servidor de administración está habilitada. Estos 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 funcione con el Servidor de administración a través de 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 incorporado] 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 posterior.

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 migrar desde Kaspersky Endpoint Agent en Web Console.

   Cómo migrar la configuración de la tarea y la directiva de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console.

   En la ventana principal de Web Console, seleccione **Operaciones** → **Migración de Kaspersky Endpoint Agent**.

   Esto ejecuta el Asistente de migración de tareas y directivas. Siga las instrucciones del Asistente.

Paso 1. Migración de la directiva

El Asistente de migración crea una nueva directiva que fusiona la configuración de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuya configuración desee fusionar 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 fusionar la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

Paso 2. Migración de la tarea

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desea crear para la directiva de Kaspersky Endpoint Security. Vaya al siguiente paso.

Paso 3. Fin del Asistente

Salga del Asistente. Como resultado, el asistente hace lo siguiente:

- Cree una nueva directiva de Kaspersky Endpoint Security.

La directiva fusiona 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 nueva directiva 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 nueva directiva combinada.

Luego de realizar la migración de Kaspersky Endpoint Agent a 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.

- Cree nuevas tareas 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 de Kaspersky Sandbox. Puede agregar la clave con la tarea *Agregar clave*. Como resultado, se agregarán dos claves a la aplicación: *Kaspersky Endpoint Security* y *Kaspersky Sandbox*.

4. **Instalar/actualizar la aplicación de 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 utilizando los siguientes métodos:

   - Mediante el servicio de actualización de Kaspersky.
   - De manera 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 usar 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 mediante Kaspersky Security Center.

   Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tiene 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. Después de esto, Kaspersky Endpoint Security pasa a usar el agente incorporado 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**

Luego de la instalación o actualización de la aplicación, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.
- El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de haber activado la funcionalidad de agente incorporado.
- 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 admite trabajar con la solución Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* es una solución que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. 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 adquirir todas las unidades funcionales o las unidades funcionales individuales por separado. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform. La aplicación incluye agentes incorporados para los componentes EDR y NDR. La aplicación también admite trabajar con el componente de Sandbox, que forma parte de KATA.

Herramientas de inteligencia de amenazas

Kaspersky Endpoint Detection and Response usa las siguientes herramientas de 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 en la 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 los datos de Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan con mayor velocidad a las amenazas, que el rendimiento de algunos componentes de protección aumente y que la posibilidad de encontrarse con falsos positivos disminuya.

Principio de operación de la solución

La aplicación Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y monitorea de forma continua los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos del 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. Luego, el agente incorporado se administra mediante la consola de Kaspersky Anti Targeted Attack Platform, incluidas las tareas en ejecución, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Configuración de Kaspersky Endpoint Security para trabajar con EDR / NDR (KATA)

Se puede utilizar la siguiente configuración para trabajar con EDR / NDR (KATA):

- **[KES+Agente incorporado]**. 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 incorporado para EDR (KATA) está disponible en Kaspersky Endpoint Security 12.1 para Windows o versiones posteriores. El agente incorporado para NDR (KATA) está disponible en Kaspersky Endpoint Security 12.7 para Windows o versiones posteriores.

- **[EPP de terceros+EDR Agent]**. En esta configuración, la seguridad de la infraestructura de TI la proporciona la Plataforma de protección de endpoints (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 está usando 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 durante la instalación de Kaspersky Endpoint Security.

Si está usando Kaspersky Endpoint Security 11.9.0 - 12.0, debe instalar Kaspersky Endpoint Agent por separado ya que, 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 incorporado con EDR / NDR (KATA)

Para la integración con EDR/NDR (KATA), debe agregar el componente relevante: Endpoint Detection and Response (KATA) o Network Detection and Response (KATA). Puede seleccionar los componentes para la integración con EDR/NDR (KATA) durante la instalación o la actualización de la aplicación, además de usar la tarea *Cambiar componentes de la aplicación*.

A partir de la versión 12.11 de Kaspersky Endpoint Security para Windows, el componente EDR (KATA) pasó a llamarse **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, y 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 usar 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 posterior.
- EDR (KATA): Kaspersky Endpoint Security para Windows 12.1 o posterior. Para obtener más información 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 con EDR/NDR (KATA).
- La aplicación está activada y las características están cubiertas por la licencia.
- Los componentes Endpoint Detection and Response (KATA) y Network Detection and Response (KATA) están habilitados.
- Los componentes de la aplicación que garantizan el funcionamiento de EDR/NDR (KATA) están habilitados y funcionan. Los siguientes componentes garantizan la operación de EDR / NDR (KATA):
  - Protección contra archivos peligrosos.
  - Protección contra amenazas web.
  - Protección contra amenazas de correo.
  - Prevención de exploits.
  - Detección de comportamiento.
  - Prevención de intrusiones en el host.

- Protección vía AMSI.
- Análisis en segundo plano.
- Kaspersky Security Network.

https://www.youtube.com/watch?v=cZzgtBoeC7k

https://www.youtube.com/watch?v=gd-rySv0ThQ

El proceso de integración con Endpoint Detection and Response (KATA) incluye los siguientes pasos:

1. **Instalar 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 mejora, además de usar la tarea *Cambiar componentes de la aplicación*.

   Debe reiniciar el equipo para terminar de actualizar la aplicación con los nuevos componentes.

2. **Activar Endpoint Detection and Response (KATA) y Network Detection and Response (KATA)**

   Tiene que comprar una licencia por separado para EDR (KATA) y NDR (KATA) (por ejemplo, complemento de Kaspersky Endpoint Detection and Response [KATA]).

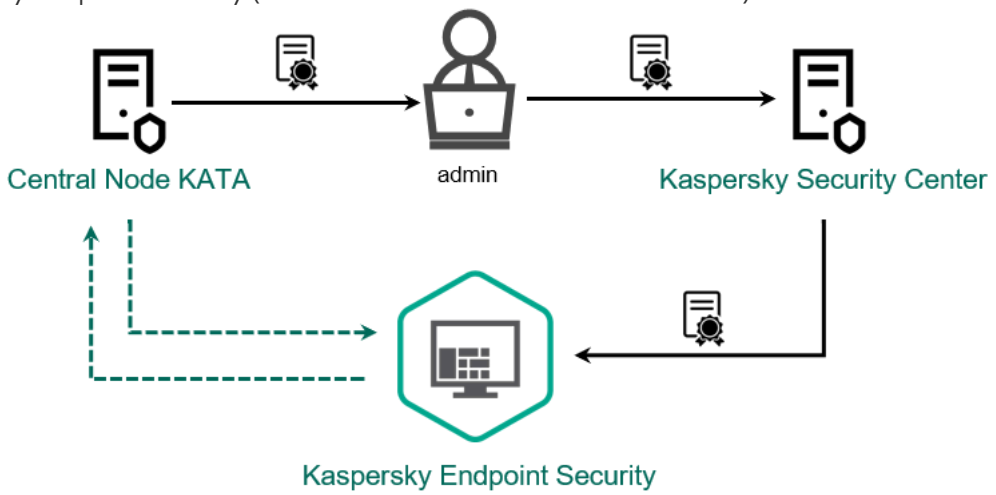
   La funcionalidad estará disponible después de agregar una clave separada que cubre la funcionalidad EDR (KATA) y NDR (KATA). Como resultado, se agregan varias claves en el equipo: una para Kaspersky Endpoint Detection and Response (KATA) y Network Detection and Response (KATA).

   La licencia para la funcionalidad independiente de EDR (KATA) y NDR (KATA) es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad de EDR (KATA) y NDR (KATA) esté incluida en la licencia y de que esté en ejecución en la interfaz local de la aplicación.

3 Conexión a Central Node

Kaspersky Anti Targeted Attack Platform exige 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). Luego, 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 habilitar esta verificación, debe activar la autenticación bidireccional en la configuración de Central Node y Kaspersky Endpoint Security. Para usar autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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 a 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 correspondiente 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 del servidor**.

7. Configure la conexión del servidor:

   - **Tiempo de espera (s)**. 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).

   - **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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

8. Haga clic en **Aceptar**.

9. Agregue servidores de Central Node. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

   Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 íconos de candado y guarde los cambios.

Cómo conectar un equipo con Kaspersky Endpoint Security a 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 ficha **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-premise)** o **Network Detection and Response (KATA)**.

5. Active el interruptor correspondiente: **Endpoint Detection and Response Expert (on-premise) HABILITADO** o **Network Detection and Response (KATA) HABILITADO**.

6. Para configurar EDR (KATA), seleccione **Endpoint Detection and Response Expert (versión 7.1 o anterior)** de la lista de soluciones.

7. Haga clic en **Configuración de conexión**.

8. Configure la conexión del servidor:

   - **Tiempo de espera (s)**. 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

     El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

9. Haga clic en **Aceptar**.

10. Agregue servidores de Central Node. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

    Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 íconos de candado y guarde los cambios.

Puede agregar un certificado TLS de manera local mediante el uso de la línea de comandos.

Como resultado, se agrega el equipo a la consola de Kaspersky Anti Targeted Attack Platform. El estado de funcionamiento de los componentes aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de componentes, también puede consultar los informes disponibles en 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 agregarás a la lista de componentes de Kaspersky Endpoint Security.

Puede verificar 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 se instaló y la licencia no cubre la funcionalidad, la consola muestra el estado **No compatible con la licencia** en lugar de **Sin instalar**.

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 Sensor de Endpoint** (*En ejecución*, *Iniciándose*, *Detenida*, *En pausa*, *Error* o *Desconocido*). Web Console no muestra el estado de Endpoint Sensor.

Configuración de la telemetría de EDR (KATA)

Telemetría es una lista de eventos que ocurrieron 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 casi continuamente. Kaspersky Endpoint Security inicia la sincronización con el servidor cuando se cumple alguna de las siguientes condiciones:

- Se ha agotado el intervalo de sincronización.
- La cantidad de eventos en el búfer supera 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 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 restaura 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 esto, puede optimizar la configuración de transmisión de eventos, por ejemplo, para establecer un valor máximo de eventos por hora (consulte las instrucciones a continuación).

Si está usando Kaspersky Anti Targeted Attack Platform junto con otra solución que también usa telemetría, puede desactivar la telemetría para KATA (EDR) (consulte las instrucciones a continuación). Esto le permite optimizar la carga del servidor para estas soluciones. Por ejemplo, si tiene implementada la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Respuesta ante amenazas 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 correspondiente 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 la opción **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 las tareas y la configuración de la aplicación modificada.
6. Asegúrese de que la casilla de verificación **Enviar telemetría a KATA** esté seleccionada.

7. De ser necesario, ajuste la sincronización a la configuración del sistema en el bloque **Configuración de la transmisión de datos**:

   - **Retraso máximo de transmisión de eventos (s)**. La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos.

   - **Cantidad máxima de eventos por paquete**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. La configuración predeterminada es de 1024 eventos.

8. Si es necesario, seleccione la casilla **Habilitar regulación de solicitudes** en el bloque **Regulación de solicitudes**.

   Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, 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:

   - **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada es 15 %.

10. Para aplicar la directiva a los equipos, cierre los íconos 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premise)**.

5. Para configurar EDR (KATA), seleccione **Endpoint Detection and Response Expert (versión 7.1 o anterior)** de 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 la transmisión de datos**.

7. Configure la opción **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 las tareas y la configuración de la aplicación modificada.

8. Asegúrese de que la casilla de verificación **Enviar telemetría a servidores de KATA** esté seleccionada.

9. De ser necesario, ajuste la sincronización a la configuración del sistema en el bloque **Configuración de la transmisión de datos**:

   - **Retraso máximo de transmisión de eventos (s)**. La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos.

   - **Cantidad máxima de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. La configuración predeterminada es de 1024 eventos.

10. Si es necesario, seleccione la casilla **Habilitar regulación de solicitudes** en el bloque **Regulación de solicitudes**.

    Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, 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:

    - **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada es 15 %.

12. Para aplicar la directiva a los equipos, cierre los íconos 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 ficha **Configuración de la aplicación**.

4. Vaya a la sección **Integración KATA** → **Exclusiones de telemetría**.

5. En **Configuración de la transmisión de datos**, seleccione la casilla de verificación **Usar exclusiones**.

6. Haga clic en **Agregar** y configure las exclusiones:

Los criterios se combinan con la lógica *Y*.

- **Ruta**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara. Para que la exclusión funcione, se debe especificar la ruta de acceso al archivo.
- **Línea de comandos**. Comando utilizado para ejecutar el objeto.
- **Descripción**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo).

  Para 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**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

1. Seleccione **Kaspersky Endpoint Security para Windows (14.1)** → **Reversión de la actualización**.

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

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- 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 no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 3. Programación de la tarea

Configure la programación de la tarea, por ejemplo, manualmente.

Paso 4. Nombre de la tarea

Ingrese un nombre para la tarea.

Paso 7. Completar creación de la tarea

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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 optar por no enviar datos de comunicaciones de red para 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 correspondiente 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 objetos**.
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 **Uso para los siguientes tipos de eventos**.
6. Guarde los cambios.

Cómo crear una exclusión de telemetría con 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de telemetría**.

5. Seleccione la ficha **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 que se enviará**. Kaspersky Endpoint Security permite optimizar la cantidad de datos transmitidos y excluir de la telemetría eventos con ciertos códigos: 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 los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo. **Uso para los siguientes tipos de eventos**: • **Modificación de archivos**. • **Eventos de red**. • **Proceso: entrada interactiva de la consola**. • **Módulo cargado**. • **Registro modificado**. • **Registros DNS**. • **Acceso al proceso**. • **Infiltración de código**. • **Consulta WMI**. • **Tubería**. • **LDAP**. • **AMSI**.

Parámetro	Descripción
Comunicaciones de red excluidas	**Nombre de la regla**. **Sentido**. **Protocolo**. **Socket de tipo raw**. **Número de protocolo**. **Certificado TLS**. **Puerto o intervalo local**. **Puerto o intervalo 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.
Operaciones de archivos excluidas	**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 ingresar una máscara. **Tipo de operación**. **Ruta anterior**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.

Parámetro	Descripción
Operaciones DNS excluidas	**Nombre de la regla**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a 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**.
Operaciones LDAP excluidas	**Nombre de la regla**. **Alcance de la búsqueda de LDAP**. **Filtro**. **Nombre diferenciado para la búsqueda de objetos LDAP**. **Atributos de objeto**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.

Parámetro	Descripción
Consultas de acceso a procesos excluidas	**Nombre de la regla**. **Tipo de operación**. **Acceso solicitado al proceso**. **Rastreo de la pila de llamadas**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso**, **Proceso principal**, **Archivo del proceso de destino**, **Identificador de proceso de origen** y **Identificador de proceso de destino**. • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara. • **Texto de la línea de comandos**. Comando utilizado para ejecutar el archivo. • **Especifique los criterios de activación de la regla y los tipos de eventos en los que se usará esta regla**. Valor del parámetro FileDescription de un recurso RT_VERSION (VersionInfo). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.
Inyecciones de código excluidas	**Nombre de la regla**. **Método de acceso**. **Pila de llamadas**. **Línea de comandos modificada**. **Dirección de inyección**. **Nombre del DLL inyectado**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.

Parámetro	Descripción
Consultas WMI excluidas	**Nombre de la regla**. **Tipo de operación WMI**. **Consulta remota**. **Nombre de un equipo que ejecutó un comando WMI**. **Cuenta de usuario WMI**. **Comando WMI ejecutado**. **Espacio de nombres WMI**. **Filtro de consumidores de eventos WMI**. **Nombre del consumidor de eventos WMI creado**. **Código fuente de un consumidor de eventos WMI**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.
Operaciones de tuberías excluidas	**Nombre de la regla**. **Nombre de la tubería**. **Tipo de operación**. Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.

Parámetro	Descripción
Cambios del 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 los criterios de activación de la regla con un operador lógico AND. **Proceso** y **Proceso principal**: • **Ruta completa**. Ruta completa de acceso al archivo que incluye su nombre y extensión. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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). • **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). • **Sumas de comprobación de archivos**. MD5 y SHA256. También puede seleccionar un archivo manualmente y la aplicación completará de manera automática 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`, ya que 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 mostrará los parámetros de `C:\windows\syswow64\cmd.exe`. Ese comportamiento se debe a peculiaridades del sistema operativo.
Operaciones excluidas para dispositivos	**Nombre de la regla**. **Tipo de dispositivo**. **Id. del dispositivo**. **Nombre del dispositivo**.

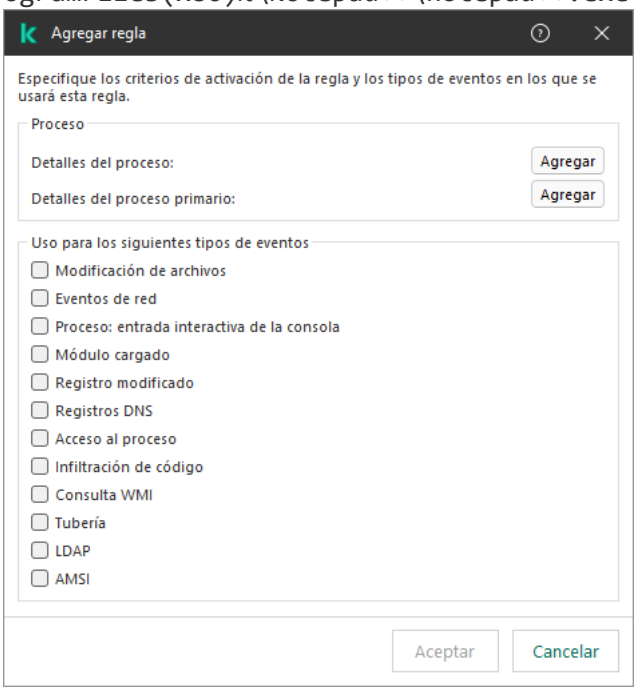
Ejemplo 1. Procesos excluidos

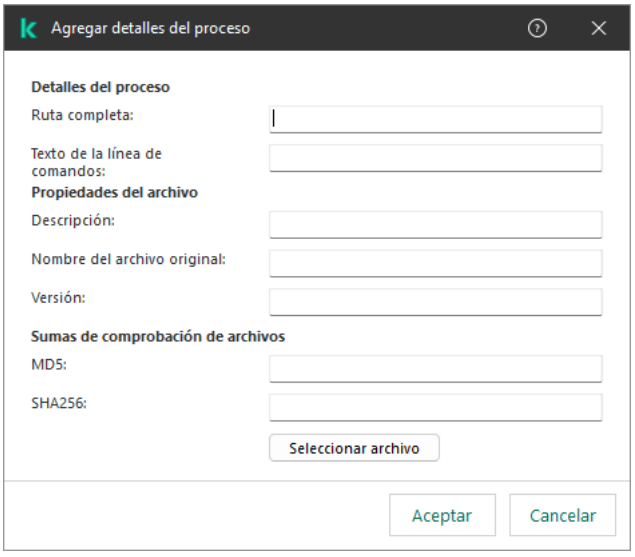
Para excluir eventos (procesos) de aplicaciones de terceros de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Procesos excluidos** y agregue el archivo ejecutable de la aplicación.

Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND.

Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara. Por ejemplo:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`





Exclusión de un proceso

Ejemplo 1. Modificación de archivos

Si edita scripts con frecuencia en la aplicación Notepad++ y desea excluir los eventos de modificación para los scripts correspondientes, agregue el archivo ejecutable Notepad++ a las exclusiones de telemetría.

Especifique la configuración de la siguiente manera:

- **Ruta completa**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Uso para los siguientes tipos de eventos**: Modificación de archivos.

Ejemplo 2. Eventos de red

Si usa la aplicación WinSCP para administrar archivos en un servidor remoto y desea excluir eventos de red, agregue el archivo ejecutable WinSCP a las exclusiones de telemetría.

Especifique la configuración de la siguiente manera:

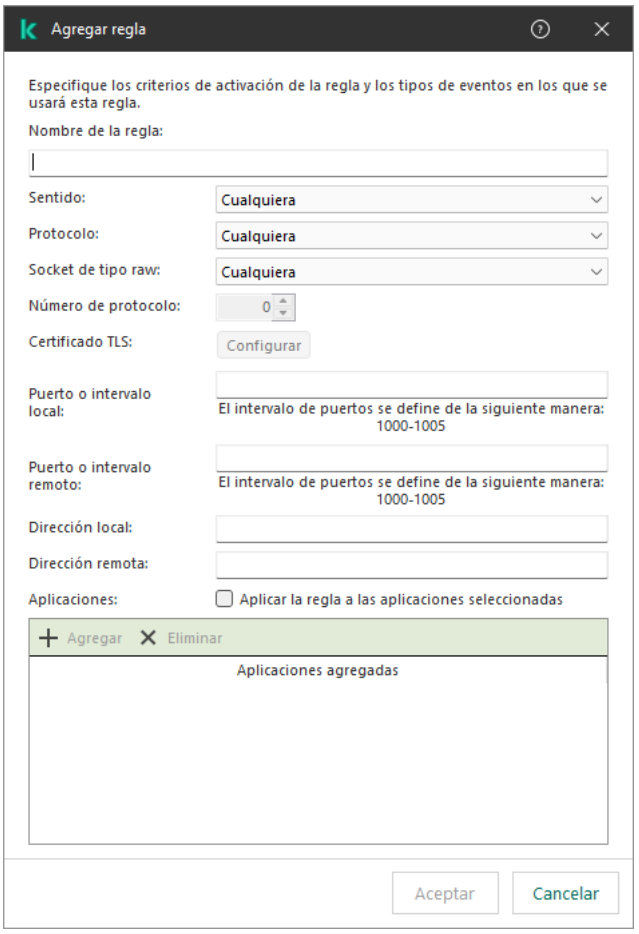
- **Ruta completa**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (opcional).
- **Uso para los siguientes tipos de eventos**: Eventos de red.

Ejemplo 2. Comunicaciones de red excluidas

Para excluir eventos de conexión de servicios remotos de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Comunicaciones de red excluidas** y agregue las opciones de configuración de conexión: protocolo, puerto, dirección, dirección IP y certificado TLS, entre otras.

Kaspersky Endpoint Security combina los criterios de activación de la regla 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 usa un servidor web corporativo y desea excluir los eventos de navegador cuando se conecta a dicho servidor web, agregue la dirección IP del servidor y el archivo ejecutable del navegador a las exclusiones de telemetría.

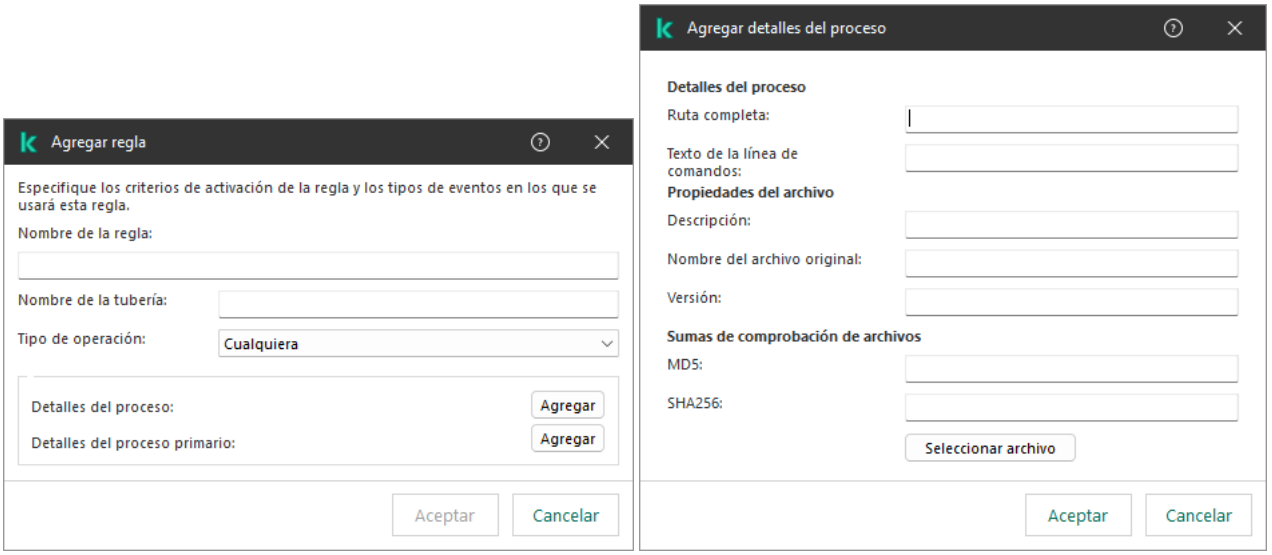
Especifique la configuración de la siguiente manera:

- **Protocolo**: TCP.
- **Puerto o intervalo 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 archivos excluidas

Para excluir eventos que involucran operaciones con archivos de confianza de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Operaciones de archivos excluidas** y agregue el archivo de confianza.

Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND.



Operaciones de archivo excluidas

Si una aplicación escribe en un registro y desea excluir los eventos de modificación de archivos de registro, agregue 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 de archivos.
- **Ruta completa**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Ejemplo 4. Modificaciones de registros excluidas

Para excluir eventos de modificación de registros de la telemetría, abra la ventana de exclusiones de telemetría de EDR en la pestaña **Cambios del registro excluidos** y agregue una clave de registro.

Kaspersky Endpoint Security combina los criterios de activación de la regla con un operador lógico AND.

Si una aplicación modifica con frecuencia sus valores de registro y desea excluir estos eventos de modificación de registro de la telemetría, agregue 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 los objetos en servidores especiales con imágenes virtuales implementadas de los sistemas operativos Microsoft Windows (servidores de Sandbox). Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

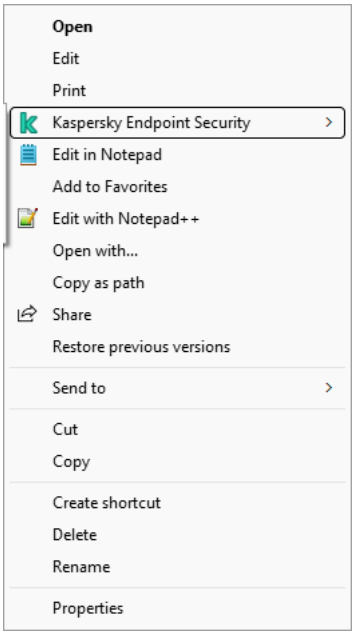
> Para activar KATA Sandbox, necesita una clave de licencia que incluya la funcionalidad de KATA o KEDR. Para obtener detalles sobre las funcionalidades disponibles, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

KATA Sandbox permite analizar archivos en los siguientes modos:

- *Manualmente*. El usuario envía manualmente el archivo para analizarlo desde el menú contextual (**Enviar a Sandbox**). Al enviar un archivo a Sandbox, la aplicación analiza el archivo con bases de datos antivirus.
- *Automáticamente*. La aplicación detecta objetos y los envía a Sandbox para analizarlos de manera automática.

Una vez que el archivo se envía a Sandbox, el usuario puede acceder a él. 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 respuesta a amenazas 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 una versión posterior. Para que KATA Sandbox funcione en modo automático, se debe implementar Kaspersky Anti Targeted Attack Platform 8.0.



Analizar en KATA Sandbox desde el menú contextual

Integración del agente incorporado con KATA Sandbox

Es necesario agregar el componente Sandbox para la integración con KATA Sandbox. Puede seleccionar el componente Sandbox durante la instalación o la actualización, además de usar la tarea *Cambiar componentes de la aplicación*.

Para enviar archivos para su análisis, debe habilitar la integración con KATA Sandbox y agregar un servidor de Central Node que se implementa dentro de la solución. El componente se puede administrar solo mediante el uso de Kaspersky Security Center Web Console. No puede administrar este componente mediante el uso de la Consola de administración (MMC).

Para habilitar o deshabilitar la integración con KATA Sandbox:

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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Sandbox**.
5. Use el interruptor **Integración con Sandbox HABILITADA** para habilitar o deshabilitar el componente.

6. Seleccione el modo de funcionamiento de KATA Sandbox:

- **Manualmente**. El usuario envía manualmente el archivo para analizarlo desde el menú contextual (**Enviar a Sandbox**).
- **Automáticamente**. La aplicación detecta objetos y los envía a Sandbox para analizarlos de manera automática.
- **Combinado**.

7. Haga clic en el vínculo **Configuración de conexión**.

8. Configure la conexión del servidor de Central Node:

- **Tiempo de espera (ms)**. Tiempo de conexión agotado 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 conexión agotado para el 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 solicitudes**. 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 la cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Sandbox deja de agregar 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, tiene que preparar un certificado TLS. Luego, debe agregar el certificado al equipo mediante una directiva. También debe agregar 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

9. En el bloque **Conexión a servidores de Sandbox**, haga clic en el botón **Agregar**.

10. Se abre una ventana para que ingrese la dirección del servidor de Sandbox (IPv4, IPv6, DNS) y el puerto.

    Para obtener más información sobre la implementación de imágenes virtuales y la configuración de los servidores de Central Node, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

11. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

De esta manera, el componente Sandbox está habilitado. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Sandbox** se agregará 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 respuesta a amenazas automáticamente (por ejemplo, elimina el objeto e inicia un Análisis de áreas críticas).

Para configurar acciones de respuesta a amenazas:

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 ficha **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 esta opción está seleccionada, 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 Cuarentena.

   - **Ejecutar análisis de áreas críticas**. Si esta opción está seleccionada, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del kernel, los procesos en ejecución y los sectores de inicio del disco.

   - **Crear tarea de Análisis de IOC**. Si esta opción está seleccionada, Kaspersky Endpoint Security crea automáticamente la tarea *Análisis de IOC (tarea de análisis de IOC independiente).* Para esta tarea, puede configurar el modo de ejecución, el alcance del análisis y la acción que se realizará al detectar un IOC (*Mover la copia a la Cuarentena, eliminar objeto* o *Ejecutar análisis de áreas críticas*). Para modificar otros opciones de la tarea *Análisis de IOC*, vaya a la configuración de la tarea.

6. Si es necesario, establezca la configuración de la tarea *Análisis de IOC* en el bloque **Alcance del Análisis de IOC**.

   - **Áreas críticas del archivo**. Si esta opción esta seleccionada, Kaspersky Endpoint Security realiza un análisis de IOC solo en áreas críticas del archivo del equipo: memoria del núcleo y sectores de inicio.

   - **Áreas de archivos en la unidad del sistema del equipo**. Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC en la unidad del sistema del equipo.

7. Si es necesario, establezca la configuración de la tarea *Análisis de IOC* en el bloque **Ejecute la tarea de Análisis de IOC**.

   - **Manualmente**. Modo de ejecución en el que puede iniciar la tarea de *Análisis de IOC* manualmente en el momento que sea conveniente para usted.

   - **Automáticamente**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta automáticamente la tarea *Análisis de IOC* después de que se detecta una amenaza.

   - **Ejecutar solo cuando el equipo esté inactivo**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea de *Análisis de IOC* si el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security pone la tarea en pausa. Esto significa que la tarea puede tardar varios días en completarse.

8. Establezca la configuración avanzada de la tarea para *Análisis de IOC*.

9. Para aplicar la directiva a los equipos, cierre los íconos 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 incorporado 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 llevará a cabo todas las funciones de Kaspersky Endpoint Agent. La carga en los servidores de Kaspersky Anti Targeted Attack Platform seguirá siendo la misma.

Cuando despliegue 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, se eliminará Kaspersky Endpoint Agent del equipo. El mismo comportamiento en el sistema ocurrirá cuando actualice Kaspersky Endpoint Security a la versión 12.1 o posterior.

> Kaspersky Endpoint Security no es compatible con Kaspersky Endpoint Agent. No puede instalar estas dos 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 posterior.

- Kaspersky Security Center versión 14.2 o posterior (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 incorporado] 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 posterior. Según el tipo de consola de Kaspersky Security Center que esté utilizando, actualice el complemento de administración en la Consola de administración (MMC) o en el complemento web de la Web Console.

2 **Migrar directivas y tareas**

Transfiera la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows. Las siguientes opciones están disponibles:

- 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 la tarea y la directiva de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en Web Console.

  En la ventana principal de Web Console, seleccione **Operaciones** → **Migración de Kaspersky Endpoint Agent**.

  Esto ejecuta el Asistente de migración de tareas y directivas. Siga las instrucciones del Asistente.

  Paso 1. Migración de la directiva

  El Asistente de migración crea una nueva directiva que fusiona la configuración de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuya configuración desee fusionar 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 fusionar la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

  Paso 2. Migración de la tarea

  El Asistente de migración no admite tareas de EDR (KATA). Omita este paso.

  Paso 3. Fin del Asistente

  Salga del Asistente. Al finalizar el asistente, se creará una nueva directiva de Kaspersky Endpoint Security. La directiva fusiona 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 nueva directiva 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 nueva directiva combinada.

  El Asistente de migración de Web Console omite la siguiente configuración de directiva y no la migra:

  - Prohibición de modificación de 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 al equipo. Debe prohibir la modificación de la configuración y cerrar el "candado".

  - Contenedor cifrado.

    Si utiliza autenticación de dos factores para conectarse a los servidores de Central Node, debe volver a agregar el contenedor cifrado.

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 estándar de conversión por lotes de directivas y tareas. 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 funcione 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 aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 se 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 cause ninguna carga adicional en su equipo en comparación con Kaspersky Endpoint Agent. Kaspersky Endpoint Security utiliza la telemetría no solo para EDR (KATA) sino también para el funcionamiento de los componentes de protección de las aplicaciones. Por lo tanto, no es necesario transferir exclusiones de telemetría de EDR individuales. Si nota que el rendimiento del equipo disminuye, compruebe el funcionamiento de la aplicación (consulte el paso 7 Comprobación del rendimiento).

3 Licencia de la funcionalidad de 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 agregar la clave con la tarea *Agregar clave*. Como resultado, se agregarán dos claves a la aplicación: *Kaspersky Endpoint Security* y *Kaspersky Endpoint Detection and Response (KATA)*.

Las licencias de complementos de Kaspersky Endpoint Detection and Response (KATA) en equipos con funciones EDR Optimum o EDR Expert previamente activadas implica las siguientes consideraciones especiales:

- Si está usando un *archivo de clave* para obtener licencias de Kaspersky Endpoint Security con las funciones EDR Optimum o EDR Expert, no puede agregar una clave separada para el complemento de Kaspersky Endpoint Detection and Response (KATA). Puede cambiar al uso de un código de activación para la licencia o comunicarse con su proveedor de servicios para obtener un nuevo archivo de clave y activar las funciones de Kaspersky Endpoint Security y EDR. El proveedor de servicios proporcionará uno o más archivos de clave para la licencia.

- Si está usando un *archivo de clave* para obtener licencias de Kaspersky Endpoint Security sin las funciones EDR Optimum o EDR Expert, puede agregar una clave para el complemento de Kaspersky Endpoint Detection and Response (KATA) sin solicitar que se vuelvan a emitir los archivos de clave.

- Si está usando un *código de activación* para la licencia, 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 deshabilitados.

- 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/actualizar la aplicación de Kaspersky Endpoint Security**

Para migrar la funcionalidad de 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 utilizando los siguientes métodos:

- Mediante el servicio de actualización de Kaspersky.

- De manera 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 usar 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 mediante Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tiene acceso a las licencias actuales de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes en función de un conjunto de componentes de Kaspersky Endpoint Agent. Después de esto, Kaspersky Endpoint Security pasa a usar el agente incorporado 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**

Luego de la instalación o actualización de la aplicación, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.

- El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes con la tarea *Cambiar componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de haber activado la funcionalidad de agente incorporado.

- Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

6. **Comprobación de la conexión con el servidor de Kaspersky Anti Targeted Attack Platform**

Compruebe la conexión con el servidor de Kaspersky Anti Targeted Attack Platform. Para hacerlo:

1. Compruebe que tiene un certificado válido.

2. Compruebe la configuración de conexión con el servidor.

3. Compruebe el registro de eventos.

   Si se establece una conexión con el servidor, la aplicación envía el evento *Se estableció la conexión al servidor de EDR Expert*. Si no hay un evento de conexión exitosa y no hay eventos con errores de conexión, compruebe la configuración del registro de eventos y habilite el envío de eventos para Endpoint Detection and Response (KATA).

El estado de conexión del servidor no afecta el estado del equipo en la consola de Kaspersky Security Center. Por lo tanto, si no hay conexión con el servidor, el equipo aún puede tener el estado *Aceptar*. Compruebe el registro de eventos para verificar la conexión con el servidor.

7 **Comprobación del rendimiento**

Si el rendimiento de la computadora se ralentiza después de instalar o actualizar una aplicación, puede optimizar la transferencia de datos. Para hacerlo:

1. Deshabilite el componente EDR (KATA) y verifique si la degradación del rendimiento se debe a EDR (KATA).

2. Para aplicaciones de confianza, deshabilite la recopilación de telemetría en las operaciones de entrada de la consola (habilitada de manera predeterminada).

3. Agregue aplicaciones que reduzcan el rendimiento de la computadora a la lista de aplicaciones de confianza.

4. Comuníquese con el Servicio de soporte técnico de Kaspersky. Los expertos en soporte lo ayudarán a configurar el filtrado de telemetría en Kaspersky Anti Targeted Attack Platform. Esto reducirá la cantidad de tráfico. Si el rendimiento de la computadora 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 la solución de Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* es una solución de ciberseguridad para empresas que incluye las aplicaciones de Kaspersky que le permiten a una organización defenderse contra la mayoría de los tipos de riesgos de ciberseguridad y cubrir los escenarios de propagación de amenazas más importantes. Los componentes de EDR Expert (on-premises) se implementan en Open Single Management Platform (OSMP). Esta plataforma ejecuta escenarios de múltiples plataformas en una única interfaz y permite integrar aplicaciones de Kaspersky con aplicaciones de terceros en un sistema integral de seguridad.

Uno de los elementos principales de la solución es *SIEM*. SIEM supervisa eventos provenientes de todos los componentes y los correlaciona entre sí mediante reglas que definen el proveedor y el usuario. EDR Expert (on-premises) analiza la telemetría y los registros recibidos de la infraestructura corporativa para detectar ataques de forma automática y permite investigar incidentes mediante un gráfico de investigación unificado que combina todos los eventos recopilados en EDR Expert (on-premises), incluidos los eventos de las aplicaciones de Kaspersky y de productos de seguridad de terceros.

Para responder ante incidentes avanzados, EDR Expert (on-premises) utiliza escenarios predefinidos y definidos por el usuario. También puede aplicar acciones de respuesta de aplicaciones de terceros y escenarios de respuesta que implican múltiples aplicaciones.

Herramientas de inteligencia de amenazas

Kaspersky Endpoint Detection and Response usa las siguientes herramientas de 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 en la 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 los datos de Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan con mayor velocidad a las amenazas, que el rendimiento de algunos componentes de protección aumente y que la posibilidad de encontrarse con falsos positivos disminuya.

Principio de operación de la solución

La aplicación Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y monitorea de forma continua los procesos, las conexiones de red abiertas y los archivos que se modifican.

> Cuando se instala en modo estándar en la infraestructura VDI, Kaspersky Endpoint Security es compatible con la integración con EDR Expert (on-premises). Sin embargo, no se garantiza el funcionamiento de las demás funcionalidades de la aplicación. Para proteger las máquinas virtuales en la infraestructura de VDI, recomendamos usar Kaspersky Endpoint Security en Modo de Light Agent.

La información sobre los eventos del 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 colección de telemetría.

La integración de EDR Expert (on-premises) se configura en la consola de Kaspersky Security Center. Luego, el agente incorporado se administra mediante Open Single Management Platform (OSMP), incluidas las tareas en ejecución, la administración de objetos en Cuarentena, la visualización de informes y otras acciones.

Configuración de Kaspersky Endpoint Security para trabajar con EDR Expert (on-premises)

Se puede utilizar la siguiente configuración para trabajar con EDR Expert (on-premises):

- **[KES+Agente incorporado]**. 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 incorporado para EDR Expert (on-premises) está disponible en Kaspersky Endpoint Security 12.11 para Windows o versiones posteriores.

- **[EPP de terceros+EDR Agent]**. En esta configuración, la Endpoint Protection Platform (EPP) de terceros proporciona la seguridad de la infraestructura de TI. 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 incorporado con EDR Expert (on-premises)

Para integrarlo con la solución Endpoint Detection and Response, debe agregar 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 funcione Endpoint Detection and Response Expert (on-premises):

- Se instaló OSMP (Open Single Management Platform).

- La aplicación está activada y las características están cubiertas por 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: habilitados y funcionan. Los siguientes componentes garantizan la operación de EDR Expert (on-premises):

  - Protección contra archivos peligrosos.

  - Protección contra amenazas web.

  - Protección contra amenazas de correo.

  - Prevención de exploits.

  - Detección de comportamiento.

  - Prevención de intrusiones en el host.

- Motor de reparación.
- Control de anomalías adaptativo.

Configurar la integración con EDR Expert (on-premises) implica realizar los siguientes pasos:

1. **Cómo probar el componente EDR Expert (on-premises):**

   Puede seleccionar el componente EDR Expert (on-premises) durante la instalación o la actualización, además de usar la tarea *Cambiar componentes de la aplicación*.

   Debe reiniciar el equipo para terminar de actualizar la aplicación con el nuevo componente.

2. **Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Tiene que comprar una licencia por separado para EDR Expert (on-premises) (complemento de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La funcionalidad se vuelve disponible después de agregar una clave diferente para Kaspersky Endpoint Detection and Response Expert (on-premises). Como resultado, se agregan dos claves en el equipo: una para Kaspersky Endpoint Security y otra 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 de EDR Expert (on-premises) esté incluida en la licencia y de que esté en ejecución en la interfaz local de la aplicación.

3. **Conexión a servidores de recopilación de telemetría y al servidor de respuesta**

   Kaspersky Endpoint Detection and Response Expert (on-premises) exige una conexión de confianza entre Kaspersky Endpoint Security y dos servidores:

   - Un *servidor de recopilación de telemetría* es un servidor que forma parte de una solución SIEM y que recopila, normaliza, correlaciona, analiza y almacena información sobre los eventos que ocurren en el equipo.
   - Un *servidor de respuesta* es un servidor que recibe y analiza datos, estudia el comportamiento de los objetos y publica los resultados de dichos estudios.

   Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Luego, 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 habilitar esta verificación, debe activar la autenticación bidireccional en la configuración del servidor y de Kaspersky Endpoint Security. Para usar autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premise)**.

5. Active el interruptor de **Endpoint Detection and Response Expert (on-premise) HABILITADO**.

6. Para configurar EDR Expert (on-premises), seleccione **Endpoint Detection and Response Expert (versión 8.0 o posterior)** de la lista de soluciones.

7. Configure la conexión de los *servidores de colección de telemetría*:

   a. En el bloque **Conexión a servidores de recopilación de telemetría**, haga clic en el vínculo **Configuración de conexión**.

   b. Configure la conexión de los servidores de colección de telemetría:

      - **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor.

      - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en Open Single Management Platform (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 habilitarla en la configuración del servidor y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Después de configurar el servidor, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña.

        El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

   d. Agregue servidores de colección de telemetría. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

      Puede agregar varias direcciones de servidores de colección de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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**, establezca la configuración de **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 a amenazas y envía los resultados de la tarea.

   b. Haga clic en el vínculo **Configuración de conexión**.

   c. Configure la conexión de los servidores de respuesta:

      - **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor.

      - **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en Open Single Management Platform (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 habilitarla en la configuración del servidor y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Después de configurar el servidor, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña.

        El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   d. Haga clic en **Aceptar**.

   e. Agregue los servidores de respuesta. Para hacerlo, especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al servidor.

      Puede agregar varias direcciones de servidores de respuestas. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 🔒 íconos de candado y guarde los cambios.

Como resultado, la computadora se agrega a la lista de dispositivos administrados en la Plataforma Única de Administración Abierta (OSMP). El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (on-premises)** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Configuración de telemetría de EDR Expert (on-premises)

Telemetría es una lista de eventos que ocurrieron en el equipo protegido. Kaspersky Endpoint Security analiza los datos de telemetría y los envía a los servidores de colección de telemetría durante la sincronización. Los eventos de telemetría llegan al servidor casi continuamente. Kaspersky Endpoint Security inicia la sincronización con el servidor cuando se cumple alguna de las siguientes condiciones:

- Se ha agotado el intervalo de sincronización.
- La cantidad de eventos en el búfer supera 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 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 restaura 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 esto, puede optimizar la configuración de transmisión de eventos, por ejemplo, para establecer un valor máximo de eventos por hora (consulte las instrucciones a continuación).

Para establecer la configuración de telemetría, realice los siguientes 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premise)**.
5. Para configurar EDR Expert (on-premises), seleccione **Endpoint Detection and Response Expert (versión 8.0 o posterior)** de la lista de soluciones.
6. Asegúrese de que la casilla de verificación **Enviar telemetría a servidores de recolección de telemetría** está seleccionada en el bloque **Configuración de la transmisión de datos**.
7. Si es necesario, seleccione la casilla **Enviar telemetría solo con IOA**. El *indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que podría señalar un ataque dirigido. La aplicación compara el comportamiento regular en el sistema con estas reglas y registros de eventos que son indicativos de un ataque dirigido. La aplicación usa la tecnología de *análisis de transmisión*, que permite dar seguimiento a estos eventos en tiempo real.

8. De ser necesario, ajuste la sincronización a la configuración del sistema en el bloque **Configuración de la transmisión de datos**:

   - **Retraso máximo de transmisión de eventos (s)**. La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos.

   - **Cantidad máxima de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. La configuración predeterminada es de 1024 eventos.

9. Si es necesario, desmarque la casilla **Habilitar regulación de solicitudes** en el bloque **Regulación de solicitudes**.

   Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, 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 habilitada de forma predeterminada.

10. Configure los ajustes de optimización para enviar eventos al servidor:

    - **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada es 15 %.

11. En el bloque **Conexión a servidores de respuesta**, ingrese 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 las tareas y la configuración de la aplicación modificada.

13. Para aplicar la directiva a los equipos, cierre los 🔒 íconos de candado y guarde los cambios.

Exclusiones de telemetría EDR Expert (on-premises)

Para mejorar el rendimiento y optimizar la transmisión de datos al servidor recopilación de telemetría, puede agregar las exclusiones de telemetría. Por ejemplo, puede optar por no enviar datos de comunicaciones de red para aplicaciones individuales.

El uso de demasiadas reglas puede aumentar la carga del servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos agregar solo las reglas necesarias.

Para crear una exclusión de telemetría con 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de telemetría**.
5. Seleccione la ficha **Telemetría de EDR Expert (on-premise)**.
6. En el bloque **Exclusiones generales**, haga clic en el botón **Agregar**.
   Se abre la ventana **Agregar regla de exclusión**.
7. Si es necesario, cambie el estado de la regla. De forma predeterminada, la regla está habilitada.
8. Ingrese 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 que activa la regla IOA se excluirá de la telemetría enviada.
10. Si se selecciona la opción **Excluir IOA** especifique las reglas de IOA que se agregarán a las exclusiones:
    - **Excluir todo**. Cuando se cumpla la condición especificada, la aplicación excluirá de la telemetría los eventos generados en base a 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 información sobre las reglas de 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 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 inferior al valor especificado en la condición, el evento se descartará.
≤	Si el valor del campo es inferior o igual al valor especificado en la condición, el evento se filtrará.
=	Si el valor del campo es igual al valor especificado en la condición, el evento se filtrará.
≥	Si el valor del campo es superior o igual al valor especificado en la condición, el evento se filtrará.
>	Si el valor del campo es superior al valor especificado en la condición, el evento se filtrará.
≠	Si el valor del campo no es igual al valor especificado en la condición, el evento se filtrará.
es parecido a	Si el valor del campo se corresponde con la máscara especificada en la condición, el evento será filtrado. La aplicación admite los caracteres `*` y `?` al ingresar una máscara:
no es parecido a	Si el valor del campo no se corresponde con la máscara especificada en la condición, el evento se filtrará. La aplicación admite los caracteres `*` y `?` al ingresar una máscara:

Operador	Descripción
uno de	Si el valor del campo se corresponde 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 se corresponde con ninguno de los valores de la lista especificada en la condición, el evento se considera filtrado.
es similar a uno de	Si el valor del campo se corresponde con una de las máscaras especificadas en la condición, el evento se filtrará. La aplicación admite los caracteres * y ? al ingresar una máscara.
no es similar a uno de	Si el valor del campo no se corresponde con ninguna de las máscaras especificadas en la condición, el evento se descartará. La aplicación admite los caracteres * y ? al ingresar una máscara.
existe	Si el campo especificado en la condición está presente en el evento, este se filtrará.
no existe	Si el campo especificado en la condición no está presente en el evento, este se filtrará.
contiene	Si el valor especificado en la condición está presente en el valor del campo, este se filtrará.
es igual a	Si el valor del campo es igual al valor especificado en la condición, el evento se filtrará. El análisis no distingue entre mayúsculas y minúsculas.
AND a nivel de bits	Si el resultado de la operación AND (&) a nivel de bits entre el valor del campo y el valor especificado en la condición es 1, este se filtrará.

12. Si es necesario, puede crear criterios de filtro complejos agregando múltiples condiciones de filtro y grupos de condiciones. También puede agregar condiciones anidadas y grupos de condiciones a un grupo de condiciones. Puede utilizar los siguientes operadores:

    - **Y** significa que el filtro selecciona los eventos que cumplen todas las condiciones especificadas.
    - **O** significa que el filtro selecciona eventos que cumplen una de las condiciones especificadas.
    - **NOT** (para utilizar este operador, seleccione la opción **Agregar NOT antes**) significa que el filtro selecciona los 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 el equipo ejecuta la Plataforma de Gestión Única Abierta (OSMP), puede analizar la regla de filtrado que ha creado. Para ejecutar el análisis, haga clic en el botón **Verificar regla**.

    En la ventana que se abre, se mostrará una tabla con los eventos filtrados según la regla creada. Para obtener más detalles, consulte la Ayuda de EDR Expert (on-premises).

14. Si es necesario, en **Todos los tipos de eventos**, agregue 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 utilizando el interruptor **Enviar evento**. De manera predeterminada, la transmisión de telemetría está habilitada para todos los tipos de eventos.

    d. En el bloque **Reglas de exclusiones**, haga clic en el botón **Agregar**.

    Se abre la ventana **Agregar regla de exclusión**.

    e. Realice las acciones descritas en los pasos 7 a 13 para cada regla que agregue.

15. Para algunos tipos de eventos, también puede agregar reglas de inclusión para expandir la telemetría recopilada:

    a. En el bloque **Reglas de inclusión**, haga clic en el botón **Agregar**.

       Se abre la ventana **Agregar regla de inclusión**.

    b. Ingrese un nombre para la regla.

    c. En **Condición**, ingrese valores para los campos mostrados. 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 íconos de candado y guarde los cambios.

Exportar e importar filtros de eventos de EDR Expert (on-premises)

Puede exportar la lista de exclusiones a un archivo JSON. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de identificadores de eventos. También puede utilizar la función de exportación/importación para crear una copia de seguridad de los filtros de eventos o para migrar la lista a un servidor diferente.

> El uso de demasiadas reglas puede aumentar la carga del servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos agregar solo las reglas necesarias.

Cómo exportar e importar los 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 correspondiente 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 objetos**.

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, escriba el nombre del archivo JSON al que quiere exportar los filtros de eventos. Seleccione también la carpeta en la que se guardará este archivo.

    b. Guarde el archivo.

       Kaspersky Endpoint Security exportará 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 cual quiere importar los filtros de eventos.

   c. Abra el archivo.

      Si ya existen reglas de filtrado de eventos en la computadora, Kaspersky Endpoint Security las reemplaza al importar.

8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo exportar e importar filtros de eventos 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de telemetría**.

5. Seleccione la ficha **Telemetría de EDR Expert (on-premise)**.

6. Para exportar los filtros de eventos:

   a. Haga clic en **Exportar**.

   b. En la ventana que se abre, escriba el nombre del archivo JSON al que quiere exportar los filtros de eventos. Seleccione también la carpeta en la que se guardará este archivo.

   c. Guarde el archivo.

      Kaspersky Endpoint Security exportará 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 cual quiere importar los filtros de eventos.

   c. Seleccione cómo desea que se importen las reglas de filtrado de eventos: agregando reglas existentes o descartando reglas existentes y reemplazándolas por nuevas.

   d. Abra el archivo.

8. Para aplicar la directiva a los equipos, cierre los íconos 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 directiva 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 sola directiva, deberá usar perfiles de directiva. Debe configurar los ajustes de 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 directiva.

El uso de perfiles de directiva 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, estos ajustes se aplicarán a todos los grupos de administración; no se aplicarán los ajustes de integración de los perfiles de directiva.

- Al usar perfiles de directiva 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, los ajustes de integración con EDR Expert (on-premises) de los perfiles de directiva serán reemplazados por los ajustes de la directiva, lo que hará que el componente funcione incorrectamente. Deberá restablecer la configuración del componente Endpoint Detection and Response Expert (on-premises) según las instrucciones que se indican a continuación.

- Al usar perfiles de directiva 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 los ajustes de integración con EDR Expert (on-premises) a los dispositivos administrados desde los perfiles de directiva.

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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Endpoint Detection and Response Expert (on-premise)**.

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 posterior)**.

6. Vuelva a **Endpoint Detection and Response Expert (versión 7.1 o anterior)**.

7. Guarde los cambios.

Solo Endpoint Detection and Response Expert (cloud)

La integración de Kaspersky Endpoint Security para Windows con Kaspersky Endpoint Detection and Response Expert (cloud) no está disponible temporalmente. Se prevé que esta funcionalidad esté disponible a finales de 2026. Manténgase al tanto de las Notas de la versión para obtener información sobre actualizaciones y nuevas funciones de las aplicaciones.

Kaspersky Endpoint Security para Windows admite la integración con la solución de Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* es una solución de ciberseguridad para empresas que incluye las aplicaciones de Kaspersky que le permiten a una organización defenderse contra la mayoría de los tipos de riesgos de ciberseguridad y cubrir los escenarios de propagación de amenazas más importantes. Los componentes de EDR Expert (cloud) Expert (cloud) se implementan en Open Single Management Platform (OSMP). Esta plataforma ejecuta escenarios de múltiples plataformas en una única interfaz y permite integrar aplicaciones de Kaspersky con aplicaciones de terceros en un sistema integral de seguridad.

La integración con Kaspersky Endpoint Detection and Response Expert (cloud) no es compatible con equipos basados en la arquitectura Arm.

Uno de los elementos principales de la solución es *SIEM*. SIEM supervisa eventos provenientes de todos los componentes y los correlaciona entre sí mediante reglas que definen el proveedor y el usuario. EDR Expert (cloud) analiza la telemetría y los registros recibidos de la infraestructura corporativa para detectar ataques de forma automática y permite investigar incidentes mediante un gráfico de investigación unificado que combina todos los eventos recopilados en EDR Expert (cloud), incluidos los eventos de las aplicaciones de Kaspersky y de productos de seguridad de terceros.

Para responder ante incidentes avanzados, EDR Expert (cloud) utiliza escenarios predefinidos y definidos por el usuario. También puede aplicar acciones de respuesta de aplicaciones de terceros y escenarios de respuesta que implican múltiples aplicaciones.

Herramientas de inteligencia de amenazas

Kaspersky Endpoint Detection and Response usa las siguientes herramientas de 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 en la 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 los datos de Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan con mayor velocidad a las amenazas, que el rendimiento de algunos componentes de protección aumente y que la posibilidad de encontrarse con falsos positivos disminuya.

Principio de operación de la solución

La aplicación Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y monitorea de forma continua los procesos, las conexiones de red abiertas y los archivos que se modifican.

La información sobre los eventos del 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 colección de telemetría.

La integración de EDR Expert (cloud) se configura en la consola de Kaspersky Security Center. Luego, el agente incorporado se administra mediante Open Single Management Platform (OSMP), incluidas las tareas en ejecución, la administración de objetos en Cuarentena, la visualización de informes y otras acciones.

Integración del agente incorporado con EDR Expert (cloud)

Para configurar la integración con la solución Kaspersky Endpoint Detection and Response (cloud), debes 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 (nube)

Para que EDR Expert (cloud) funcione, deben cumplirse 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, comuníquese con el Servicio de soporte técnico.
- Se instaló OSMP (Open Single Management Platform).
- Kaspersky Endpoint Security instalado en modo estándar.
- La aplicación Kaspersky Endpoint Security está activada y las características están cubiertas por la licencia.
- Ha aceptado los términos del Acuerdo de procesamiento de datos de Kaspersky Endpoint Detection and Response Expert (cloud).
- El componente Endpoint Detection and Response Expert (cloud) está habilitado.
- Los componentes de la aplicación que garantizan el funcionamiento de EDR Expert (cloud) están: habilitados y funcionan.
  - Protección contra archivos peligrosos.
  - Protección contra amenazas web.
  - Protección contra amenazas de 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 (nube)

Configurar la integración con EDR Expert (cloud) implica realizar los siguientes pasos:

1. **Instalación del 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 usar 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)**

   Tiene que comprar una licencia por separado para Kaspersky Endpoint Detection and Response Expert (cloud).

   La funcionalidad se vuelve disponible después de agregar una clave diferente para Kaspersky Endpoint Detection and Response (cloud). Como resultado, se agregan dos claves en el equipo: una para Kaspersky Endpoint Security y otra 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 de EDR Expert (cloud) esté incluida en la licencia y de que esté en ejecución en la interfaz local de la aplicación.

3. **Conexión a servidores de recopilación de telemetría y al servidor de respuesta**

   Kaspersky Endpoint Detection and Response Expert (cloud) Expert (on-premise) exige una conexión de confianza entre Kaspersky Endpoint Security y dos servidores:

   - Un *servidor de recopilación de telemetría* es un servidor que forma parte de una solución SIEM y que recopila, normaliza, correlaciona, analiza y almacena información sobre los eventos que ocurren en el equipo.
   - Un *servidor de respuesta* es un servidor que recibe y analiza datos, estudia el comportamiento de los objetos y publica 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 ficha **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) DESHABILITADO**.

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 la configuración en la sección **Herencia**:

   - **Heredar la configuración de conexión de la directiva** (valor predeterminado) La configuración de la conexión se heredará de la directiva principal. No podrá editar la configuración.

   - **Usar configuraciones de conexión personalizadas**. Puede establecer la configuración de conexión manualmente.

7. La pestaña **Servidor de respuesta** muestra el nombre de dominio completo y el puerto del servidor de respuesta, que se obtienen 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 de verificación **Usar túnel TCP para respuesta**.

   b. Especifique la dirección del servidor (IPv4, IPv6) y el puerto para conectarse al túnel.

8. Si es necesario, configure 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 a amenazas y envía los resultados de la tarea.

9. Vaya a la pestaña **Servidor de colección de telemetría**.

10. Configure los ajustes de conexión del servidor de recopilación de telemetría:

    a. Haga clic en el vínculo **Editar**.

    b. En la ventana que se abre, seleccione el servidor de recopilación de telemetría de la lista. El recopilador de KUMA actúa como servidor de recolección de telemetría en EDR Expert (cloud). Para obtener más detalles, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform.

    Si se produce un error al conectarse al servidor de recolección de telemetría, seleccione un servidor diferente. Si no puede conectarse al servidor de recolección de telemetría, comuníquese con el Servicio de soporte técnico.

    c. Si es necesario, puede configurar una conexión al servidor de recolección de telemetría mediante un túnel TCP, tal como lo haría para el servidor de respuesta.

11. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Como resultado, la computadora se agrega a la lista de dispositivos administrados en la Plataforma Única de Administración Abierta (OSMP). El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Expert (cloud)** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Configuración de telemetría de EDR Expert (cloud)

Telemetría es una lista de eventos que ocurrieron en el equipo protegido. Kaspersky Endpoint Security analiza los datos de telemetría y los envía a los servidores de colección de telemetría durante la sincronización. Los eventos de telemetría llegan al servidor casi continuamente. Kaspersky Endpoint Security inicia la sincronización con el servidor cuando se cumple alguna de las siguientes condiciones:

- Se ha agotado el intervalo de sincronización.
- La cantidad de eventos en el búfer supera 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 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 restaura 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 esto, puede optimizar la configuración de transmisión de eventos, por ejemplo, para establecer un valor máximo de eventos por hora (consulte las instrucciones a continuación).

Para establecer la configuración de telemetría, realice los siguientes 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 ficha **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 pestaña **Configuración de la transmisión de datos**.
6. Asegúrese de que la casilla de verificación **Envío de telemetría HABILITADO** esté seleccionada.
7. Si es necesario, seleccione la casilla **Enviar telemetría solo con IOA**. El *indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que podría señalar un ataque dirigido. La aplicación compara el comportamiento regular en el sistema con estas reglas y registros de eventos que son indicativos de un ataque dirigido. La aplicación usa la tecnología de *análisis de transmisión*, que permite dar seguimiento a estos eventos en tiempo real.
8. Si es necesario, establezca la configuración de sincronización del servidor:
   - **Retraso máximo de transmisión de eventos (s)**. La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos.
   - **Cantidad máxima de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. La configuración predeterminada es de 1024 eventos.
9. Vaya a la pestaña **Regulación de solicitudes**.

10. Si es necesario, deshabilite la limitación de solicitudes mediante el interruptor **Regulación de solicitudes HABILITADA**.

    Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, 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 habilitada de forma predeterminada.

11. Configure los ajustes de optimización para enviar eventos al servidor:

    - **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos (%)**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada es 15 %.

12. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Exclusiones de telemetría EDR Expert (cloud)

Para mejorar el rendimiento y optimizar la transmisión de datos al servidor recopilación de telemetría, puede agregar las exclusiones de telemetría. Por ejemplo, puede optar por no enviar datos de comunicaciones de red para aplicaciones individuales.

> El uso de demasiadas reglas puede aumentar la carga del servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos agregar solo las reglas necesarias.

Para crear una exclusión de telemetría con 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de telemetría**.

5. Seleccione la ficha **Telemetría de EDR Expert (cloud)**.

6. En el bloque **Exclusiones generales**, haga clic en el botón **Agregar**.

   Se abre la ventana **Agregar regla de exclusión**.

7. Si es necesario, cambie el estado de la regla. De forma predeterminada, la regla está habilitada.

8. Ingrese 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 que activa la regla IOA se excluirá de la telemetría enviada.

10. Si se selecciona la opción **Excluir IOA** especifique las reglas de IOA que se agregarán a las exclusiones:

- **Excluir todo**. Cuando se cumpla la condición especificada, la aplicación excluirá de la telemetría los eventos generados en base a 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 información sobre las reglas de 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 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 inferior al valor especificado en la condición, el evento se descartará.
≤	Si el valor del campo es inferior o igual al valor especificado en la condición, el evento se filtrará.
=	Si el valor del campo es igual al valor especificado en la condición, el evento se filtrará.
≥	Si el valor del campo es superior o igual al valor especificado en la condición, el evento se filtrará.
>	Si el valor del campo es superior al valor especificado en la condición, el evento se filtrará.
≠	Si el valor del campo no es igual al valor especificado en la condición, el evento se filtrará.
es parecido a	Si el valor del campo se corresponde con la máscara especificada en la condición, el evento será filtrado. La aplicación admite los caracteres `*` y `?` al ingresar una máscara:
no es parecido a	Si el valor del campo no se corresponde con la máscara especificada en la condición, el evento se filtrará. La aplicación admite los caracteres `*` y `?` al ingresar una máscara:
uno de	Si el valor del campo se corresponde 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 se corresponde con ninguno de los valores de la lista especificada en la condición, el evento se considera filtrado.
es similar a uno de	Si el valor del campo se corresponde con una de las máscaras especificadas en la condición, el evento se filtrará. La aplicación admite los caracteres * y ? al ingresar una máscara.
no es similar a uno de	Si el valor del campo no se corresponde con ninguna de las máscaras especificadas en la condición, el evento se descartará. La aplicación admite los caracteres * y ? al ingresar una máscara.
existe	Si el campo especificado en la condición está presente en el evento, este se filtrará.
no existe	Si el campo especificado en la condición no está presente en el evento, este se filtrará.
contiene	Si el valor especificado en la condición está presente en el valor del campo, este se filtrará.
es igual a	Si el valor del campo es igual al valor especificado en la condición, el evento se filtrará. El análisis no distingue entre mayúsculas y minúsculas.
AND a nivel de bits	Si el resultado de la operación AND (&) a nivel de bits entre el valor del campo y el valor especificado en la condición es 1, este se filtrará.

12. Si es necesario, puede crear criterios de filtro complejos agregando múltiples condiciones de filtro y grupos de condiciones. También puede agregar condiciones anidadas y grupos de condiciones a un grupo de condiciones. Puede utilizar los siguientes operadores:

    - **Y** significa que el filtro selecciona los eventos que cumplen todas las condiciones especificadas.
    - **O** significa que el filtro selecciona eventos que cumplen una de las condiciones especificadas.
    - **NOT** (para utilizar este operador, seleccione la opción **Agregar NOT antes**) significa que el filtro selecciona los 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 comprobar la regla de filtrado que ha creado, haga clic en el botón **Verificar regla**.

    En la ventana que se abre, se mostrará una tabla con los eventos filtrados según la regla creada. Para obtener más detalles, consulte la Ayuda de EDR Expert (cloud).

14. Si es necesario, en **Todos los tipos de eventos**, agregue 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 utilizando el interruptor **Enviar evento**. De manera predeterminada, la transmisión de telemetría está habilitada para todos los tipos de eventos.

    d. En el bloque **Reglas de exclusiones**, haga clic en el botón **Agregar**.

    Se abre la ventana **Agregar regla de exclusión**.

    e. Realice las acciones descritas en los pasos 7 a 13 para cada regla que agregue.

15. Para algunos tipos de eventos, también puede agregar reglas de inclusión para expandir la telemetría recopilada:

    a. En el bloque **Reglas de inclusión**, haga clic en el botón **Agregar**.

    Se abre la ventana **Agregar regla de inclusión**.

    b. Ingrese un nombre para la regla.

    c. En **Condición**, ingrese valores para los campos mostrados. 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.

Exportar e importar filtros de eventos de EDR Expert (cloud)

Puede exportar la lista de exclusiones a un archivo JSON. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de identificadores de eventos. También puede utilizar la función de exportación/importación para crear una copia de seguridad de los filtros de eventos o para migrar la lista a un servidor diferente.

El uso de demasiadas reglas puede aumentar la carga del servidor de recopilación de telemetría y reducir el rendimiento del equipo. Recomendamos agregar solo las reglas necesarias.

Para exportar o importar filtros de eventos 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de telemetría**.
5. Seleccione la ficha **Telemetría de EDR Expert (cloud)**.
6. Para exportar los filtros de eventos:

   a. Haga clic en **Exportar**.

   b. En la ventana que se abre, escriba el nombre del archivo JSON al que quiere exportar los filtros de eventos. Seleccione también la carpeta en la que se guardará este archivo.

   c. Guarde el archivo.

   Kaspersky Endpoint Security exportará 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 cual quiere importar los filtros de eventos.

   c. Seleccione cómo desea que se importen las reglas de filtrado de eventos: agregando reglas existentes o descartando reglas existentes y reemplazándolas por 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de telemetría**.

5. Seleccione la ficha **Telemetría de EDR Expert (cloud)**.

6. Para exportar los filtros de eventos:

   a. Haga clic en **Exportar**.

   b. En la ventana que se abre, escriba el nombre del archivo JSON al que quiere exportar los filtros de eventos. Seleccione también la carpeta en la que se guardará este archivo.

   c. Guarde el archivo.

   Kaspersky Endpoint Security exportará 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 cual quiere importar los filtros de eventos.

   c. Seleccione cómo desea que se importen las reglas de filtrado de eventos: agregando reglas existentes o descartando reglas existentes y reemplazándolas por nuevas.

   d. Abra el archivo.

8. Para aplicar la directiva a los equipos, asegúrese de que los candados estén cerrados (🔒) y guarde los cambios.

Gestión de la 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 Cuarentena solo cuando se integra con la solución 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 usa la cuenta del sistema (SYSTEM) para mover los archivos a cuarentena.

Puede definir la configuración de cuarentena solo en Kaspersky Security Center Web Console. También puede usar la Consola de Kaspersky Security Center para administrar objetos en cuarentena (restaurar, eliminar, agregar, etc.). De manera local, en el equipo, solo puede restaurar el objeto a través de la línea de comando.

Configurar el 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 suficiente espacio en el almacenamiento en la cuarentena*. Para evitar que la cuarentena se quede sin espacio en el disco, debe establecer un umbral en el cual Kaspersky Endpoint Security genere un evento *El almacenamiento de cuarentena tiene espacio insuficiente*. No puede configurar un período de retención para eliminar automáticamente archivos en cuarentena.

Si en su organización se implementa la solución Kaspersky Anti Targeted Attack Platform (EDR), recomendamos aumentar el tamaño de Cuarentena. Al realizar un análisis YARA, la aplicación puede encontrar un gran volcado de memoria. Si el tamaño del volcado de memoria supera el tamaño de Cuarentena, el análisis de YARA finaliza con un error y el volcado de memoria no se pone en cuarentena. Se recomienda que el tamaño de Cuarentena configurado coincida con el tamaño total de la memoria RAM del equipo (por ejemplo, 8 GB) o deshabilitar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y repositorios**.
4. En el bloque **Cuarentena**, configure el tamaño de la cuarentena:
   - **Limitar el tamaño de la Cuarentena a N MB**. Si la casilla está seleccionada, el espacio de Cuarentena se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo es de 1024 MB. Una vez que la Cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security envía el evento *No hay suficiente espacio en el almacenamiento en la cuarentena* a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación deja de mover nuevos objetos a cuarentena. Debe vaciar manualmente la Cuarentena.

     Si la casilla no está marcada, el tamaño de Cuarentena es limitado por el espacio libre disponible en el disco.
   - **Avisarme cuando el almacenamiento de la Cuarentena alcance el N %**. Valor umbral de la Cuarentena. Por ejemplo, puede establecer el umbral de la Cuarentena en 50 %. Una vez que la Cuarentena alcance 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 moviendo nuevos objetos a cuarentena.

     Si esta casilla está desmarcada, la aplicación no genera eventos cuando se alcanza el umbral de cuarentena.
5. Guarde los cambios.

Cómo configurar el tamaño máximo de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Informes y repositorios**.

5. En el bloque **Cuarentena**, configure el tamaño de la cuarentena:

   - **Limitar el tamaño de la Cuarentena**. Si la casilla está seleccionada, el tamaño de Cuarentena se limitará al valor definido. Si la casilla no está marcada, el tamaño de Cuarentena es limitado por el espacio libre disponible en el disco. Es posible que esto sea necesario para completar el análisis YARA porque la aplicación podría guardar un archivo de volcado de memoria de gran tamaño.

   - **Tamaño máximo de Cuarentena (MB)**. Si la casilla está seleccionada, el espacio de Cuarentena se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo es de 1024 MB. Una vez que la Cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security envía el evento *No hay suficiente espacio en el almacenamiento en la cuarentena* a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación deja de mover nuevos objetos a cuarentena. Debe vaciar manualmente la Cuarentena.

     Si la casilla no está marcada, el tamaño de Cuarentena es limitado por el espacio libre disponible en el disco.

   - **Avisarme cuando el almacenamiento de la Cuarentena alcance el (%)**. Valor umbral de la Cuarentena. Por ejemplo, puede establecer el umbral de la Cuarentena en 50 %. Una vez que la Cuarentena alcance 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 moviendo nuevos objetos a cuarentena.

6. Guarde los cambios.

Envío de datos acerca de los archivos en cuarentena a Kaspersky Security Center

Para realizar acciones con objetos en cuarentena en Web Console, debe habilitar el envío de datos de archivos en cuarentena al Servidor de administración. Por ejemplo, puede descargar un archivo de la cuarentena para analizarlo en Web Console. El envío de datos de archivos en cuarentena debe estar habilitado para todas las funciones de Kaspersky Sandbox y Kaspersky Endpoint Detection and Response para que pueda funcionar.

Cómo habilitar 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Configuración general** → **Informes y repositorios**.

4. En el bloque **Transferencia de datos al Servidor de administración**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, seleccione la casilla **Archivos en cuarentena**.

6. Guarde los cambios.

Cómo habilitar la transferencia de datos de archivos en cuarentena a 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 ficha **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 **Acerca de los archivos en Cuarentena**.

6. Guarde los cambios.

Como resultado, puede ver una lista de archivos en cuarentena en su equipo en la Consola de Kaspersky Security Center. Puede usar la Consola de Kaspersky Security Center para administrar objetos en cuarentena (restaurar, eliminar, agregar, etc.). Para obtener más información sobre el funcionamiento de Cuarentena, consulte la Ayuda de Kaspersky Security Center.

Restauración de archivos en Cuarentena

De manera predeterminada, Kaspersky Endpoint Security restaura los archivos a su carpeta de origen. Si se eliminó la carpeta de destino o si el usuario no tiene derechos de acceso a esa carpeta, la aplicación coloca el archivo en la carpeta `%DataRoot%\QB\Restored`. A continuación, debe mover manualmente el archivo a la carpeta de destino.

Para restaurar los archivos en Cuarentena, siga estos pasos:

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

2. Se abre la lista de archivos en Cuarentena; en dicha lista, seleccione 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. En el caso de las soluciones EDR Optimum y EDR Expert, la aplicación elimina el archivo después de la restauración. En el caso de otras soluciones, las aplicaciones guardan una copia del archivo en 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 respuestas a amenazas de todas las soluciones de Kaspersky Detection and Response. Si su organización tiene implementadas múltiples soluciones de Detection and Response (por ejemplo, EDR Optimum y MDR), Kaspersky Endpoint Security muestra el historial de respuestas a amenazas para todas ellas. Esto le permite analizar el rendimiento de las soluciones de Detection and Response en un equipo separado y optimizar la configuración de estas soluciones.

El centro de supervisión proporciona la siguiente información:

- Información sobre las tareas de respuesta a amenazas (por ejemplo, la tarea *Finalizar proceso*)

- Cambios en las reglas de prevención de ejecución y aislamiento de la red

Si la respuesta a amenazas encuentra un error relacionado con el acceso a un recurso compartido de red, dicho error se omite en el historial de respuestas a amenazas que se muestra.

Para ir al centro de supervisión de acciones de EDR, siga estos pasos:

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 ficha **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security para Windows**.
   Se abre la configuración local de la aplicación.
5. Seleccione la ficha **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 de respuesta a 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. La solución *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* administra eventos e información de seguridad (SIEM) en la infraestructura informática de las organizaciones. KUMA permite detectar, analizar y mitigar las amenazas de seguridad antes de que puedan hacer daño.

La aplicación Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y monitorea de forma continua los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos del equipo (telemetría) se envía al servidor de Kaspersky Unified Monitoring and Analysis Platform (KUMA). En la consola, KUMA muestra los eventos como una lista sin marcas, 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 marcas. Para acceder a todas las funciones de KUMA, necesita comprar una licencia e implementar la solución según la Guía del administrador de KUMA.

Integración de Kaspersky Endpoint Security con KUMA

Para usar 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 con KUMA.
- La aplicación está activada y las características están cubiertas por la licencia.
- El componente de integración con KUMA está habilitado.

Configurar la integración con KUMA implica realizar los siguientes pasos:

1. **Instalación del componente de integración con KUMA**

   Puede seleccionar el componente de integración con KUMA durante la instalación o la actualización de la aplicación, además de usar la tarea *Cambiar componentes de la aplicación*.

   Debe reiniciar el equipo para terminar de actualizar la aplicación con el nuevo componente.

2. **Activación de KUMA**

   Además de una licencia de 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 Kaspersky Endpoint Security para Windows KUMA).

Si instala 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 para KUMA solamente.

La funcionalidad estará disponible después de agregar la clave independiente de KUMA. 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 que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad de KUMA esté incluida en la licencia y de que esté en funcionamiento en la interfaz local de la aplicación.

3 **Conexión a KUMA**

Para conectar el equipo con Kaspersky Endpoint Security a la solución KUMA:

1. En la directiva de Kaspersky Endpoint Security, agregue las direcciones del servidor de KUMA y especifique la configuración de red de la conexión.

2. En la consola de KUMA, agregue un recopilador con conectores del tipo TCP o UDP, y especifique la configuración de la red básica de la conexión. Para obtener detalles sobre la administración de recopiladores, consulte la Ayuda de Kaspersky Unified Monitoring and Analysis Platform.

Puede establecer una conexión de confianza entre los servidores de KUMA y Kaspersky Endpoint Security. Para configurar una conexión de confianza, debe utilizar un certificado TLS. Puede obtener un certificado TLS en el servidor principal KUMA (consulte la configuración del conector de tipo TCP en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). Luego, debe agregar el certificado TLS a Kaspersky Endpoint Security (consulte las instrucciones a continuación).

Para que la conexión sea más segura, también puede habilitar la verificación del equipo en KUMA (autenticación bidireccional). Para habilitar esta verificación, debe activar la autenticación bidireccional en la configuración de KUMA y Kaspersky Endpoint Security. Para usar autenticación bidireccional, también necesitará un contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Debe generar un certificado con la clave privada en el formato del contenedor PKCS#12 en una autoridad de certificación externa. Luego, debe agregar el archivo de almacenamiento PFX en la consola de KUMA y en Kaspersky Endpoint Security (consulte la configuración del conector de tipo TCP en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform).

Cómo conectar un equipo con Kaspersky Endpoint Security a KUMA 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Integración con KUMA**.

4. Seleccione la casilla de verificación **Integración con KUMA**.

5. En el bloque **Configuración de la integración**, seleccione la casilla **Habilitar la transmisión de eventos de Windows a un servidor KUMA**.

6. Si es necesario, seleccione la casilla **Usar cifrado TLS** en el bloque **Configuración de conexión con los servidores de KUMA**.

7. Configure la conexión de confianza:

   a. Haga clic en **Configuración de conexión con los servidores de KUMA**.

   b. Configure la conexión del servidor:

      - **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor de KUMA. 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 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 modo TLS **With verification** (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 Kaspersky Endpoint Security y KUMA. Para usar la autenticación bidireccional, en la consola de KUMA, en la configuración del conector TCP, debe seleccionar el modo TLS **Custom PFX** (consulte la configuración del conector de tipo TCP en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). Luego, debe obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Después de configurar los ajustes de KUMA, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

        El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

8. Agregue los servidores de KUMA:

   a. Haga clic en **Agregar**.

      Esta acción abre el formulario donde puede agregar un servidor de KUMA.

   b. Seleccione el protocolo para conectarse a los servidores de KUMA: **HTTP/HTTPS**, **TCP** o **UDP**.

      Si selecciona el protocolo **HTTP/HTTPS**, de forma predeterminada, la aplicación utiliza HTTPS para la conexión a los servidores de KUMA. Para usar HTTP, debe especificar de forma manual este protocolo en la dirección del servidor (por ejemplo, `http://server.com`).

   c. Ingrese la dirección del servidor (IPv4 o IPv6) y el puerto para conectarse al servidor.

   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.

9. Si es necesario, configure la opción **Retraso máximo de transmisión de eventos (s)** en el bloque **Configuración de la transmisión de datos**. Cuando se agota el tiempo especificado, Kaspersky Endpoint Security intenta conectarse al mismo servidor o se conecta al siguiente servidor de la lista si hay varios servidores. La configuración predeterminada es de 30 segundos.

10. 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de agentes integrados** → **Integración con KUMA**.

5. Active el interruptor de **Integración con KUMA HABILITADA**.

6. Si es necesario, active el interruptor **Usar cifrado TLS** en el bloque **Configuración de conexión con el servidor**.

7. Configure la conexión de confianza:

   a. Haga clic en **Configuración de conexión**.

   b. Configure la conexión del servidor:

   - **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor de KUMA. 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 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 modo TLS **With verification** (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 Kaspersky Endpoint Security y KUMA. Para usar la autenticación bidireccional, en la consola de KUMA, en la configuración del conector TCP, debe seleccionar el modo TLS **Custom PFX** (consulte la configuración del conector de tipo TCP en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). Luego, debe obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Después de configurar los ajustes de KUMA, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.

     > El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

   c. Haga clic en **Aceptar**.

8. Agregue los servidores de KUMA:

   a. Haga clic en **Agregar**.

      Esta acción abre el formulario donde puede agregar un servidor de KUMA.

   b. Seleccione el protocolo para conectarse a los servidores de KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

      Si selecciona el protocolo **HTTP/HTTPS**, de forma predeterminada, la aplicación utiliza HTTPS para la conexión a los servidores de KUMA. Para usar HTTP, debe especificar de forma manual este protocolo en la dirección del servidor (por ejemplo, `http://server.com`).

   c. Ingrese la dirección del servidor (IPv4 o IPv6) y el puerto para conectarse al servidor.

   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.

9. Si es necesario, configure la opción **Retraso máximo al enviar eventos (s)** en el bloque **Configuración de conexión con el servidor**. Cuando se agota el tiempo especificado, Kaspersky Endpoint Security intenta conectarse al mismo servidor o se conecta al siguiente servidor de la lista si hay varios servidores. La configuración predeterminada es de 30 segundos.

10. Guarde los cambios.

Puede verificar que la integración con KUMA esté configurada correctamente en la consola de KUMA (para obtener más información, consulte Ayuda de Kaspersky Unified Monitoring and Analysis Platform). El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación* en la consola de Kaspersky Security Center. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz local de Kaspersky Endpoint Security. El componente **Integración con KUMA** se agregará a la lista de componentes de Kaspersky Endpoint Security.

4 Habilitar el envío de datos de telemetría al servidor de KUMA

De manera predeterminada, el envío de eventos al servidor KUMA está deshabilitado. Para asegurarse de que KUMA funcione correctamente, debe habilitar el envío de telemetría. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*.

Cómo habilitar el envío de datos de telemetría al servidor de 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 correspondiente 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 objetos**.

5. En el bloque **Configuración de telemetría** → **Telemetría 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 íconos de candado y guarde los cambios.

Cómo habilitar el envío de telemetría al servidor 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de telemetría**.
5. Seleccione la ficha **Telemetría 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 íconos de candado y guarde los cambios.

Filtrar eventos para enviar a KUMA

De manera predeterminada, el envío de eventos al servidor KUMA está deshabilitado. Para asegurarse de que KUMA funcione correctamente, debe habilitar el envío de telemetría. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*. Para mejorar el rendimiento y optimizar la transmisión de datos al servidor de KUMA, puede agregar o excluir eventos individuales de la telemetría de forma manual. 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 correspondiente 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 objetos**.
5. En el bloque **Configuración de telemetría** → **Telemetría KUMA**, haga clic en el botón **Configuración**.
6. En la ventana que se muestra, configure los filtros de eventos que se enviarán a KUMA.

   Puede configurar el filtrado de eventos para los registros estándar *Application*, *Security* y *System* o agregar otro registro manualmente:

   a. Abra las propiedades del registro o haga clic en el botón **Agregar** e ingrese 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 agregados a las reglas de exclusión.
   - **Enviar solo los eventos seleccionados**. En este modo, la aplicación solo envía los eventos agregados a las reglas de inclusión.

c. Cree listas de reglas de exclusión o inclusión para el modo de envío de eventos relevante.

Para agregar reglas, debe indicar el identificador del evento en el registro de eventos de Windows. Puede enumerar varios identificadores de eventos en una regla. Para especificar varios ID de eventos, use el carácter coma ("`,`").

d. Si es necesario, habilite el registro de eventos utilizando la casilla de verificación junto al nombre del registro.

7. Para aplicar la directiva a los equipos, cierre los íconos 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Configuración de telemetría**.

5. Seleccione la ficha **Telemetría KUMA**.

6. En la ventana que se muestra, configure los filtros de eventos que se enviarán a KUMA.

Puede configurar el filtrado de eventos para los registros estándar *Application*, *Security* y *System* o agregar otro registro manualmente:

a. Abra las propiedades del registro o haga clic en el botón **Agregar** e ingrese 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 agregados a las reglas de exclusión.

- **Enviar solo los eventos seleccionados**. En este modo, la aplicación solo envía los eventos agregados a las reglas de inclusión.

c. Cree listas de reglas de exclusión o inclusión para el modo de envío de eventos relevante.

Para agregar reglas, debe indicar el identificador del evento en el registro de eventos de Windows. Puede enumerar varios identificadores de eventos en una regla. Para especificar varios ID de eventos, use el carácter coma ("`,`").

d. Si es necesario, habilite el registro de eventos utilizando el interruptor junto al nombre del registro.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Exportar e importar filtros de eventos de KUMA

Puede exportar la lista de exclusiones a un archivo JSON. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de identificadores de eventos. También puede utilizar la función de exportación/importación para crear una copia de seguridad de los filtros de eventos o para migrar la lista a un servidor diferente.

El uso de demasiadas reglas puede aumentar la carga en el servidor KUMA y reducir el rendimiento del equipo. Recomendamos agregar solo las reglas necesarias.

Cómo exportar e importar los 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 correspondiente 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 objetos**.
5. En el bloque **Configuración de telemetría** → **Telemetría KUMA**, haga clic en el botón **Configuración**.
6. Para exportar los filtros de eventos:
   a. Seleccione los registros de eventos con filtros que quiere exportar.
   b. Haga clic en el botón → **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo JSON al que quiere exportar los filtros de eventos. Seleccione también la carpeta en la que se guardará este archivo.
   d. Guarde el archivo.
      Kaspersky Endpoint Security exportará 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 cual quiere importar los filtros de eventos.
   c. Abra el archivo.
      Si ya existen reglas de filtrado de eventos en la computadora, Kaspersky Endpoint Security las reemplaza al importar.
8. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo exportar e importar filtros de eventos 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 ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de telemetría**.
5. Seleccione la ficha **Telemetría KUMA**.
6. Para exportar los filtros de eventos:
   a. Seleccione los registros de eventos con filtros que quiere exportar.
   b. Haga clic en el botón → **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo JSON al que quiere exportar los filtros de eventos. Seleccione también la carpeta en la que se guardará este archivo.
   d. Guarde el archivo.

      Kaspersky Endpoint Security exportará 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 cual quiere importar los filtros de eventos.
   c. Abra el archivo.

      Si ya existen reglas de filtrado de eventos en la computadora, Kaspersky Endpoint Security las reemplaza al importar.
8. Para aplicar la directiva a los equipos, cierre los íconos 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 almacenamientos conectados a la red y sistemas operativos de Microsoft Windows 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 más detalles sobre el funcionamiento de la solución, consulte la Ayuda de Kaspersky Security for Windows Server. A partir de la versión 11.8.0 de Kaspersky Endpoint Security, ahora puede migrar de Kaspersky Security for Windows Server a Kaspersky Endpoint Security para Windows y usar la misma solución a fin de 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 14.2 o versiones posteriores. 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 ajustes 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 admite 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 anticipación. 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, encienda los componentes de la aplicación gradualmente. Es decir, comience habilitando solo el componente Protección contra archivos peligrosos, luego habilite otros componentes de protección, luego habilite los componentes de control y así sucesivamente. En cada paso, debe asegurarse de que la aplicación funcione correctamente y supervisar el rendimiento del servidor. La arquitectura de KES difiere de KSWS, por lo tanto, el sistema operativo también puede comportarse de manera diferente.
- Realice la migración gradualmente. Primero migre un solo servidor, luego varios servidores y luego realice la migración en todos los servidores de la organización.
- Migre diferentes tipos de servidores por separado. Es decir, primero migre los servidores de bases de datos, luego los servidores de correo, etc.
- La migración en servidores de alta carga implica 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 protección con contraseña). Después de la migración, también se recomienda verificar si el asistente de migración migró correctamente todos los ajustes.

Migre de KSWS a KES en el siguiente orden:

1. **Migrar 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. **Instalar Kaspersky Endpoint Security**

Puede instalar Kaspersky Endpoint Security de las siguientes maneras:

- Instalar KES después de eliminar KSWS (recomendado).

  La utilidad kavremover no admite la gestión de KSWS.

- Instalación de KES sobre KSWS.

3. Activar KES con una clave KSWS

4. **Confirme que la aplicación funciona correctamente después de la migración**

   Después de migrar de KSWS a KES, asegúrese de que la aplicación funcione correctamente. Verifique el estado del servidor en la consola (debe ser *Aceptar*). Asegúrese de que no se informen errores para la aplicación, también verifique 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 se admite)* El firewall realiza las funciones del firewall de KSWS a 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 se admite)* Puede configurar la interacción del usuario en la configuración de la interfaz de la aplicación.
Integration with Kaspersky Security Center	Conector del Agente de red
Endpoint Agent	*(no se admite)* 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 contra amenazas de red
Anti-Cryptor	Detección de comportamiento
Anti-Cryptor for NetApp	*(no se admite)*

Componente de Kaspersky Security for Windows Server	Componente de Kaspersky Endpoint Security para Windows
Traffic Security	Protección contra amenazas web Protección contra amenazas de correo Control web
On-Demand Scan	Núcleo de la aplicación
ICAP Network Storage Protection	*(no se admite)* Kaspersky Endpoint Security no admite componentes de protección de almacenamiento en red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(no se admite)* Kaspersky Endpoint Security no admite componentes de protección de almacenamiento en red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.
Real-Time File Protection	Protección contra amenazas de archivo
Script Monitoring	*(no se admite)* La Supervisión de scripts está manejada por otros componentes, por ejemplo, Protección vía AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Control de aplicaciones
Performance counters	*(no se admite)*

Correspondencia de las configuraciones 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 en los valores predeterminados.

Application settings

Scalability, interface and scanning settings

La configuración de la aplicación no es compatible con 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)* La ventana principal de Kaspersky Endpoint Security y el ícono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente de forma predeterminada. 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 del análisis.
Limit CPU usage for scanning threads	*(no migra)* Kaspersky Endpoint Security no limita el uso de la CPU al analizar. 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 es compatible con los sistemas HSM.

Security and reliability

La configuración de seguridad de KSWS se migra a la sección **Configuración general**, Configuración de la aplicación y a las subsecciones 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	**Habilitar la Autoprotección** (subsección **Configuración de la aplicación**)
Apply password protection	*(no migra)* Kaspersky Endpoint Security tiene una función integrada de protección con contraseña (vea la subsección **Interfaz**).
Perform task recovery	*(no migra)* Kaspersky Endpoint Security solo restaura automáticamente las tareas de *Análisis de malware*. Kaspersky Endpoint Security ejecuta otras tareas según una programación.
Do not start scheduled scan tasks	**Posponer las tareas programadas cuando el equipo funciona con carga de batería** (subsección **Configuración de la aplicación**)
Stop current scan tasks	*(no migra)* Cuando el equipo recibe energía 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** Configuración de red y a las subsecciones 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 el servidor proxy para las direcciones locales** (subsección **Configuración de red**)
Proxy server authentication settings	**Autenticarse ante el servidor proxy** (subsección **Configuración de red**) La contraseña de autenticación del servidor proxy no se migra. Después de migrar una directiva, la contraseña debe ingresarse 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 KES locales en **Tareas locales**, Administración de tareas. También puede configurar un programa para ejecutar las tareas *Análisis de malware* y *Actualización de 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 de análisis** (Exclusiones de 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 agregar estas exclusiones manualmente. Las exclusiones como áreas predefinidas deben configurarse en la configuración de la tarea *Análisis de malware*. Las exclusiones como direcciones web de scripts deben agregarse a las direcciones web de confianza para la Protección contra amenazas web.
Apply also to subfolders (Exclusions)	**Incluir subcarpetas** (Exclusiones de análisis)
Objects to detect (Exclusions)	**Tipo del objeto detectado** (Exclusiones de análisis)
Exclusion usage scope (Exclusions)	**Componentes de protección** (Exclusiones de 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 de análisis)
Trusted process (Trusted process)	**Aplicaciones de confianza** Los métodos de confianza de selección de procesos/aplicaciones difieren en KSWS y KES. 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 del archivo, dichos procesos de confianza no se migran. Después de la migración, debe agregar dichos 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 de 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 en una conexión de 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 en una conexión de unidad extraíble**: • **Máxima protección** • **Recomendado** Los niveles de seguridad de KSWS corresponden a los modos de análisis de KES de la siguiente manera: • Maximum protection – Máxima protección • 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 de almacenamiento de KSWS se migra a la sección **Configuración general**, subsección [Informes y repositorios] y a la sección **Protección básica contra amenazas**, susbsección [Protección contra amenazas de red].

Configuración de almacenamiento

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.14.1\QB`.
Maximum Backup size (MB)	**Limitar el tamaño de Copia de seguridad a N MB** (sección **Configuración general** → **Informes y repositorios**)
Threshold value for space available (MB)	*(no migra)* Kaspersky Endpoint Security registra el evento *El almacenamiento de cuarentena tiene espacio insuficiente* 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.14.1\QB`.
Maximum Quarantine size (MB)	*(no migra)* Kaspersky Endpoint Security usa una copia de seguridad para almacenar objetos probablemente infectados. Durante la migración, Kaspersky Endpoint Security ignora la configuración de la cuarentena.
Threshold value for space available (MB)	*(no migra)* Kaspersky Endpoint Security usa una copia de seguridad para almacenar objetos probablemente infectados. Durante la migración, Kaspersky Endpoint Security ignora la configuración de la 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 básica contra amenazas** → **Protección contra amenazas de 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 básica contra amenazas**, subsección **Protección contra amenazas de archivo**.

Configuración de la 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 • Ante operaciones de ejecución • Ante operaciones de acceso • Ante operaciones de acceso y modificación
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	Alcance de la protección
Schedule settings	*(no migra)* Kaspersky Endpoint Security utiliza su propio programa para pausar Protección contra archivos peligrosos.

KSN Usage

La configuración de KSWS para Kaspersky Security Network se migra a la sección **Protección avanzada contra amenazas**, 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 para la Declaración de Kaspersky Security Network cuando se instala la aplicación, se crea una nueva directiva o se habilita el uso de Kaspersky Security Network.
Send data about scanned files	*(no migra)* Kaspersky Endpoint Security envía datos sobre archivos analizados automáticamente si KSN está habilitado.
Send data about requested URLs	*(no migra)* Kaspersky Endpoint Security envía datos sobre las URL solicitadas automáticamente si KSN está habilitado.
Send Kaspersky Security Network statistics	**Habilitar el modo KSN extendido**
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	**Usar el Servidor de administración como servidor proxy de KSN**
Schedule settings	*(no migra)* No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

Traffic Security

La configuración de seguridad de tráfico de KSWS se migra a la sección **Protección básica contra amenazas**, subsección Protección contra amenazas web y Protección contra amenazas de 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 separadas en Kaspersky Endpoint Security.
Apply certificate-based rules	*(no migra)* Kaspersky Endpoint Security no admite 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 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 pueden usarse para dañar el dispositivo protegido.
Allow access to legitimate advertisement	*(no migra)* Puede administrar el acceso a publicidad legítima utilizando la categoría de recursos web *Anuncios* 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 es compatible con ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Modo **Analizar conexiones cifradas** / **Analizar siempre las conexiones cifradas** (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 protocolos siguientes: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Además, puede bloquear las conexiones SSL 2.0 en 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 desmarca las casillas **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 ajustes para la aplicación de confianza: • Se selecciona la casilla de verificación **No analizar el tráfico de red**. KES no analiza el tráfico de red en busca de direcciones IP ni puertos remotos. • Se desactivan las demás casillas de verificación en la configuración de las aplicaciones de confianza.
Security port	*(no migra)*
Use malicious URL database to scan web links	**Comprobar si la dirección web está en la base de datos de direcciones web maliciosas** (subsección **Protección contra amenazas web**)
Use anti-phishing database to scan web pages	**Comprobar si la dirección web está en la base de datos de direcciones web fraudulentas** (subsección **Protección contra 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	**Utilizar análisis heurístico** (subsecciones **Protección contra amenazas web** y **Protección contra amenazas de correo**)
Security level	*(no migra)* Kaspersky Endpoint Security tiene sus propios niveles de seguridad para los componentes de Protección contra amenazas web y Protección contra amenazas de correo. De forma predeterminada, Kaspersky Endpoint Security establece el nivel de seguridad recomendado.
Enable mail threat protection	**Protección contra amenazas de correo** (subsección **Protección contra amenazas de correo**) **Conectar extensión de Microsoft Outlook** **Solo mensajes entrantes** (Alcance de la protección) **Analizar al recibir** (Protección de correo electrónico)
Schedule settings	*(no migra)* No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

Exploit Prevention

La configuración de Prevención de exploits de KSWS se migra a la sección **Protección avanzada contra amenazas**, 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 detectarse un exploit**: • **Bloquear** • **Informar**
Notify about abused processes via Terminal Service	*(no migra)* Kaspersky Endpoint Security no admite servicios de terminal.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(no migra)* Kaspersky Endpoint Security evita constantemente los exploits de los procesos vulnerables.
Protected processes	**Habilitar la protección de la memoria de procesos del sistema** Kaspersky Endpoint Security no admite la selección de procesos protegidos. Solo puede habilitar 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

La configuración de Protección contra amenazas de red de KSWS se migra a la sección **Protección básica contra amenazas**, subsección Protección contra amenazas de red.

Configuración de Protección contra amenazas de 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 contra amenazas de red** Si el modo **Pass-through** está seleccionado, la protección contra amenazas de red está deshabilitada. Si los modos **Only inform about network attacks** o **Block connections when attack is detected** están seleccionados, se habilita Protección contra amenazas de red. 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 habilitado.
Do not control excluded IP addresses	**Exclusiones**
Schedule settings	*(no migra)* No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

Script Monitoring

Kaspersky Endpoint Security no es compatible con el componente de Supervisión de scripts. La Supervisión de scripts está manejada por otros componentes, por ejemplo, Protección vía 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)	Juegos de azar, loterías, sorteos
Alcohol	Alcohol, tabaco, drogas
Anonymous proxy servers	Anonimizadores
Anorexia	*(no migra)*
Rentals for real estate	*(no migra)*
Audio, video and software	Software, audio, video
Banks	Bancos
Blogs	Blogs
Military	Armas, explosivos, contenido militar
For children	*(no migra)*
Discrimination	Violencia e 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	Juegos de azar, 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	Juegos de azar, loterías, sorteos
Medicine	*(no migra)*
Fashion	*(no migra)*
Music	*(no migra)*
Drugs	Alcohol, tabaco, drogas
Violence	Violencia e intolerancia
Discontent	*(no migra)*
Illegal drugs	Alcohol, tabaco, drogas
Hate and discrimination	Violencia e intolerancia

Categorías de Kaspersky Security for Windows Server	Categorías de Kaspersky Endpoint Security para Windows
Obscene vocabulary	Malas palabras, 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, contenido militar
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 la web
Traveling	*(no migra)*
TV and radio	Medios de comunicación
Teasers and ads services	Anuncios
Religion	Religiones, asociaciones religiosas
Restaurants, cafe and food	*(no migra)*
Dating sites	Sitios de citas
Sex education	Contenido para adultos
Social networks	Redes sociales
Sport	*(no migra)*
Betting	Juegos de azar, loterías, sorteos
Suicide	Violencia e intolerancia
Tobacco	Alcohol, tabaco, drogas
Torrents	Torrents
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 e 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**	**Acción** (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 permite migrar reglas de Control de lanzamiento de aplicaciones. La funcionalidad de migración de reglas de Control de lanzamiento de aplicaciones tiene algunas limitaciones. De forma predeterminada, el Control de lanzamiento de aplicaciones de KSWS tiene dos reglas: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Si al menos una regla de KSWS de origen tiene la configuración **Allow**, durante la migración, KES crea una nueva regla de autorización: **Aplicaciones con certificados raíz de confianza**. Es decir, Control de aplicaciones de KES utiliza una única regla para permitir la ejecución de scripts, paquetes MSI y archivos ejecutables de confianza. Si ambas reglas de KSWS de origen tienen la configuración **Deny**, KES no agrega reglas para administrar aplicaciones con certificados raíz de confianza.
Apply rules to executable files	*(no migra)* No se puede configurar el alcance de la aplicación de reglas en la configuración de Control de aplicaciones de KES. Control de aplicaciones de KES aplica reglas a todo tipo de archivos: archivos ejecutables, scripts y paquetes MSI. Si se incluyen todos los tipos de archivos en el alcance de la aplicación de reglas en KSWS, durante la migración, KES transfiere las reglas a KSWS. Si se excluye algún tipo de archivo del alcance de la aplicación de reglas en KSWS, durante la migración, KES también transfiere las reglas a KSWS, pero se selecciona **Probar reglas** como acción de Control de aplicaciones.
Monitor loading of DLL modules	**Supervisar la carga de módulos DLL (aumenta significativamente la carga del sistema)**
Apply rules to scripts and MSI packages	*(no migra)* No se puede configurar el alcance de la aplicación de reglas en la configuración de Control de aplicaciones de KES. Control de aplicaciones de KES aplica reglas a todo tipo de archivos: archivos ejecutables, scripts y paquetes MSI. Si se incluyen todos los tipos de archivos en el alcance de la aplicación de reglas en KSWS, durante la migración, KES transfiere las reglas a KSWS. Si se excluye algún tipo de archivo del alcance de la aplicación de reglas en KSWS, durante la migración, KES transfiere las reglas a KSWS, pero se selecciona **Probar reglas** como 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 agrega una nueva regla de autorización. Se especifica la categoría KL **Otro software\Aplicaciones, de confianza según su reputación en KSN** 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 según su reputación en KSN**.
Automatically allow software distribution via applications and packages listed	El control de distribución de software en KSWS y KES funciona de manera diferente. Durante la migración, KES agrega nuevas reglas de autorización para las aplicaciones que permiten la distribución automática de software. Se especifica el hash de archivo como condición de activación de reglas.
Always allow software distribution via Windows Installer	El control de distribución de software en KSWS y KES funciona de manera diferente. Durante la migración, KES agrega nuevas reglas de autorización para las aplicaciones que permiten la distribución automática de software (**Software distribution applications and packages allowed**). Se especifica el hash de archivo como condición de activación de reglas. En propiedades de la cuenta, la casilla de verificación **Actualizadores de confianza** está seleccionada.
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 de manera diferente. Durante la migración, KES agrega nuevas reglas de autorización para las aplicaciones que permiten la distribución automática de software. Se especifica el hash de archivo como condición de activación de reglas. En propiedades de la cuenta, la casilla de verificación **Actualizadores de confianza** está seleccionada.
Schedule settings	*(no migra)* Si se configura un programa para el componente en la configuración de KSWS, se habilita el componente Control de aplicaciones en la migración. Si no se configura un programa para el componente en la configuración de KSWS, se deshabilita Control de aplicaciones al momento de la migración. No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

Device Control

La configuración de Control de dispositivos KSWS se migra a la sección **Controles de seguridad**, subsección **Control de dispositivos**.

La 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 opera en el modo *Active*. Auditoría proporciona estadísticas de conexión de dispositivos continuamente.
Allow using all external devices when the Device Control task is not running	*(no migra)* El 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 deshabilitadas.
Schedule settings	*(no migra)* Kaspersky Endpoint Security utiliza su propio programa para obtener acceso a ciertos tipos de dispositivos.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security no admite componentes de protección de almacenamiento en 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 en red. Si necesita estos componentes, puede continuar usando Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security no es compatible con Anti-Cryptor para NetApp. La funcionalidad Anti-Cryptor es proporcionada por otros componentes de la aplicación, como Detección de comportamiento.

Network activity control

Firewall Management

Kaspersky Endpoint Security no es compatible con la gestión de firewall de KSWS. El firewall realiza las funciones del firewall de KSWS a 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 avanzada contra amenazas**, subsección, **Detección de comportamiento**.

Configuración de Anti-Cryptor

Configuración de KSWS	Configuración de KES
Operation mode: • **Statistics only** • **Active**	**Al detectar intentos de cifrado externo en las carpetas compartidas**: • **Informar** • **Bloquear**
Heuristic analyzer	*(no migra)* Kaspersky Endpoint Security no utiliza el análisis heurístico para la 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 agregar manualmente exclusiones después de la migración.
Schedule settings	*(no migra)* No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

System Inspection

File Integrity Monitor

La configuración de Monitor de integridad de archivos de KSWS se migra a la sección **Controles de seguridad**, subsección **Control de integridad del sistema**.

Configuración de 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 de operaciones sobre archivos que se realizaron durante el período de interrupción del monitoreo.
Block attempts to compromise the USN log	*(no migra)* Kaspersky Endpoint Security no bloquea los intentos de comprometer el registro de USN.
Monitoring scope	**Alcance del monitoreo** → **Archivo** *(compatible con limitaciones)* Los registros deshabilitados del alcance del monitoreo no se migran a KES. Kaspersky Endpoint Security agrega solo registros habilitados al alcance del monitoreo.
Trusted users	**Grupos de usuarios o usuarios de confianza**
File operation markers	**Marcadores de las operaciones sobre archivos**
Calculate checksum for the file if possible	**Ejecución de hash**
Exclusions	**Exclusiones** → **Archivo**

Log Inspection

La configuración de Inspección de registro de KSWS se migra a la sección **Controles de seguridad**, subsección **Inspección de registros**.

Configuración de Inspección de registro

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 habilitadas.
Custom rules	**Reglas personalizadas** La regla predefinida de **A service was installed in the system (for Server 2003 OS)** no se migra a KES.
Apply predefined rules for log inspection	*(no migra)* Kaspersky Endpoint Security aplica todas las reglas predefinidas habilitadas.
Predefined rules	**Reglas predefinidas**
Password brute-force detection	**Detección de ataques de fuerza bruta**
Network logon detection	**Detección de inicios de sesión en la red**
Exclusions (IP addresses)	**Exclusiones** (Dirección IP)
Exclusions (users)	**Exclusiones** (Usuarios)
Schedule settings	*(no migra)* No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

Logs and notifications

Task logs

La configuración de los registros de KSWS se migran a la sección **Configuración general**, subsecciones Interfaz y Informes y repositorios.

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.14.1\Report`.
Remove task logs older than N day(s)	*(no migra)* Puede configurar el período de almacenamiento para los informes de KES en **Configuración general**, **Informes y repositorios**.
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.
Integration with SIEM	*(no migra)* Puede configurar la integración 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 la configuración de notificaciones por correo electrónico se migra 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 actualizaron**
Application database is extremely out of date	**Enviar la notificación "Bases de datos extremadamente desactualizadas" si las bases de datos no se actualizaron**
Critical areas scan has not been performed for a long time	*(no migra)* Kaspersky Endpoint Security genera un evento de Análisis de áreas críticas no realizado 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 repositorios.

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 Copias de seguridad**
Blocked hosts	*(no migra)* Kaspersky Endpoint Security envía automáticamente datos sobre hosts bloqueados.

Tasks

Activating the application

Kaspersky Endpoint Security no es compatible con la tarea de *Application activation* (KSWS). Puede crear una tarea *Agregar clave* (KES), agregar una clave de licencia al Paquete de instalación o habilitar la distribución automática de claves de licencia.

Copying Updates

La configuración de la tarea de *Copying Updates* (KSWS) se migra a la tarea de *Actualización de bases de datos y módulos de la aplicación* (KES).

Configuración de la tarea de 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 fuentes de actualización, incluidos los servidores de actualización de Kaspersky. Si la primera fuente de actualización no está disponible, Kaspersky Endpoint Security le permite obtener actualizaciones de otra fuente 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 siguiente carpeta**

Baseline File Integrity Monitor

La configuración de la tarea *Baseline File Integrity Monitor* (KSWS) se migra a la tarea *Comprobación de 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 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 calcular la suma de comprobación.
Scan scope	**Alcance del monitoreo** (subsección **Control de integridad del sistema**)

Database Update

La configuración de la tarea de *Database Update* (KSWS) se migra a la tarea de *Actualización de bases de datos y módulos de la aplicación* (KES).

Configuración de la tarea de actualización de la base 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 fuentes de actualización, incluidos los servidores de actualización de Kaspersky. Si la primera fuente de actualización no está disponible, Kaspersky Endpoint Security le permite obtener actualizaciones de otra fuente 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 de *Software Modules Update* (KSWS) se migra a la tarea de *Actualización de bases de datos y módulos de la aplicación* (KES).

Configuración de la tarea de 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 fuentes de actualización, incluidos los servidores de actualización de Kaspersky. Si la primera fuente de actualización no está disponible, Kaspersky Endpoint Security le permite obtener actualizaciones de otra fuente 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 verifica continuamente la disponibilidad de actualizaciones críticas para los 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 de *Rollback of Application Database Update* (KSWS) se migra a la tarea de *Reversión de la actualización* (KES). La tarea nueva *Reversión de la actualización* (KES) tiene una programación de inicio de tarea: *Manual*.

On-Demand Scan

La configuración de la tarea de *On-Demand Scan* (KSWS) se migra a la tarea de *Análisis de malware* (KES).

Configuración de la tarea de análisis antivirus

Configuración de Kaspersky Security for Windows Server	Configuración de Kaspersky Endpoint Security para Windows
Scan scope	**Alcance del análisis**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Nivel de seguridad**: • **Alto** • **Recomendado** • **Bajo** 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** • **Archivos analizados según su formato** • **Archivos analizados según su 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 **Archivos analizados según su 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 solo archivos nuevos y modificados**
Scan of compound objects: • La **All archives** • **All SFX archives** • La **All email databases** • La **All packed objects** • La **All plain email** • La **All embedded OLE objects**	**Análisis de archivos compuestos**: • **Analizar archivos de almacenamiento**. • **Analizar archivos de almacenamiento protegidos por contraseña**. • **Analizar paquetes de distribución**. • **Analizar archivos de formato de correo electrónico**. • **Analizar archivos 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 falla la desinfección**. • **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 que se analicen durante más de N s**
Do not scan compound objects larger than N MB	**No desempaquetar archivos compuestos grandes**
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 los archivos sin conexión en su totalidad.

Application Integrity Check

La configuración de la tarea de *Application Integrity Control* (KSWS) se migra a la tarea de *Comprobación de integridad de la aplicación* (KES).

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security no es compatible con la tarea de *Applications Launch Control Generator*. Puede generar reglas en Configuración de control de aplicaciones.

Rule Generator for Device Control

Kaspersky Endpoint Security no es compatible con la tarea de *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 encontrar 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 tiene se instalan de la siguiente manera:

- Protección vía AMSI, Prevención de intrusiones en el host, Motor de reparación se instalan con la configuración predeterminada.
- Los componentes Prevención de ataques BadUSB, Control de anomalías adaptativo, Cifrado de datos, 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 propiedades del paquete de instalación. Después de instalar Kaspersky Endpoint Security y migrar las 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 la tarea y la directiva de KSWS de las siguientes maneras:

- Uso del Asistente de conversión por lotes de directivas y tareas (en adelante también "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 se puede migrar a Web Console y Cloud Console.

  El asistente de conversión por lotes funciona de manera diferente para las distintas versiones de Kaspersky Security Center. Recomendamos actualizar la solución a la versión 14.2 o una 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 ajustes de directivas.

- Uso del Asistente de nueva directiva de Kaspersky Endpoint Security para Windows.

  El Asistente de nueva directiva le permite crear una directiva de KES basada en una directiva de KSWS.

Los procedimientos de migración de directivas de KSWS son diferentes cuando se utiliza el Asistente de migración y el Asistente para nuevas directivas.

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 ajustes de directivas que se activa en una computadora si el equipo cumple con las reglas de activación configuradas. La etiqueta del dispositivo `UpgradedFromKSWS` se selecciona como el criterio de activación del perfil de directiva. Kaspersky Security Center agrega automáticamente la etiqueta `UpgradedFromKSWS` a todas las computadoras en las 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 agregar 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 agregue 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 el funcionamiento de 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 perfiles 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, seleccione 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. Seleccionar la aplicación para la que desea convertir directivas y tareas

En este paso, debe seleccionar Kaspersky Endpoint Security para Windows. Vaya al siguiente paso.

Paso 2. Conversión de directivas

El asistente de migración crea perfiles de directivas de KSWS dentro de una directiva de KES. Seleccione las directivas de Kaspersky Security for Windows Server que desee convertir a perfiles de directivas. Vaya al siguiente paso.

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. Se nombrarán nuevas tareas como *<nombre de la tarea de KSWS> (convertido)*. Vaya al siguiente paso.

Paso 5. Fin del Asistente

Salga del Asistente. Como resultado, el asistente hace lo siguiente:

- Se agregan nuevos perfiles de directiva a la directiva de Kaspersky Endpoint Security.

  La directiva incluye perfiles con la configuración de Kaspersky Security for Windows Server. La nueva directiva tiene el estado *Activa*. El asistente deja sin cambios las directivas de KSWS.

- Cree nuevas tareas de Kaspersky Endpoint Security.

  Las nuevas tareas son copias de las tareas de KSWS. El asistente deja sin cambios 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 la etiqueta del 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, una directiva de KES corresponderá a una directiva de KSWS. El asistente no convierte la directiva en un perfil.

Cómo usar el Asistente de nueva directiva para migrar la configuración de la directiva 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Haga clic en **Nueva directiva**.

   Se inicia el Asistente para directivas.
5. Siga las instrucciones del Asistente para directivas.

Paso 1. Seleccionar la aplicación para crear la directiva de grupo

Seleccione la aplicación **Kaspersky Endpoint Security para Windows (14.1)**.

Paso 2. Asignar un nombre a la directiva de grupo

Escriba un nombre para la directiva de grupo, por ejemplo, *Directiva de la oficina*.

Seleccione la casilla de verificación **Usar la configuración de la directiva creada para una versión más antigua de la aplicación**. Haga clic en **Examinar** y seleccione 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. Seleccionar el modo de uso de la aplicación en los equipos

Seleccione **Modo estándar para proteger hosts**. Kaspersky Endpoint Security proporciona una directiva común para todos los modos de la aplicación y tipos de SO.

Recomendamos usar diferentes directivas para diferentes modos y tipos de sistemas operativos.

Paso 5. Importación de 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 CFG. Al importar un archivo de configuración de la aplicación, no toda la configuración de la directiva está disponible para el asistente. Por ejemplo, los perfiles de directivas no aparecen en la configuración de la aplicación. Si desea transferir toda la configuración y todos los 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 criptocontenedores. Si utiliza la autenticación bidireccional al conectarse a los servidores, debe especificar las contraseñas del criptocontenedor desde cero.

Paso 6 - 10. Configuración de las opciones 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

Configure la zona de confianza. Puede agregar exclusiones de análisis y aplicaciones de confianza predefinidas. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en el modo de Light Agent en los entornos virtuales de Citrix y VMware.

Paso 12. Seleccionar el estado de la directiva

- **Activas**. Después de la próxima sincronización, la directiva se usará 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.

- **Inactivas**. 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 con 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 sale del perímetro de la red de la organización.

Salga del 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 con contraseña de KSWS no se migra. Kaspersky Endpoint Security tiene una función de protección con 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 agregar estas exclusiones manualmente.

  Para asegurarse de que Kaspersky Endpoint Security funcione 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 aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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. El firewall realiza las funciones del firewall de KSWS a 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 la configuración de KSN para componentes individuales. Kaspersky Endpoint Security usa KSN para todos los componentes de la aplicación. Para usar 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 es necesario, agregue reglas de Control web.

- Servidor proxy. La contraseña de conexión del servidor proxy no se migra. Ingrese la contraseña que usará para conectarse al servidor proxy manualmente.

- Programas de componentes individuales. Kaspersky Endpoint Security no admite la configuración de programaciones para componentes individuales. Los componentes están siempre encendidos mientras Kaspersky Endpoint Security está operativo.

- Conjunto de componentes. El conjunto de características disponibles en Kaspersky Endpoint Security depende de si el sistema operativo está diseñado para estaciones de trabajo o para servidores. Por ejemplo, fuera 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 todos los ajustes en la nueva directiva tienen una prohibición aplicada sobre 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 ajustes **Soporte para el usuario** (sección **Interfaz**). Si es necesario, configure la opción de heredar los ajustes desde 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 los ajustes de la tarea *Análisis de malware* 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 deshabilitada.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security tiene un agente incorporado para trabajar con soluciones de Detection and Response. Si es necesario, transfiera la configuración de la directiva de Kaspersky Endpoint Agent a la directiva de Kaspersky Endpoint Security.

- Tareas de *Actualización de bases de datos y módulos de la aplicación*. Asegúrese de que la configuración de la tarea *Actualización de bases de datos y módulos de la aplicación* se haya migrado correctamente. En lugar de las tres tareas de KSWS, KES usa una sola tarea de KES. Puede optimizar las tareas de *Actualización de 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*, *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 de dispositivos.

Migración de la zona de confianza de KSWS

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo. Puede migrar los objetos de la zona de confianza 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 basada en la directiva de KSWS*. KSWS y KES tienen diferentes conjuntos de componentes y características, por lo que, después de la migración, debe verificar que las exclusiones cumplan con los requisitos de seguridad corporativos. Los métodos para agregar exclusiones a la zona de confianza también son diferentes en KES y KSWS. El asistente de migración no tiene herramientas para migrar todas las exclusiones de KSWS. Esto significa que después de la migración, debe agregar manualmente algunas de las exclusiones de KSWS.

Para asegurarse de que Kaspersky Endpoint Security funcione 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 aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 la zona 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	→	**Tipo del objeto detectado**
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 algunas limitaciones. La migración de una exclusión depende del método de selección del objeto:

- Predefined scope: *no migra*.

  Después de la migración, debe agregar estas exclusiones manualmente. Las exclusiones como áreas predefinidas deben configurarse en la configuración de la tarea *Análisis de malware*.

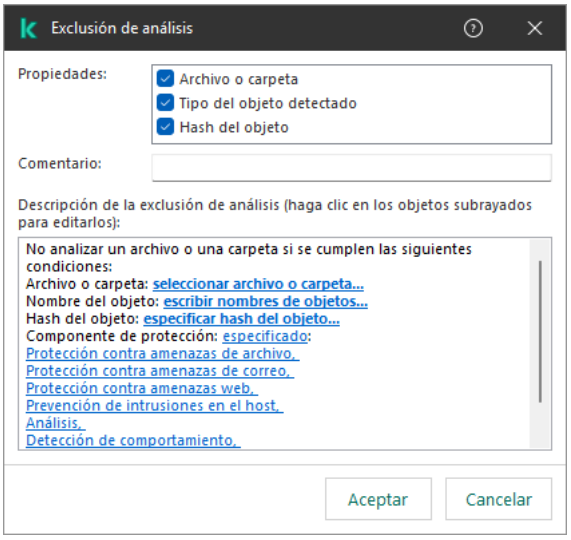
- Disk, folder or network location: migra a las exclusiones de KES que tienen el método "Archivo o carpeta" seleccionado en las propiedades.

- File: migra a las exclusiones de KES que tienen el método "Archivo o carpeta" seleccionado en las propiedades.

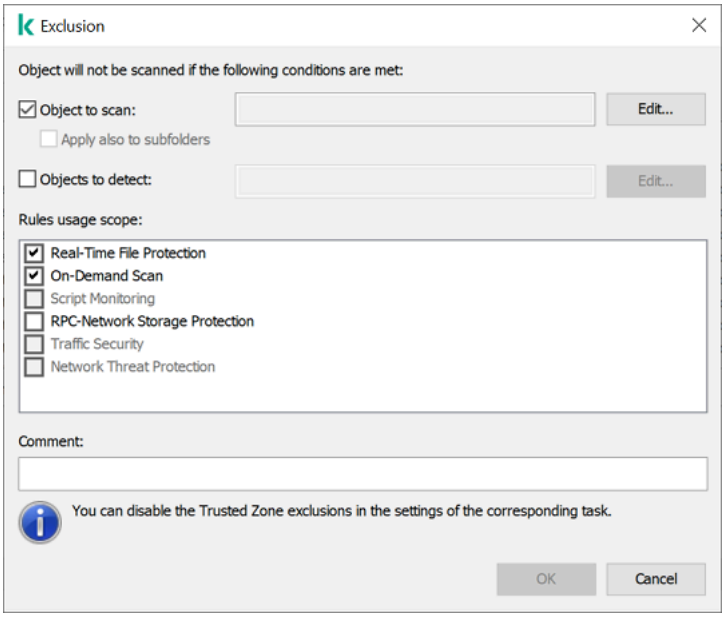
- Script file or web address: *no migra*.

  Después de la migración, debe agregar estas exclusiones manualmente. Las exclusiones como direcciones web de scripts deben agregarse a las direcciones web de confianza para la Protección contra amenazas web.

Si la casilla de verificación **Apply also to subfolders** está seleccionada para el objeto analizado, esta configuración se migra a las exclusiones de KES (la casilla de verificación **Incluir subcarpetas**).



Configuración de exclusión de KES



Configuración de exclusión 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 **Tipo del objeto detectado** seleccionado en sus propiedades. El nombre del objeto detectado corresponde con la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`). Kaspersky Endpoint Security admite máscaras con el signo de interrogación `?` (representa cualquier carácter) y el asterisco `*` (representa cualquier secuencia de caracteres).

Migración del alcance del uso de una exclusión

El alcance del uso de una exclusión es un conjunto de componentes al que se aplica la exclusión. KES y KSWS tienen diferentes conjuntos de componentes para que el asistente de migración no pueda migrar el alcance del uso de una exclusión. Por lo tanto, si se selecciona al menos un componente en el alcance del uso de KSWS, KES aplica la exclusión a todos los componentes de la aplicación.

Puede configurar el alcance del uso de KSWS en la configuración de la zona de confianza y también en la configuración de los componentes de protección de KSWS. Para hacerlo, puede seleccionar o desmarcar la casilla de verificación **Apply Trusted Zone** en la sección correspondiente de la directiva. La configuración de los componentes de protección de KES no incluye esta casilla de verificación. Esto significa que el estado de la zona de confianza en la configuración del componente individual se pierde tras la migración. Después de completar la migración, seleccione los componentes a los que se aplica la exclusión en la configuración de la zona de confianza en 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 modificaciones.

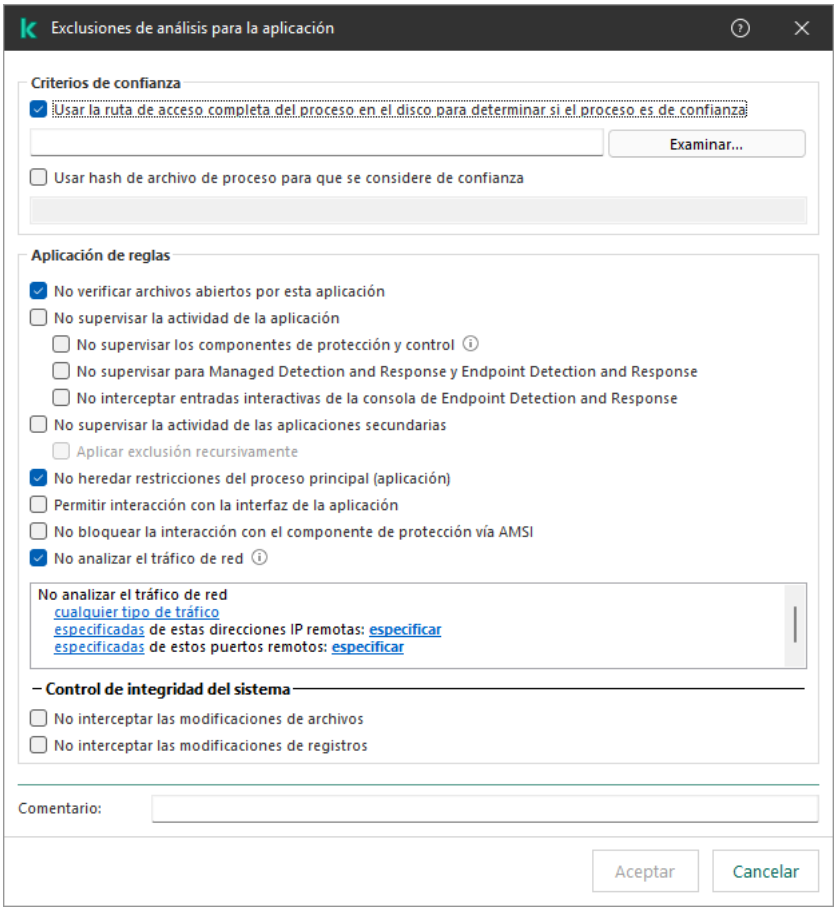
Migración de procesos de confianza

Los procesos de confianza de KSWS se migran a los procesos de confianza de KES con algunas limitaciones. La migración de procesos de confianza depende del método de selección del objeto:

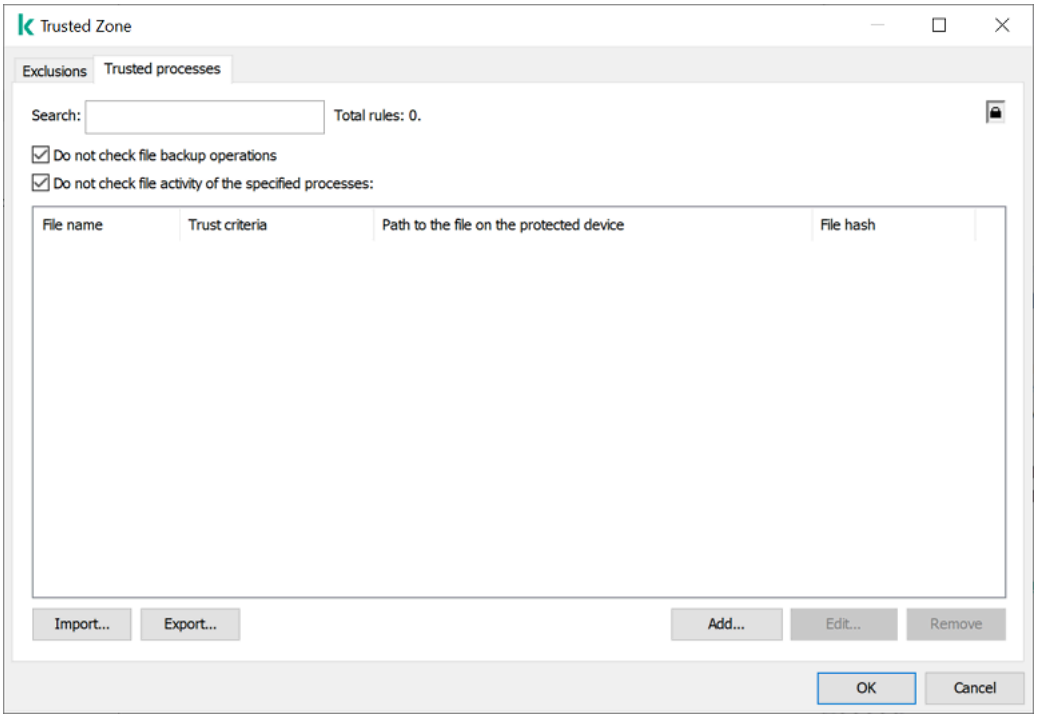
- Path to the file on the protected device: migra a las aplicaciones de confianza de KES.
- File hash: *no migra*.

Si KSWS tiene procesos de confianza configurados como un hash del archivo, dichos procesos de confianza no se migran. Después de la migración, debe agregar dichos procesos de confianza manualmente.

Si la casilla de verificación **Do not check file backup operations** está seleccionada en la configuración del proceso de confianza, esta configuración se migrará a las aplicaciones de confianza de KES (la casilla de verificación **No supervisar la actividad de la aplicación**).



Configuración de la aplicación de confianza de KES



Configuración del proceso de confianza de KSWS

Migración de las reglas de Control de inicio de aplicaciones de KSWS

Control de inicio de aplicaciones de KSWS está bloqueado de manera predeterminada. Es decir, 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 de Control de aplicaciones de KES establece automáticamente el modo de control **Lista de admitidos**, que corresponde al principio de bloqueo predeterminado.

Puede migrar las 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 basada en la directiva de KSWS*.

Migración del modo de Control de inicio de aplicaciones

El modo de Control de inicio de aplicaciones de KSWS se 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 forma predeterminada, el Control de lanzamiento de aplicaciones de KSWS tiene 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 con un certificado raíz de confianza. Si al menos una regla de KSWS predefinida tiene la configuración **Allow**, durante la migración, el asistente crea una nueva regla de autorización: **Aplicaciones con certificados raíz de confianza**. Es decir, Control de aplicaciones de KES utiliza una única regla para permitir la ejecución de scripts, paquetes MSI y archivos ejecutables de confianza.

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 manera diferente en KSWS y KES; por lo tanto, el asistente de migración crea *categorías de aplicaciones*, que incluyen condiciones y exclusiones de las reglas de KSWS, y agrega estas categorías de aplicaciones a las reglas de KES. El asistente usa las condiciones **Certificado**, **Ruta de acceso a carpeta** y **Hash del archivo** en las categorías de aplicaciones. 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 usuario. A continuación, el asistente crea categorías de aplicaciones que incluyen condiciones y exclusiones de las reglas de KSWS y agrega las categorías de aplicaciones 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

Los principios de operación de Control de inicio de aplicaciones de KSWS y Control de aplicaciones de KES son diferentes, 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)* No se puede configurar el alcance de la aplicación de reglas en la configuración de Control de aplicaciones de KES. Control de aplicaciones de KES aplica reglas a todo tipo de archivos: archivos ejecutables, scripts y paquetes MSI. Si se incluyen todos los tipos de archivos en el alcance de la aplicación de reglas en KSWS, durante la migración, KES transfiere las reglas a KSWS. Si se excluye algún tipo de archivo del alcance de la aplicación de reglas en KSWS, durante la migración, KES también transfiere las reglas a KSWS, pero se selecciona **Probar reglas** como acción de Control de aplicaciones.
Monitor loading of DLL modules	**Supervisar la carga de módulos DLL (aumenta 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)* No se puede configurar el alcance de la aplicación de reglas en la configuración de Control de aplicaciones de KES. Control de aplicaciones de KES aplica reglas a todo tipo de archivos: archivos ejecutables, scripts y paquetes MSI. Si se incluyen todos los tipos de archivos en el alcance de la aplicación de reglas en KSWS, durante la migración, KES transfiere las reglas a KSWS. Si se excluye algún tipo de archivo del alcance de la aplicación de reglas en KSWS, durante la migración, KES transfiere las reglas a KSWS, pero se selecciona **Probar reglas** como 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 agrega una nueva regla de autorización. Se especifica la categoría KL **Otro software\Aplicaciones, de confianza según su reputación en KSN** 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 según su reputación en KSN**.
Automatically allow software distribution via applications and packages listed	El control de distribución de software en KSWS y KES funciona de manera diferente. Durante la migración, KES agrega nuevas reglas de autorización para las aplicaciones que permiten la distribución automática de software. Se especifica el hash de archivo como condición de activación de reglas.
Always allow software distribution via Windows Installer	El control de distribución de software en KSWS y KES funciona de manera diferente. Durante la migración, KES agrega nuevas reglas de autorización para las aplicaciones que permiten la distribución automática de software (**Software distribution applications and packages allowed**). Se especifica el hash de archivo como condición de activación de reglas. En propiedades de la cuenta, la casilla de verificación **Actualizadores de confianza** está seleccionada.
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 de manera diferente. Durante la migración, KES agrega nuevas reglas de autorización para las aplicaciones que permiten la distribución automática de software. Se especifica el hash de archivo como condición de activación de reglas. En propiedades de la cuenta, la casilla de verificación **Actualizadores de confianza** está seleccionada.
Schedule settings	*(no migra)* Si se configura un programa para el componente en la configuración de KSWS, se habilita el componente Control de aplicaciones en la migración. Si no se configura un programa para el componente en la configuración de KSWS, se deshabilita Control de aplicaciones al momento de la migración. No es posible configurar una programación separada para el componente. El componente está siempre encendido mientras Kaspersky Endpoint Security está operativo.

Instalación de KES en lugar de KSWS

Puede instalar Kaspersky Endpoint Security de las siguientes maneras:

- Instalar KES después de eliminar KSWS (recomendado).
- Instalación de KES sobre KSWS.

Eliminar Kaspersky Security for Windows Server

Puede eliminar la aplicación de forma remota utilizando la tarea *Desinstalar aplicación de forma remota* 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 elimine 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 utilizó la utilidad kavremover. La utilidad kavremover no admite la gestión de KSWS.

Si Protección con contraseña está habilitada para restringir el acceso a KSWS, escriba la contraseña de desinstalación en la configuración del paquete de instalación de KES.

Después de eliminar KSWS, instale Kaspersky Endpoint Security para Windows mediante cualquier método disponible.

Instalar Kaspersky Endpoint Security

Cuando instala KES de forma remota, los componentes que seleccionó en 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 encontrar 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 la instalación de KES sobre KSWS falla, 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 mediante 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 mediante *Cambiar componentes de la aplicación*.

Migrar la configuración [KSWS+KEA] a la configuración [KES+agente incorporado]

Para permitir el uso de Kaspersky Endpoint Security para Windows como parte de EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA y MDR, se agregó 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 los agentes incorporados de Kaspersky Endpoint Security. Además, se eliminará Kaspersky Endpoint Agent del equipo.

Migrar la configuración [KSWS+KEA] a [KES+agente incorporado] incluye los siguientes pasos:

1. **Migración de KSWS a KES**

   Migrar de KSWS a KES implica instalar Kaspersky Endpoint Security en lugar de Kaspersky Security for Windows Server.

   Los administradores suelen habilitar la protección con contraseña para restringir el acceso a KSWS y KEA. A partir de Kaspersky Security Center Linux 15.1, puede ingresar la contraseña de desinstalación de la aplicación en la configuración de la tarea *Instalar aplicación de forma remota*. La tarea permite ingresar solo una contraseña de desinstalación. Es decir, si se configura la misma contraseña para KSWS y KEA, las aplicaciones KSWS y KEA se eliminarán correctamente. Si las contraseñas son diferentes, la eliminación de una de las aplicaciones generará un error de acceso. Para completar la migración, debe deshabilitar la Protección con contraseña para la aplicación cuya contraseña no pudo escribir en la configuración de la tarea *Instalar aplicación de forma remota*.

   Para realizar la migración, debe seleccionar los componentes necesarios para admitir las soluciones de Detection and Response como parte de Kaspersky Endpoint Security. Luego de instalar la aplicación, Kaspersky Endpoint Security pasa a usar el agente incorporado y elimina Kaspersky Endpoint Agent.

2. **Migrar las directivas y tareas**

   Migrar las directivas y tareas [KSWS+KEA] a [KES+agente incorporado] incluye 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, un perfil de directiva con el nombre *UpgradedFromKSWS<Nombre de la directiva Kaspersky Security for Windows Server>* se agrega a la directiva de KES. También se crean nuevas tareas de KES con los nombres *<nombre de la tarea KSWS> (convertido)*.

   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> y <Nombre de la directiva de Kaspersky Endpoint Agent>*. También se crean nuevas tareas y tareas de KES.

3. **Funcionalidad de licencia**

   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 luego de actualizar la aplicación a la versión 11.7.0. No necesita realizar ninguna otra acción.

   Si utiliza una licencia independiente de complemento Kaspersky Endpoint Detection and Response Optimum para activar la funcionalidad EDR Optimum, debe asegurarse de que la clave de complemento EDR Optimum se agregue al repositorio de Kaspersky Security Center y de que la funcionalidad de distribución automática de claves de licencia esté habilitada. Luego 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 *Agregar clave*.

No necesita activar la funcionalidad de Kaspersky Sandbox. Kaspersky Sandbox estará disponible de forma inmediata luego de la actualización y activación de 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. Luego 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**

   Luego de la actualización, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

   - Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.
   - El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes 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 de EDR Optimum esté activada mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de que la funcionalidad de distribución automática de claves de licencia de EDR Optimum esté activada.

Asegúrese de que Kaspersky Security for Windows Server se haya eliminado con éxito

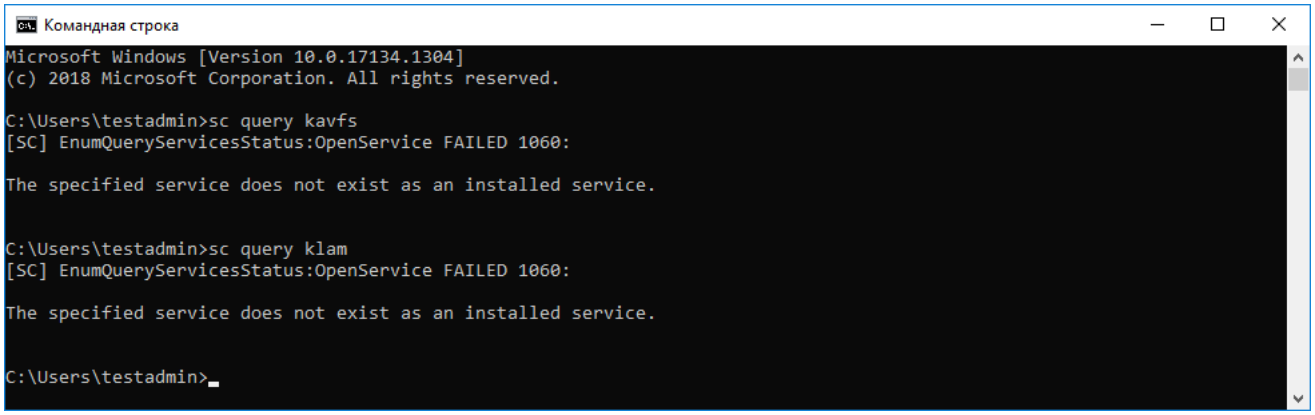
Asegúrese de que Kaspersky Security for Windows Server esté completamente eliminado:

- La carpeta `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` no existe.
- Los siguientes servicios no están disponibles:
  - Kaspersky Security Service (KAVFS)
  - Servicio de Kaspersky Security Management (KAVFSGT)
  - Servicio de Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Servicio de Kaspersky Security Script Checker (KAVFSSCS)

  Puede verificar los servicios en ejecución en el Administrador de tareas o al emitir el comando `sc query` (ver 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 al emitir 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 hayan eliminado correctamente

Si los archivos de la aplicación o del controlador permanecen en el servidor, elimine los archivos relevantes 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`.

Activar KES con una clave de KSWS

Después de instalar la aplicación, puede activar Kaspersky Endpoint Security para Windows (KES) utilizando 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 admite la *licencia de Kaspersky Security for Storage*. Para trabajar con esta licencia, debe utilizar Kaspersky Security for Windows Server.

Si desea activar KES con una clave KSWS, puede utilizar solo el código de activación. Si utiliza un archivo de clave para activar la aplicación, debe comunicarse con Soporte técnico para obtener un archivo de clave de Kaspersky Endpoint Security.

Método de activación de Kaspersky Security for Windows Server	Migrar la clave a Kaspersky Endpoint Security para Windows.
Distribución automática de la clave de licencia de KSWS a los equipos.	Si la distribución automática de claves está habilitada en las propiedades de la clave de licencia de KSWS, KES se activa automáticamente con la clave de KSWS.
La clave KSWS se agrega mediante una tarea.	Si su KSWS se activa mediante la tarea, la clave de licencia de KSWS se elimina durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede agregar una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.
La clave KSWS se agrega 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 elimina durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede agregar una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.
La clave KSWS se agrega al paquete de instalación.	Si su KSWS se activa con la clave del paquete de instalación, la clave de licencia de KSWS se elimina durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede agregar una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.
Imagen de máquina virtual paga (Imagen de máquina de Amazon – AMI) en Amazon Web Services (AWS).	Si compró Kaspersky Security Center como una imagen de máquina virtual paga (Imagen de máquina de Amazon – AMI) en Amazon Web Services (AWS), no es necesario activar KES. En este caso, Kaspersky Security Center usa la suscripción de AWS que ya se agregó a la aplicación.
Imagen gratuita de Kaspersky Security Center lista para usar con su propia licencia (Licencias adquiridas por el usuario – modelo BYOL).	Si está utilizando una imagen gratuita de Kaspersky Security Center lista para usar con su propia licencia en un entorno de nube (el modelo Licencias adquiridas por el usuario – BYOL), debe activar la aplicación usando cualquier método disponible. Necesitará una licencia de Kaspersky Hybrid Cloud Security.

Consideraciones especiales para migrar servidores de alta carga

En servidores de alta carga, es importante supervisar el rendimiento y evitar fallas. Después de la migración a Kaspersky Endpoint Security para Windows, recomendamos deshabilitar temporalmente los componentes de la aplicación que utilizan una cantidad sustancial de recursos del servidor en relación con otros componentes. Después de asegurarse de que el servidor funcione con normalidad, puede volver a habilitar los componentes de la aplicación.

Recomendamos migrar servidores de alta carga de la siguiente manera:

1. Cree una directiva de Kaspersky Endpoint Security con la configuración predeterminada.

   Los ajustes predeterminados se consideran óptimos. Esta configuración está recomendada por los expertos de Kaspersky. La configuración predeterminada proporciona el nivel de protección recomendado y el uso óptimo de los recursos.

2. En la configuración de la directiva, deshabilite los siguientes componentes: Protección contra amenazas de red, Detección de comportamiento, Prevención de exploits, Motor de reparación, 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. Revise la configuración de la aplicación:
   - La aplicación se activa con la clave de licencia de KSWS.
   - Se aplica la nueva directiva. Los componentes seleccionados previamente están deshabilitados.
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 es necesario, cree exclusiones de análisis, agregue 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 contra amenazas de 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 modo de prueba de reglas.
11. Asegúrese de que Control de aplicaciones esté funcionando. Si es 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 funcione correctamente. Verifique el estado del servidor en la consola (debe ser *Aceptar*). Asegúrese de que no se informen errores para la aplicación, también verifique 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.

Cómo administrar la aplicación desde 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.

Cómo administrar la aplicación con la consola de Kaspersky Security Center

Instalar la aplicación usando la consola de Kaspersky Security Center no es diferente de una instalación normal. Al crear un paquete de instalación, puede agregar 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 contra amenazas web, Protección contra amenazas de correo, Control web, Prevención de ataques BadUSB, Cifrado de archivos (FLE), Cifrado de disco de Kaspersky (FDE).

No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. 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 en los informes desde la consola de Kaspersky Security Center.

Administrar la aplicación en un 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 un servidor en modo Server Core implica las siguientes consideraciones especiales:

- El servidor en modo Server Core no tiene una GUI; 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 habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación y habilitar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis de malware*. A continuación, debe iniciar la tarea *Análisis de malware*.

- 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 habilitado el modo de compatibilidad con el Estándar federal de procesamiento de información (FIPS), conecte 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
```

Migrar de [KSWS+KEA] a [KES+agente incorporado]

Al migrar de Kaspersky Security for Windows Server (KSWS) a Kaspersky Endpoint Security (KES), puede usar las siguientes recomendaciones para configurar la protección del servidor y optimizar el rendimiento. A continuación, se puede ver 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). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) también se despliega

  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 administrado por su propia directiva. Se crean tareas de *Database Update* y *On-demand scan* 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 habilitada.

- 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 está administrado por la directiva *Exchange_Policy* directiva. También se crean las tareas *Database Update*, *On-demand scan*.

Planificación de la migración

La migración implica los siguientes pasos:

1. Migrar 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. Confirmar que KES está funcionando.

El escenario de migración se realiza inicialmente en uno de los clústeres de servidores SQL. Luego, el escenario de migración se realiza en el otro clúster de servidores SQL. Luego, el escenario de migración se realiza en Microsoft Exchange.

Migrar tareas y directivas de KSWS mediante el Asistente de conversión por lotes de directivas y tareas

Para migrar tareas de KSWS, solo puede utilizar 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 sola 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 la etiqueta del 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 tareas de Kaspersky Endpoint Agent puede utilizar 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 directiva 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 del perfil de directiva* como condición de activación del perfil.

Instalación de KES en lugar de KSWS

Antes de instalar KES, debe deshabilitar 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. Crear una tarea *Instalar aplicación de forma remota* 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 con éxito.

5. Repita la instalación de KES para los grupos de administración restantes.

Kaspersky Security Center agrega automáticamente la etiqueta `UpgradedFromKSWS` a los nombres de las computadoras en la consola una vez que se completa la instalación de KES.

Para comprobar la instalación de KES, puede utilizar el *Informe del despliegue de la protección*. También puede comprobar el estado del dispositivo. Para confirmar la activación de la aplicación, puede utilizar el *Informe de uso de claves de licencia*.

Activación de EDR Optimum

Puede activar la funcionalidad EDR Optimum mediante una licencia independiente del complemento Kaspersky Endpoint Detection and Response Optimum. Debe confirmar que la clave de EDR Optimum se agrega al repositorio de Kaspersky Security Center y que la funcionalidad de distribución automática de claves de licencia está habilitada.

Para verificar la activación de EDR Optimum, puede usar el *Informe sobre el estado de los componentes de la aplicación*.

Confirmar que KES está funcionando

Para confirmar que KES está funcionando, puede verificar y ver que no se informen errores. El estado del dispositivo debe ser *Aceptar*. Tareas de actualización y análisis de malware completadas con éxito.

Modo de 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 brinda protección integral a 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 el modo de 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 de Light Agent como parte de Kaspersky Security for Virtualization Light Agent a partir de la versión 6.2.

Cuando inicia Light Agent, se establece y mantiene una conexión con la máquina virtual SVM (Secure Virtual Machine). Se implementa un Servidor de protección en la SVM. 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 (la tecnología de SharedCache). Esta tecnología aumenta la eficiencia de la solución y ofrece 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 Agent, participa en la detección de SVM por parte de Light Agent, protege la conexión entre Light Agent y SVM, y realiza otras funciones.

Consideraciones especiales para el modo de Light Agent

Puede administrar Kaspersky Endpoint Security en el modo estándar y el modo de Light Agent mediante las directivas y tareas de Kaspersky Endpoint Security. En el modo de Light Agent, algunos componentes y características de la aplicación no están disponibles.

Actualización de bases de datos y módulos de software de la aplicación

Kaspersky Endpoint Security en modo de 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 las bases de datos y los módulos de la aplicación del Servidor de protección.

Las bases de datos y los módulos de las máquinas virtuales protegidas se actualizan mediante una tarea *Actualización de bases de datos y módulos de la aplicación* especial, en la que se especifica una carpeta en la SVM como el origen de las actualizaciones. Light Agent ejecuta la tarea *Actualización de bases de datos y módulos de la aplicación* automáticamente. No puede seleccionar un origen de actualizaciones diferente, configurar la programación de la tarea ni eliminar la tarea.

La reversión de la última actualización de la base de datos de malware también se gestiona en el Servidor de protección. Después de la reversión de una actualización de bases de datos y módulos de la aplicación en la SVM, se inicia una tarea *Actualización de bases de datos y módulos de la aplicación* local especial en la máquina virtual protegida. Esta tarea hace que el Light Agent vuelva a usar el conjunto anterior de bases de datos de malware.

Kaspersky Endpoint Security en modo de Light Agent no es compatible con la tarea *Reversión de la actualización*.

Activar Light Agent

Para activar la aplicación, debe agregar una clave de licencia a la SVM a la que está conectado el Light Agent. No es necesario activar la aplicación por separado.

Otras consideraciones especiales para el modo de Light Agent

- Si crea una directiva para la aplicación, recomendamos seleccionar el modo de Light Agent. En este modo, el Asistente de nueva directiva le solicita que configure la conexión SVM. Esta configuración es necesaria para que la aplicación funcione en el modo de Light Agent.
- No puede instalar los componentes Cifrado de datos y Control de anomalías adaptativo en el modo de Light Agent. El conjunto de componentes también depende del tipo de sistema operativo huésped: 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 en Kaspersky Security Center Web Console. No es posible usar Kaspersky Security Center Cloud Console para administrar Light Agent.
- 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 nube de Kaspersky Security Network.
- No se admite el uso del servidor proxy de la aplicación para la conexión con el Servidor de integración (VIIS), el Servidor de protección (SVM) y los servidores de KSN.

Configuración preliminar de la máquina virtual

Puede instalar Kaspersky Endpoint Security en una máquina virtual que utiliza tecnología de plataforma virtual. Kaspersky Endpoint Security admite las plataformas virtuales de 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 Full User Layer para guardar el estado de las máquinas virtuales temporales, debe hacer lo siguiente antes de instalar en la plantilla de máquinas virtuales:

1. Cree el archivo C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt y agregue 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 DWORD llamado MiniFilterBypass y establézcalo en 1.

3. En el registro del sistema operativo, en la clave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, cree un nuevo valor MULTI_SZ llamado ExcludeKey y establézcalo en \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Reinicie la máquina virtual.

Para la instalación en máquinas virtuales en una infraestructura que utiliza 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 la aplicación.

2. Cree una imagen de máquina virtual que consta 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 de 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 sea 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 información, visite el Sitio web de soporte técnico de Citrix). Después de instalar la aplicación, debe instalar Citrix Provisioning Target Device.

- Al instalar la aplicación con el asistente de configuración o Kaspersky Security Center de forma remota, debe seleccionar la casilla de verificación **Garantizar la compatibilidad con Citrix PVS**.

Compatibilidad con la tecnología de Omnissa App Volumes

Antes de instalar en la plantilla de máquinas virtuales, debe crear el archivo %SVAgent%\Config\Custom\snapvol.cfg y agregar 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 obtener más detalles, consulte la documentación de Omnissa.

Instalar 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 de Light Agent es la misma que en el modo estándar. Antes de instalar Light Agent en una máquina virtual, debe asegurarse de que el Agente de red de Kaspersky Security Center esté instalado. El *Agente de red* facilita la interacción entre el Servidor de administración y una máquina virtual.

Light Agent se puede instalar en una máquina virtual de varias maneras:

- De manera remota, a través de Kaspersky Security Center.
- De manera local con el Asistente de instalación.
- De manera local con 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 instalación.

Al instalar Light Agent en un servidor, los componentes de protección avanzada (Detección de comportamiento, Prevención de exploits, Motor de reparación) se excluyen de la configuración predeterminada de la aplicación. La configuración predeterminada de la aplicación brinda el nivel de protección recomendado y un 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.

Durante la instalación de Light Agent, recomendamos seleccionar exclusiones y aplicaciones de confianza predefinidas para el entorno virtual relevante. Las exclusiones de análisis y aplicaciones de confianza predefinidas permiten 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.

Durante la instalación de Light Agent en máquinas virtuales persistentes, es posible que deba modificar el algoritmo de generación Sensor ID. Sensor ID se utiliza en la solución Kaspersky Anti Targeted Attack Platform para identificar los equipos que envían telemetría al servidor. Para crear un Sensor ID único, configure `EnableUniqueSensorID=1` al instalar la aplicación en la línea de comandos.

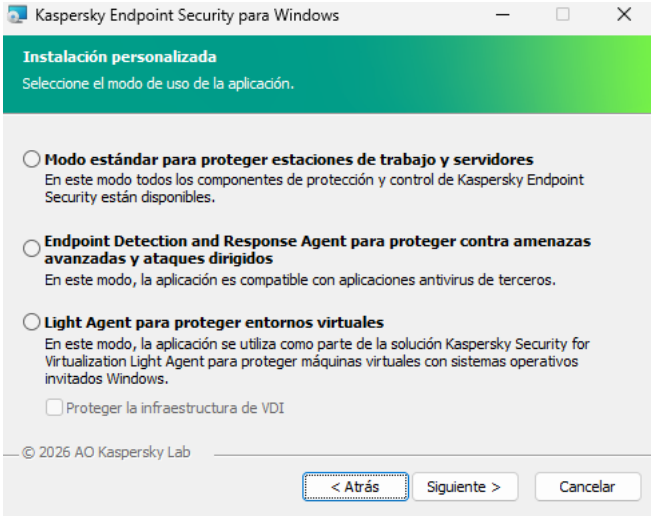
Cómo instalar Light Agent con el Asistente de configuración

1. Copie la carpeta del kit de distribución en la máquina virtual.

2. Ejecute setup_kes.exe.

   Se inicia el Asistente de instalación.

Configuración de Kaspersky Endpoint Security



Elegir la configuración de la aplicación

Seleccione la configuración de **Light Agent para proteger entornos virtuales**. Esta configuración está pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

Componentes de Kaspersky Endpoint Security

Seleccione los componentes que desea instalar (consulte la figura a continuación). Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles. Para ello, deberá ejecutar el Asistente de instalación nuevamente y seleccionar la opción que permite cambiar los componentes disponibles.

La configuración avanzada

Configuración avanzada de la instalación de la aplicación

Proteger el proceso de instalación de la aplicación. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda deshabilitar 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.

Agregar la ruta del archivo avp.com a la variable del sistema %PATH%. Puede agregar la ruta de instalación a la variable %PATH% para facilitar el uso de la interfaz de línea de comandos.

Cómo instalar Light Agent con la línea de comandos

1. Abra el símbolo del sistema (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

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   La opción `VDI` habilita el modo de protección de la VDI (Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen 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 la VDI está deshabilitado.

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 con el archivo setup.ini. También puede especificar la configuración de instalación en la línea de comandos.

Cómo instalar Light Agent con 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**.

   Se abre una lista con los 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 es 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 pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

6. Seleccione los componentes que desea instalar.

   Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles.

7. Configure la zona de confianza. Seleccione las 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 permiten configurar rápidamente la aplicación y evitar problemas de compatibilidad con el entorno virtual.

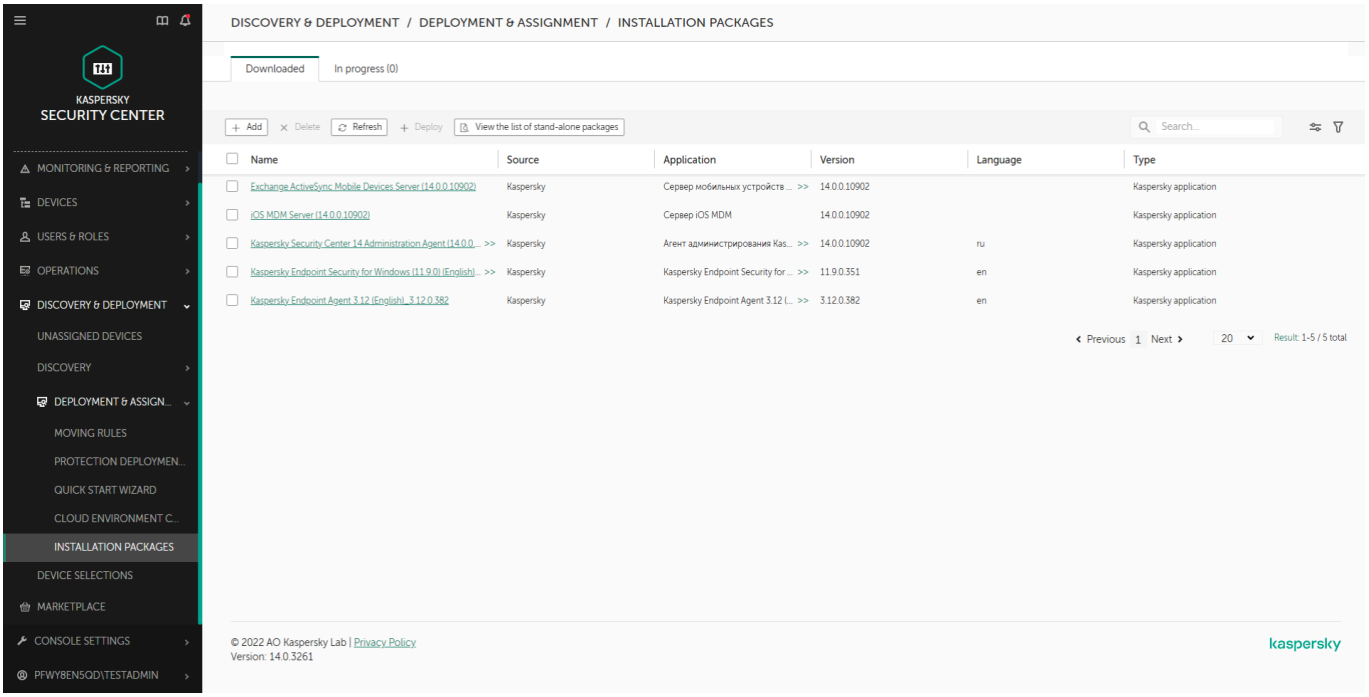
8. Guarde los cambios.

9. Crear una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que creó.

Cómo instalar Light Agent con Web Console

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

Se abre una lista con los paquetes de instalación que se han descargado a Kaspersky Security Center.



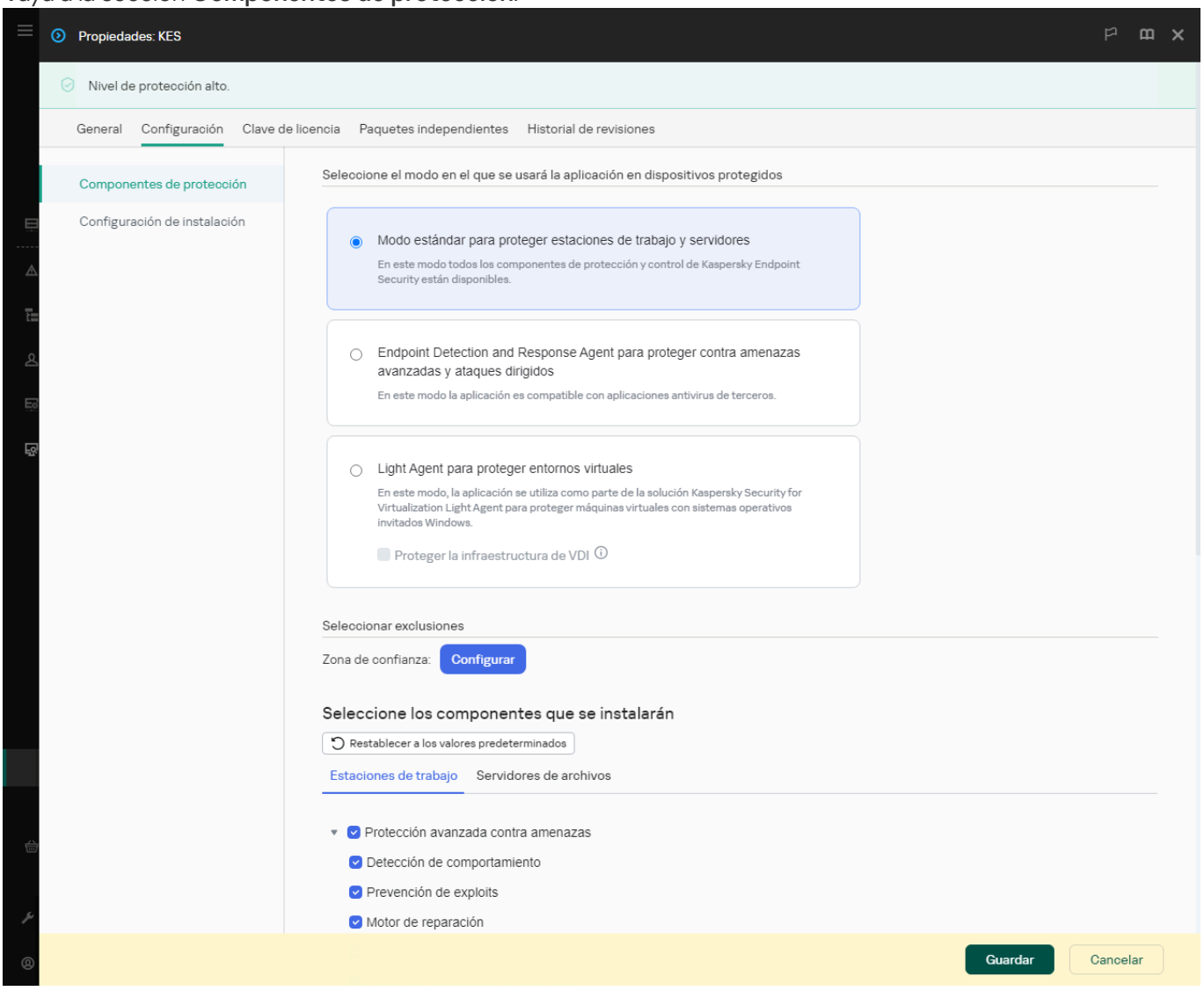
Lista de paquetes de instalación

2. Abra las propiedades del paquete de instalación de Kaspersky Endpoint Security para Windows.

   Si es necesario, cree un nuevo paquete de instalación.

3. Seleccione la ficha **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 pensada para 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 usar los componentes Cifrado de datos ni 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 de verificación **Proteger la infraestructura de VDI** (VDI significa Virtual Desktop Infrastructure). El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. En este modo, Light Agent rechaza las actualizaciones de la aplicación que exigen reiniciar la máquina virtual. Al recibir actualizaciones de la aplicación que exigen un reinicio, Light Agent genera un evento sobre la necesidad de actualizar la plantilla de las máquinas virtuales protegidas.

6. Seleccione los componentes que desea instalar.

   Una vez que haya instalado la aplicación, podrá modificar la selección de componentes disponibles.

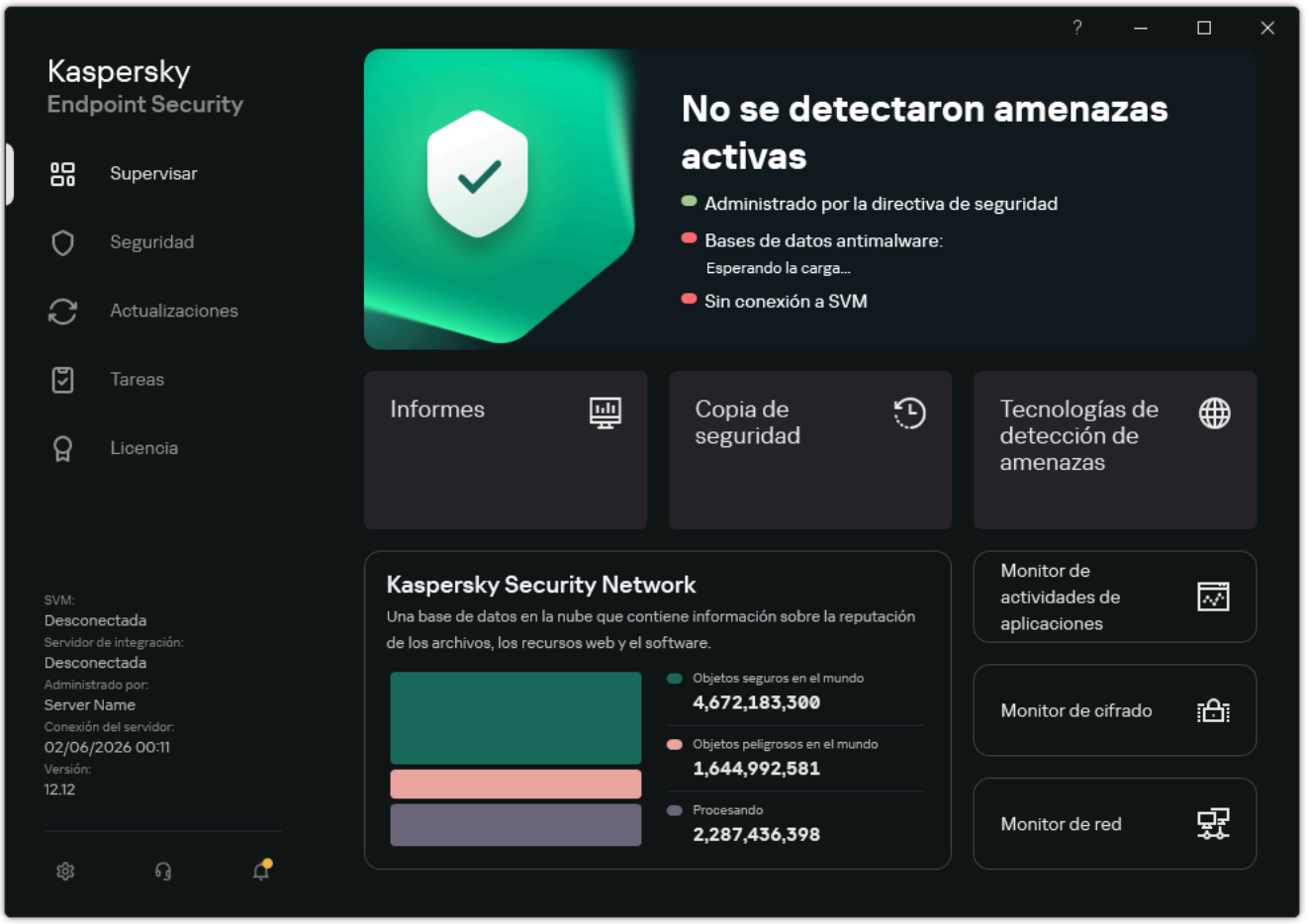
7. Configure la zona de confianza. Seleccione las exclusiones de análisis y aplicaciones de confianza predefinidas para el entorno virtual en el que está instalando la aplicación.

   Las exclusiones de análisis y aplicaciones de confianza predefinidas permiten configurar rápidamente la aplicación y evitar problemas de compatibilidad con el entorno virtual.

8. Guarde los cambios.

9. Crear una tarea de instalación remota. En las propiedades de la tarea, seleccione el paquete de instalación que creó.

Como consecuencia, Light Agent se instala en la máquina virtual. Puede utilizar la interfaz de la aplicación, y se muestra un ícono de la aplicación en el área de notificaciones . Ahora necesita configurar la conexión del Light Agent a la SVM.



Ventana principal de Light Agent

Conectar Light Agent a SVM

La solución Kaspersky Security for Virtualization Light Agent requiere una comunicación continua entre el Light Agent y la SVM. Esto es necesario para analizar los archivos enviados por el Light Agent en busca de virus y otro malware. Sin una conexión con la 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 sea 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 la SVM.

Puede obtener información sobre el estado de la conexión del Light Agent a la SVM en Kaspersky Endpoint Security o con el comando de la aplicación. La aplicación genera un evento cada vez que se pierde o se establece la conexión de la SVM del Light Agent 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 más información sobre la supervisión del estado de la 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:

- Uso del Servidor de integración (VIIS).

  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 es más útil en infraestructuras virtuales grandes porque equilibra automáticamente la carga entre las SVM, obtiene información sobre las SVM disponibles, analiza esta información y proporciona a los Light Agent una lista de Servidores de protección (SVM) que son óptimos para la conexión.

  Para que el Light Agent pueda obtener una lista de SVM, solo necesita ingresar la dirección del Servidor de integración.

- Uso de la lista de direcciones de SVM.

  Si necesita especificar SVM individuales a las que desee que el Light Agent se conecte, puede preparar una lista manualmente.

  Debe enumerar las direcciones de SVM disponibles a las que el Light Agent puede conectarse.

Cómo configurar la detección de la SVM de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Modo de Light Agent** → **Configuración de detección de la SVM**.

4. Seleccione un método de detección de la SVM.

   - **Usar el Servidor de integración**. Ingrese la configuración de la conexión al Servidor de integración. Ingrese la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) del dispositivo en el que está instalado el Servidor de integración.

   - **Usar una lista personalizada de direcciones de SVM**. Cree una lista de SVM a las que el Light Agent puede conectarse. Especifique la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) de SVM. Cada elemento de la lista debe ingresarse en una línea nueva 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 generar errores en la solución.

5. Guarde los cambios.

Cómo configurar la detección de la SVM de 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 ficha **Configuración de la aplicación**.

4. Vaya a **Modo de Light Agent** → **Configuración de detección de la SVM**.

5. Seleccione un método de detección de la SVM.

   - **Usar el Servidor de integración**. Ingrese la configuración de la conexión al Servidor de integración. Ingrese la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) del dispositivo en el que está instalado el Servidor de integración.

   - **Usar una lista personalizada de direcciones de SVM**. Cree una lista de SVM a las que el Light Agent puede conectarse. Especifique la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) de SVM. Cada elemento de la lista debe ingresarse en una línea nueva 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 generar errores en la solución.

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

Cómo configurar la detección de la SVM de Light Agent en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, en **Modo de Light Agent** haga clic en el ícono **Configuración de detección de la SVM**.

3. Seleccione un método de detección de la SVM.

   - **Usar el Servidor de integración**. Ingrese la configuración de la conexión al Servidor de integración. Ingrese la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) del dispositivo en el que está instalado el Servidor de integración.

   - **Usar una lista personalizada de direcciones de SVM**. Cree una lista de SVM a las que el Light Agent puede conectarse. Especifique la dirección IP en formato IPv4 o el nombre de dominio completo (FQDN) de SVM. Cada elemento de la lista debe ingresarse en una línea nueva 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 generar errores en la solución.

4. Guarde los cambios.

Configurar el algoritmo de selección de SVM para Light Agent

La infraestructura de la organización puede tener múltiples SVM implementadas a las que los Light Agents pueden conectarse. Para equilibrar la carga en la red y los recursos de la infraestructura virtual, debe distribuir los Light Agents entre las SVM.

Los Light Agents pueden aplicar los siguientes algoritmos de selección de SVM para la conexión:

Algoritmo estándar (predeterminado)

Si se aplica este algoritmo, después de la instalación y el inicio, el Light Agent en la máquina virtual elige conectarse a una SVM *local* con respecto al Light Agent.

El hecho de que una SVM se considere local para Light Agent depende del tipo de infraestructura virtual:

- En una infraestructura virtual basada en Basis Dynamix Enterprise, la SVM que se considera local en relación con Light Agent es la SVM implementada en el mismo nodo que la máquina virtual con Light Agent instalado.

- 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 en relación con Light Agent es la SVM implementada en el mismo hipervisor que la máquina virtual con Light Agent instalado.

- En una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud, puede especificar cómo se determina la localidad de la SVM en relación con Light Agent mediante el parámetro `StandardAlgorithmSvmLocality` en la sección `HypervisorSpecificSettings:Openstack` del archivo de configuración appsettings.json del Servidor de integración. Según 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 tomar los siguientes valores:

- `ServerGroup` – si se selecciona este valor, la SVM se considera local en relación con Light Agent si se encuentra dentro del mismo grupo del servidor que la máquina virtual donde está instalado Light Agent. Este valor se utiliza de forma predeterminada.

- `Project` – si se selecciona este valor, la SVM se considera local en relación con Light Agent si está implementada dentro del mismo proyecto OpenStack que la máquina virtual con Light Agent instalado.

- `AvailabilityZone` – si se selecciona este valor, la SVM se considera local en relación con Light Agent si se encuentra dentro de la misma zona de disponibilidad que la máquina virtual con Light Agent instalado.

Si no hay SVM locales disponibles para la conexión, Light Agent selecciona la SVM con la menor cantidad de Light Agents conectados, independientemente de la ruta de la SVM en la infraestructura virtual.

> La aplicación no determina si la SVM es local en relación con Light Agent si el modo de protección de infraestructura de gran tamaño está habilitado para el Servidor de protección en la SVM. En este caso, se recomienda usar el algoritmo de selección de SVM extendido y seleccionar el Servidor de integración como método de descubrimiento de SVM.

Algoritmo extendido

Si se aplica este algoritmo, puede definir los siguientes parámetros de selección de SVM:

- si se debe tener en cuenta o ignorar la ubicación de las SVM en la infraestructura al elegir las SVM para la conexión

- si se tiene en cuenta la ubicación de las SVM, el método para determinar la localidad de la SVM en relación con Light Agent

Si los Light Agents ignoran la ubicación de las SVM en la infraestructura, 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 SVM que se tendrá en cuenta al determinar si una SVM es local en relación con Light Agent. El hecho de que una SVM se considere local para Light Agent depende del tipo de infraestructura virtual.

En una infraestructura virtual basada en Basis Dynamix Enterprise, una SVM puede considerarse local en relación con Light Agent en cualquiera de los siguientes casos:

- Una SVM está implementada en el mismo nodo que la máquina virtual con Light Agent instalado.

- Una SVM está implementada en la misma zona que la máquina virtual con Light Agent instalado.

- Una SVM está implementada en el mismo centro de datos que la máquina virtual con Light Agent instalado.

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 en relación con Light Agent en cualquiera de los siguientes casos:

- Una SVM está implementada en el mismo hipervisor que la máquina virtual con Light Agent instalado.

- Una SVM está implementada en el mismo clúster de hipervisor que la máquina virtual con Light Agent instalado.

- Una SVM está implementada en el mismo centro de datos que la máquina virtual con Light Agent instalado.

En una infraestructura virtual que se ejecuta en la plataforma OpenStack o VK Private Cloud, una SVM puede considerarse local en relación con Light Agent en cualquiera de los siguientes casos:

- Una SVM se encuentra en el mismo grupo del servidor que la máquina virtual con Light Agent instalado.
- Una SVM está implementada en el mismo proyecto OpenStack que la máquina virtual con Light Agent instalado.
- Una SVM se encuentra en la misma zona de disponibilidad que la máquina virtual con Light Agent instalado.

Si los Light Agents consideran la ubicación de las SVM en la infraestructura al elegir a qué SVM conectarse, solo pueden conectarse a las SVM que son locales.

Por ejemplo, si especifica clúster de hipervisores como tipo de ruta de SVM, todas las SVM implementadas en este clúster de hipervisores se considerarán locales en relación con Light Agent, y Light Agent solo podrá conectarse a una de estas SVM. Si no hay SVM disponibles para la conexión en el mismo clúster en el que se ejecuta Light Agent, Light Agent no se conecta a una SVM.

Al seleccionar las SVM, los Light Agents también consideran la cantidad de Light Agents conectados para garantizar que los Light Agents se distribuyan uniformemente entre las SVM disponibles para la conexión.

Si un Light Agent utiliza el algoritmo de selección de SVM extendido, se selecciona una lista de direcciones de SVM como método de detección de SVM y el modo de protección de infraestructura grande está habilitado en una SVM, solo es posible conectar un Light Agent a esta SVM si se ignora la ruta de la SVM.

Además de los algoritmos de conexión de SVM, puede regular la conexión de los Light Agents a las SVM mediante etiquetas.

Cómo configurar el algoritmo de selección de SVM para el Light Agent 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Modo de Light Agent** → **Algoritmo de selección de SVM**.
4. Seleccione el algoritmo:
   - **Usar el algoritmo de selección estándar de SVM**. El Light Agent selecciona las SVM implementadas en el mismo hipervisor.
   - **Usar el algoritmo de selección de SVM extendido**. El Light Agent selecciona las SVM implementadas en el tipo de ruta de SVM seleccionado (de manera predeterminada, **Hipervisor**).

5. Si es necesario, seleccione la ruta de SVM para el algoritmo de selección de SVM extendido:

- **Hipervisor**. Para la conexión, el Light Agent selecciona una SVM que coincide con un criterio particular (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo hipervisor que la máquina virtual que tiene Light Agent instalado (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 del servidor que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de Basis Dynamix Enterprise).

  Si no hay SVM disponibles 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**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo clúster de hipervisores que la máquina virtual con Light Agent instalado (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 implementan en el mismo proyecto OpenStack que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de Basis Dynamix Enterprise).

  Si no hay SVM disponibles para la conexión en el mismo clúster de hipervisor o dentro del 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**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo centro de datos que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de 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**. El Light Agent ignora la ruta de SVM para conectarse al Servidor de protección. Los Light Agents tienen en cuenta otros criterios: etiquetas, cantidad de Light Agents conectados a una SVM, etc.

6. Guarde los cambios.

Cómo configurar el algoritmo de selección de SVM para el 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 ficha **Configuración de la aplicación**.
4. Vaya a **Modo de Light Agent** → **Algoritmo de selección de SVM**.
5. Seleccione el algoritmo:

   - **Usar el algoritmo de selección de SVM estándar**. El Light Agent selecciona las SVM implementadas en el mismo hipervisor.
   - **Usar el algoritmo de selección de SVM extendido**. El Light Agent selecciona las SVM implementadas en el tipo de ruta de SVM seleccionado (de manera predeterminada, **Hipervisor**).
6. Si es necesario, seleccione la ruta de SVM para el algoritmo de selección de SVM extendido:

   - **Hipervisor**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

     - Las SVM se implementan en el mismo hipervisor que la máquina virtual que tiene Light Agent instalado (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 del servidor que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de Basis Dynamix Enterprise).

     Si no hay SVM disponibles 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**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo clúster de hipervisores que la máquina virtual con Light Agent instalado (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 implementan en el mismo proyecto OpenStack que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de Basis Dynamix Enterprise).

  Si no hay SVM disponibles para la conexión en el mismo clúster de hipervisor o dentro del 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**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo centro de datos que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de 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**. El Light Agent ignora la ruta de SVM para conectarse al Servidor de protección. Los Light Agents tienen en cuenta otros criterios: etiquetas, cantidad de Light Agents conectados a una SVM, etc.

7. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar el algoritmo de selección de SVM para el Light Agent en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, en **Modo de Light Agent** haga clic en el ícono **Configuración de detección de la SVM**.

3. Seleccione el algoritmo:

   - **Usar el algoritmo de selección de SVM estándar**. El Light Agent selecciona las SVM implementadas en el mismo hipervisor.

   - **Usar el algoritmo de selección de SVM extendido**. El Light Agent selecciona las SVM implementadas en el tipo de ruta de SVM seleccionado (de manera predeterminada, **Hipervisor**).

4. Si es necesario, seleccione la ruta de SVM para el algoritmo de selección de SVM extendido:

- **Hipervisor**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo hipervisor que la máquina virtual que tiene Light Agent instalado (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 del servidor que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de Basis Dynamix Enterprise).

  Si no hay SVM disponibles 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**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo clúster de hipervisores que la máquina virtual con Light Agent instalado (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 implementan en el mismo proyecto OpenStack que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de Basis Dynamix Enterprise).

  Si no hay SVM disponibles para la conexión en el mismo clúster de hipervisor o dentro del 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**. Light Agent selecciona una SVM para conectarse a ella que cumpla con los criterios (según el tipo de infraestructura virtual):

  - Las SVM se implementan en el mismo centro de datos que la máquina virtual con Light Agent instalado (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 con Light Agent instalado (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 con Light Agent instalado (en la infraestructura virtual de 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**. El Light Agent ignora la ruta de SVM para conectarse al Servidor de protección. Los Light Agents tienen en cuenta otros criterios: etiquetas, cantidad de Light Agents conectados a una SVM, etc.

5. Guarde los cambios.

Distribuir las conexiones de los Light Agents a las SVM (etiquetas)

Se pueden conectar varios Light Agents a una SVM. Para equilibrar las conexiones del Light Agent, puede especificar una lista separada de SVM. Si está utilizando un Servidor de integración para detectar la SVM, puede usar *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 la SVM. Para obtener más información sobre cómo especificar etiquetas en la configuración de la 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 la clave de licencia EDR Optimum (Complemento de EDR Optimum) agregada. Como resultado, puede usar la funcionalidad de EDR Optimum en la máquina virtual con el Light Agent. Si se conecta el Light Agent a una SVM que no tiene 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 la 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Modo de Light Agent** → **Etiqueta de conexión de la SVM**.

4. Seleccione la casilla de verificación **Usar etiqueta de conexión** e ingrese una etiqueta de conexión de la SVM.

   Como etiqueta, puede ingresar una cadena de texto de hasta 255 caracteres. Puede usar cualquier carácter excepto el carácter `;`.

5. Guarde los cambios.

Cómo asignar una etiqueta de conexión de la 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 ficha **Configuración de la aplicación**.

4. Vaya a **Modo de Light Agent** → **Etiqueta de conexión de la SVM**.

5. Seleccione la casilla de verificación **Usar etiqueta de conexión** e ingrese una etiqueta de conexión de la SVM.

   Como etiqueta, puede ingresar una cadena de texto de hasta 255 caracteres. Puede usar cualquier carácter excepto el carácter `;`.

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

Cómo asignar una etiqueta de conexión de la SVM a un Light Agent en la interfaz de la aplicación

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

2. En la ventana de configuración de la aplicación, en **Modo de Light Agent** haga clic en el ícono **Etiqueta de conexión de la SVM**.

3. Seleccione la casilla de verificación **Usar etiqueta de conexión** e ingrese una etiqueta de conexión de la SVM.

   Como etiqueta, puede ingresar una cadena de texto de hasta 255 caracteres. Puede usar cualquier carácter excepto el carácter `;`.

4. Guarde los cambios.

Proteger la conexión entre un Light Agent y una SVM

Puede configurar el cifrado de la conexión entre los Light Agents y el Servidor de protección. Para hacerlo, debe habilitar el cifrado del canal de datos entre 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 cual está habilitada la protección de conexión solo puede conectarse a las SVM para las cuales está habilitado el cifrado del canal de datos entre Light Agent y el Servidor de protección. Un Light Agent para el cual está deshabilitada la protección de conexión solo puede conectarse a las SVM para las cuales está deshabilitado el cifrado de canal o se permite una conexión no segura entre el Servidor de protección y Light Agent.

Para obtener más información sobre cómo configurar la protección de la conexión en el Servidor de protección, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

> La protección de la conexión mediante cifrado puede reducir el rendimiento de Kaspersky Security for Virtualization Light Agent.

Cómo configurar la protección de la conexión de 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 correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Modo de Light Agent** → **Protección de la conexión**.

4. Seleccione la casilla de verificación **Cifrar canal de datos entre Light Agent y el Servidor de protección**.

5. Guarde los cambios.

Cómo configurar la protección de la conexión de 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 ficha **Configuración de la aplicación**.
4. Vaya a **Modo de Light Agent** → **Protección de la conexión**.
5. Seleccione la casilla de verificación **Cifrar canal de datos entre Light Agent y el Servidor de protección**.
6. Para aplicar la directiva a los equipos, cierre los íconos de candado y guarde los cambios.

Cómo configurar la protección de la conexión de un Light Agent en la interfaz de la aplicación

1. En la ventana principal de la aplicación haga clic en el botón .
2. En la ventana de configuración de la aplicación, en **Modo de Light Agent** haga clic en el ícono **Protección de la conexión**.
3. Seleccione la casilla de verificación **Cifrar canal de datos entre Light Agent y el Servidor de protección**.
4. Guarde los cambios.

Activar Light Agent

Si Kaspersky Endpoint Security se utiliza en el modo de Light Agent para proteger entornos virtuales, no es necesario activar la aplicación por separado. Para activar la aplicación, debe agregar una clave de licencia a la SVM. Puede agregar una clave de licencia a la SVM mediante la tarea especial en la consola de Kaspersky Security Center. No puede administrar las claves de licencia en la interfaz del Light Agent; sin embargo, puede ver la información de la licencia (consulte la imagen a continuación). También puede ver la información de licencia del Light Agent en la línea de comandos (consulte las instrucciones a continuación). El Light Agent obtiene esta información de la SVM. Para obtener más información sobre cómo activar la solución y administrar las claves de licencia, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

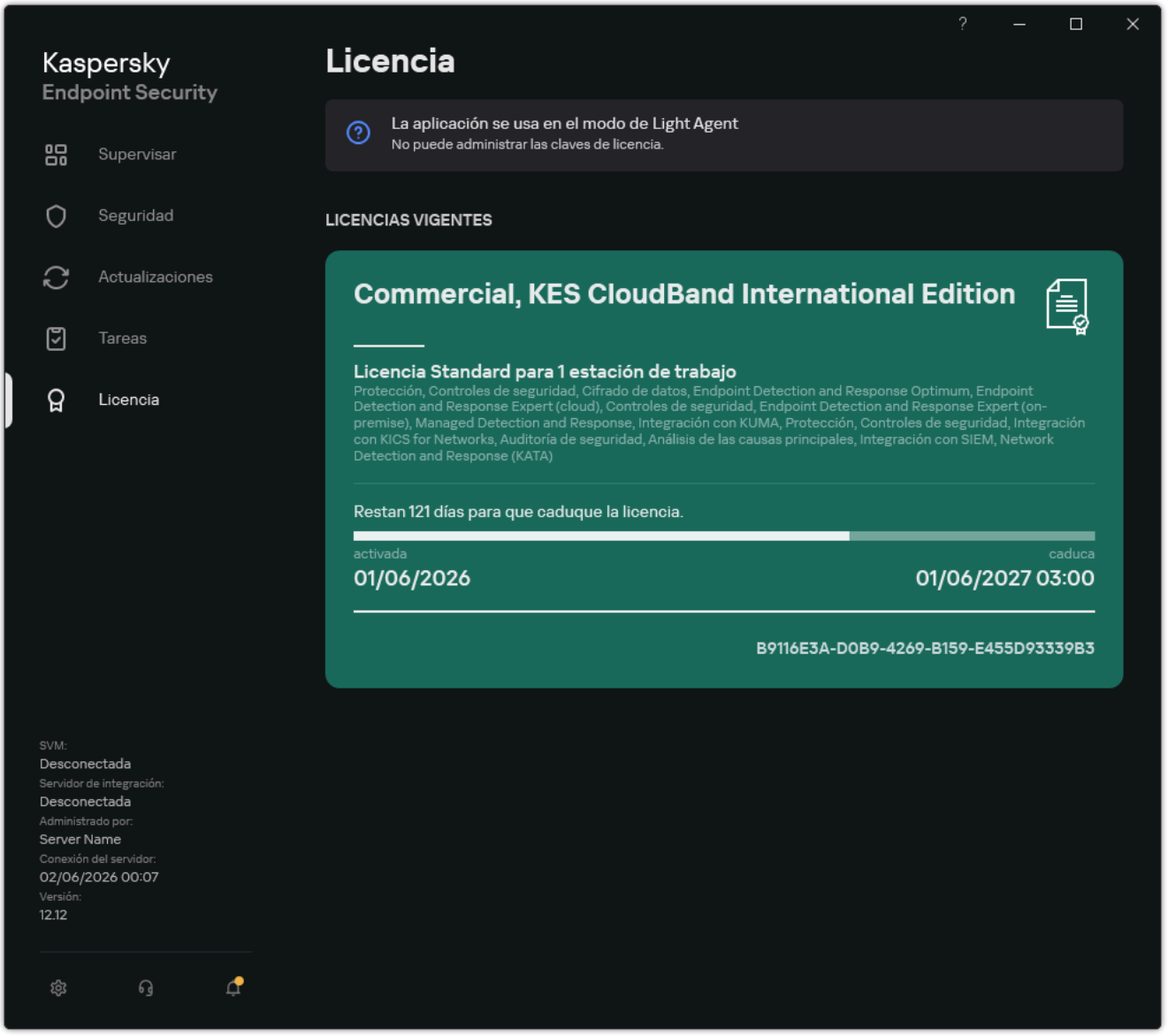
Para ver la información de licencia del Light Agent:

1. Abra el símbolo del sistema (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: la dirección de la SVM a la que está conectado el Light Agent, la cantidad de días que faltan para que caduque la licencia y otros datos. Si encuentra algún problema al activar Light Agent, consulte la Base de conocimientos de soporte técnico.



Ventana Licencias

Guía de migración de KSVLA Light Agent a KES Light Agent

Kaspersky Security for Virtualization Light Agent 5.2 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 KSVLA Light Agent 5.2 a Kaspersky Endpoint Security en el modo de Light Agent (en adelante, también denominado "KES Light Agent"). Para obtener más información sobre cómo actualizar 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 máquina virtual 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 14.2 o versiones posteriores. 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 ajustes 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 bases de datos). Después de la migración, también se recomienda verificar si el asistente de migración migró correctamente todos los ajustes.

   Si la protección con contraseña está habilitada para restringir el acceso a KSVLA Light Agent, antes de instalar KES Light Agent, debe deshabilitar la protección con contraseña en la directiva de KSVLA Light Agent. No puede ingresar 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 habilitar la protección con contraseña en la directiva de KES.

2. **Instalar Kaspersky Endpoint Security en el modo de 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 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 funcione correctamente. Active la directiva convertida. Verifique 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, también verifique la hora de la última conexión a la SVM y el estado de la protección de la máquina virtual. No es necesario activar Light Agent porque la clave de licencia se agrega a la SVM.

Instalar 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 KSVLA Light Agent

Eliminar KSVLA Light Agent

Puede eliminar la aplicación de forma remota mediante la tarea *Instalar aplicación de forma remota*, de forma local 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 mediante cualquier método adecuado.

Instalar Kaspersky Endpoint Security

> Si la protección con contraseña está habilitada para restringir el acceso a KSVLA Light Agent, antes de instalar KES Light Agent, debe deshabilitar la protección con contraseña en la directiva de KSVLA Light Agent. No puede ingresar 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 habilitar 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 una máquina 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 para instalar está determinado por 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 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 mediante 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 mediante *Cambiar componentes de la aplicación*.

Correspondencia de los componentes de KSVLA Light Agent y KES Light Agent

Los conjuntos de componentes de KSVLA Light Agent y KES Light Agent son prácticamente los mismos. KES Light Agent tiene más configuraciones que KSVLA Light Agent. Después de la migración, la nueva configuración tiene valores predeterminados.

Correspondencia de los componentes de KSVLA Light Agent y KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Núcleo de la aplicación
File Anti-Virus	Protección contra amenazas de archivo
Mail Anti-Virus	Protección contra amenazas de correo
Web Anti-Virus	Protección contra amenazas web
Firewall	Firewall
Network Attack Blocker	Protección contra amenazas de 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
System Integrity Monitoring	Control de integridad del sistema
Integration with Kaspersky Endpoint Agent	*(no se admite)* 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 vía AMSI

Migrar 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, el "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 se puede migrar a Web Console y Cloud Console.

Las siguientes consideraciones especiales están involucradas en la migración de directivas y tareas:

- Una nueva directiva tiene el nombre *<Directiva> (convertido)*.
- La nueva directiva tiene el estado *Directiva inactiva*.
- La prohibición de modificar la configuración (el "candado") no se migra. El Asistente de migración establece los valores predeterminados.

- Los perfiles de directiva no se migran. Debe agregar manualmente los perfiles de directiva.

- Administración mejorada de la zona de confianza. En KSVLA Light Agent, puede agregar exclusiones predefinidas solo durante la creación de una directiva. Posteriormente, en las propiedades de la directiva, puede configurar exclusiones predefinidas agregadas anteriormente o agregar exclusiones de forma manual. No puede agregar 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 la directiva.

- Los conjuntos de funcionalidades para configurar el control de acceso basado en derechos (RBAC) son diferentes en Kaspersky Endpoint Security y 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, seleccione 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. Seleccionar la aplicación para la que desea convertir directivas y tareas

En este paso, debe seleccionar Kaspersky Endpoint Security para Windows. Vaya al siguiente paso.

Paso 2. Conversión de directivas

Seleccione la directiva de Kaspersky Security for Virtualization Light Agent 5.2 para Windows que desee convertir. Vaya al siguiente paso.

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 de KSN. Una nueva directiva tiene el nombre *<Directiva> (convertido)*.

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 desee crear para Kaspersky Endpoint Security. Se nombrarán nuevas tareas como *<nombre de la tarea> (convertido)*. Vaya al siguiente paso.

Paso 4. Fin del Asistente

Salga del Asistente.

Después de migrar una directiva, debe abrir las propiedades de la directiva, verificar su configuración y guardar la directiva. Si no completa estos pasos, es posible que KES Light Agent ignore la directiva convertida.

Preste atención en especial a la migración de la configuración de conexión, las listas de exclusión, las aplicaciones de confianza, las direcciones web de confianza y las reglas de Control de aplicaciones de SVM de Light Agent.

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 agregó un agente incorporado 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 siguen funcionando con los agentes incorporados de Kaspersky Endpoint Security. Además, se eliminará Kaspersky Endpoint Agent 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 más información sobre cómo actualizar la versión de Kaspersky Security for Virtualization Light Agent, consulte la Ayuda de Kaspersky Security for Virtualization Light Agent.

Migrar la configuración [KSVLA Light Agent+KEA] a [KES Light Agent+agente incorporado] incluye los siguientes pasos:

1. **Migrar las directivas y tareas**

   Migrar las directivas y tareas [KSVLA Light Agent+KEA] a [KES Light Agent+agente incorporado] incluye 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 directiva nueva con el nombre *<Directiva> (convertido)*. También se crean tareas nuevas de KES con los nombres *<Nombre de la tarea> (convertido)*.

   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> y <Nombre de la directiva de Kaspersky Endpoint Agent>*. También se crean nuevas tareas y tareas de KES.

2 **Migrar de KSVLA Light Agent a KES Light Agent**

Migrar de KSVLA Light Agent a KES Light Agent implica instalar KES Light Agent en lugar de KSVLA Light Agent.

Los administradores suelen habilitar la protección con contraseña para restringir el acceso a KSVLA Light Agent y KEA. Solo puede ingresar la contraseña de desinstalación de KEA en las propiedades de la tarea *Instalar aplicación de forma remota*. Para la migración, debe deshabilitar la protección con contraseña para KSVLA Light Agent.

Para realizar la migración, debe seleccionar los componentes necesarios para admitir las soluciones de Detection and Response como parte de Kaspersky Endpoint Security. Luego de instalar la aplicación, Kaspersky Endpoint Security pasa a usar el agente incorporado y elimina Kaspersky Endpoint Agent.

3 **Funcionalidad de licencia**

Si la aplicación se utiliza en el modo de Light Agent, no es necesario activar la aplicación. Para activar la aplicación, debe agregar una clave de licencia a la SVM. También debe agregar la clave de licencia para activar funciones adicionales (por ejemplo, EDR Optimum) a la SVM. Es decir, como parte de la migración, la licencia de la funcionalidad se realiza automáticamente.

4 **Revisar el estado de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox**

Luego de la actualización, si el equipo tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el equipo tenga el Agente de red versión 13.2 o posterior instalado.
- El estado de funcionamiento del agente incorporado aparecerá en la sección *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin instalar*, instale los componentes 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 de EDR Optimum esté activada mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *Sin cobertura por la licencia*, asegúrese de que la funcionalidad de distribución automática de claves de licencia de EDR Optimum esté activada.
- Verifique el estado de la conexión de la máquina virtual a la SVM. Puede obtener información sobre el estado de la conexión del Light Agent a la SVM en Kaspersky Endpoint Security o con 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, ejecute el comando `avp.com HELP`. Para conocer la sintaxis de un comando específico, escriba `avp.com HELP <command>`.

Debe escapar los caracteres especiales en el comando. Para escapar los caracteres `&`, `|`, `(`, `)`, `<`, `>`, `^`, use el carácter `^` (por ejemplo, para usar el carácter `&`, ingrese `^&`). Para escapar el carácter `%`, escriba `%%`.

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`.

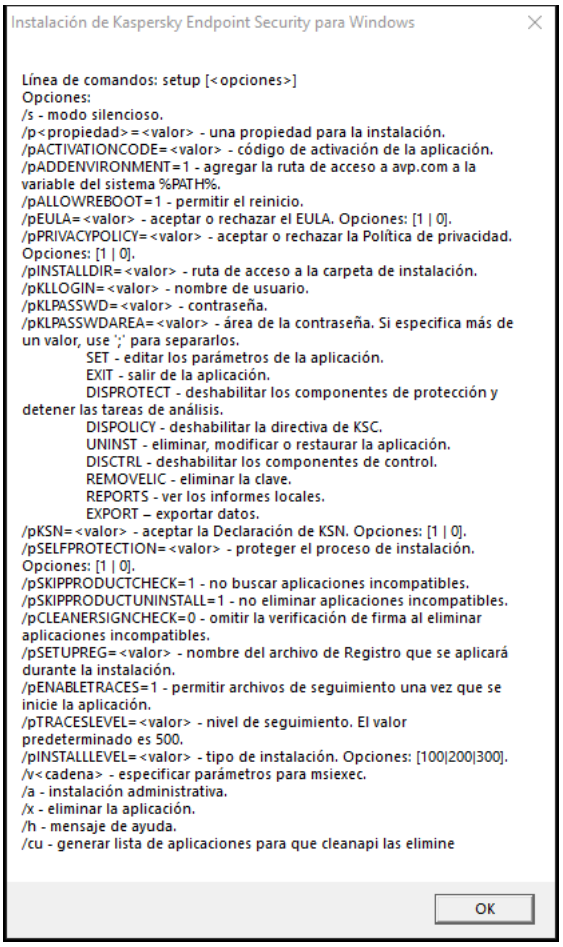
Setup. Instalación de la aplicación

Kaspersky Endpoint Security puede instalarse a través de la línea de comandos en dos modos:

- En modo interactivo usando el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez iniciada la instalación en modo silencioso, no es necesaria su participación en el proceso de instalación (instalación silenciosa). Para instalar la aplicación en modo silencioso, use los modificadores `/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 instalación disponibles, ejecute el comando `/h`. Para obtener ayuda sobre la sintaxis del comando de instalación, escriba `setup_kes.exe /h`. Como resultado, el instalador muestra una ventana con una descripción de las opciones del comando (consulte la imagen a continuación).



Descripción de las opciones del comando de instalación

Para instalar la aplicación o actualizar una versión anterior de la aplicación:

1. Abra el símbolo del sistema (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

```
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 consecuencia, la aplicación se instala en el equipo. Para confirmar que la aplicación esté instalada y comprobar su configuración, ejecute el comando `status`.

`EULA=1`	Aceptación de los términos del Contrato de licencia de usuario final. El texto del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Es necesario aceptar los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar su versión.
`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 la versión de la aplicación, deberá aceptar la Política de privacidad.
`KSN`	Participar o negarse a participar en Kaspersky Security Network (KSN). Si no especifica ningún valor para este parámetro, se le preguntará si desea participar en KSN cuando inicie Kaspersky Endpoint Security por primera vez. Valores disponibles: • `1`: participar en KSN. • `0`: negarse a participar en KSN (valor predeterminado). El paquete de distribución de Kaspersky Endpoint Security está optimizado para ser utilizado con Kaspersky Security Network. Si opta por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que se haya completado la instalación.
`CONFIGPATH=<path to the configuration file>`	Instalación de la aplicación con una configuración predefinida. Para continuar, debe cargar 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`	Permitir que el equipo se reinicie automáticamente, de ser necesario, cuando la aplicación termine de instalarse o actualizarse. Si no especifica ningún valor para este parámetro, se bloquea el reinicio automático del equipo. No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación.
`SKIPPRODUCTCHECK=1`	Deshabilite la búsqueda de software instalado. La lista de software que podría generar problemas de compatibilidad se encuentra en el archivo incompatible.txt, que forma parte del kit de distribución. Si no se fija un valor para este parámetro y se detecta algún software de esta lista, la instalación de Kaspersky Endpoint Security se detendrá.
`SKIPPRODUCTUNINSTALL=1`	Deshabilite la eliminación automática del software detectado presente en la lista incompatible.txt. Si no se fija un valor para este parámetro, Kaspersky Endpoint Security intentará eliminar el software que podría generar problemas de compatibilidad. No se puede habilitar la eliminación automática de software cuando se instala Kaspersky Endpoint Security con el instalador msiexec. Para eliminar automáticamente el software que podría generar problemas de compatibilidad, use el archivo setup_kes.exe.
`CLEANERSIGNCHECK=0|1`	Verificación de firmas digitales de los archivos de software detectados presentes en la lista 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 confiable 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 es diferente según el método de instalación del software: • `0` significa que la verificación de firma digital está deshabilitada (valor predeterminado si se implementa a través de Kaspersky Security Center). • `1` significa que la verificación de firma digital está habilitada (valor predeterminado si la aplicación se instala localmente).
`STANDALONEMODE=1`	Instalación de la aplicación en la configuración de Endpoint Detection and Response Agent (EDR Agent) para integrar 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 de protección de endpoints (EPP) de terceros en su organización junto con la solución de clase Kaspersky Endpoint Detection and Response (KATA). Esto hace que Kaspersky Endpoint Security en la configuración de Endpoint Detection and Response Agent sea compatible con aplicaciones de EPP de terceros.
`KLLOGIN`	Permite definir el nombre de usuario con el que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (componente de Protección con contraseña). El nombre de usuario se configura a la par de los parámetros `KLPASSWD` y `KLPASSWDAREA`. El nombre de usuario predeterminado es KLAdmin.

KLPASSWD	Permite definir la contraseña con la que se accederá a las funciones y a las opciones de configuración 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 manera predeterminada el nombre de usuario KLAdmin.
KLPASSWDAREA	Permite especificar el alcance de la contraseña de acceso a Kaspersky Endpoint Security. Cuando un usuario intente realizar una acción que esté dentro del alcance de la contraseña, Kaspersky Endpoint Security le solicitará las credenciales (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: deshabilitar los componentes de protección y detener las tareas de análisis. • DISPOLICY: deshabilitar la directiva de Kaspersky Security Center. • UNINST: eliminar la aplicación del equipo. • DISCTRL: deshabilitar los componentes de control. • REMOVELIC: eliminar la clave. • REPORTS: acceder a los informes. • EXPORT: exportar configuración de la aplicación. Por ejemplo, KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña. Por lo tanto, es imposible configurar el alcance de la contraseña para la cuenta de KLAdmin. Si intenta configurar el alcance 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 impide que las aplicaciones de terceros interfieran con el funcionamiento de los servicios del sistema operativo. Estos servicios incluyen, entre otros, el inicio automático de las aplicaciones. • 1 significa que la protección de los servicios del sistema operativo está habilitada (valor predeterminado). • 0 significa que la protección de los servicios del sistema operativo está deshabilitada.
ENABLETRACES	Habilitar o deshabilitar el seguimiento de la aplicación. Una vez que se inicia Kaspersky Endpoint Security, guarda los archivos de seguimiento en la carpeta %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Valores disponibles: • 1: la función de seguimiento está habilitada. • 0: la función de seguimiento está deshabilitada (valor predeterminado).
TRACESLEVEL	Nivel de detalle de los archivos de seguimiento. Valores disponibles: • 100 (crítico). Solo mensajes sobre errores graves. • 200 (alto). Mensajes sobre todos los errores, incluidos los 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	Habilitar o deshabilitar el modo de compatibilidad de Azure WVD. Valores disponibles: • 1 – El modo de compatibilidad de Azure WVD está habilitado. • 0 – El modo de compatibilidad de Azure WVD está deshabilitado (valor predeterminado). Esta función garantiza la correcta visualización del estado de la máquina virtual Azure en la consola de Kaspersky Anti Targeted Attack Platform. Para monitorear el rendimiento del equipo, Kaspersky Endpoint Security envía telemetría a los servidores de KATA. La telemetría incluye una identificación del equipo (Sensor ID). El modo de compatibilidad de Azure WVD permite asignar una Sensor ID única y permanente a estas máquinas virtuales. Si el modo de compatibilidad está desactivado, la Sensor ID puede cambiar después de reiniciar el equipo debido a cómo funcionan las máquinas virtuales de Azure. Esto puede hacer que aparezcan duplicados de máquinas virtuales en la consola.
AMPPL	Habilitar o deshabilitar el uso de la tecnología AM-PPL (Antimalware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019. Valores disponibles: • 1: los procesos de Kaspersky Endpoint Security se protegerán con la tecnología AM-PPL. • 0: los procesos de Kaspersky Endpoint Security no se protegerán con la tecnología AM-PPL.

`UPGRADEMODE`	Modo de actualización de la aplicación: • `Seamless` significa actualizar la aplicación con un reinicio del equipo (valor predeterminado). • `Force` significa actualizar la aplicación sin reiniciar. Puede actualizar la aplicación sin reiniciar el equipo a partir de la versión 11.10.0. Para actualizar una versión anterior de la aplicación, debe reiniciar el equipo. También puede instalar parches sin reiniciar el equipo a partir de la versión 11.11.0. No es necesario reiniciar al instalar Kaspersky Endpoint Security. Así, el modo de actualización se especificará en la configuración de la aplicación. Puede cambiar este parámetro en la configuración de la aplicación o en la directiva. Cuando se actualiza una aplicación ya instalada, la prioridad del parámetro de línea de comandos es inferior a 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 se establece el modo `Seamless` en la configuración de la aplicación, la actualización se instalará con el reinicio del equipo (`Seamless`).
`RESTAPI`	Administrar la aplicación a través de la API REST. Si desea administrar la aplicación mediante REST API, deberá configurar el parámetro `RESTAPI_User` para especificar el nombre de usuario. Valores disponibles: • `1`: la aplicación podrá administrarse a través de la API REST. • `0`: la aplicación no podrá administrarse a través de la API REST (valor predeterminado). Si desea administrar la aplicación mediante REST API, debe permitir el uso de sistemas de administración. Para ello, defina el parámetro `AdminKitConnector=1`. Si opta por utilizar la API REST, no podrá usar los sistemas de administración de Kaspersky para controlar la aplicación.
`RESTAPI_User`	Nombre de usuario de la cuenta de dominio de Windows que se usará para administrar la aplicación a través de la API REST. Solo este usuario podrá administrar la aplicación con la API REST. El nombre de usuario debe especificarse en formato `<DOMAIN>\<UserName>` (por ejemplo, `RESTAPI_User=COMPANY\Administrator`). El uso de la API REST está limitado a un único usuario. Especificar este valor es requisito indispensable para administrar la aplicación a través de la API REST.
`RESTAPI_Port`	Puerto que se usará 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 reconocer solicitudes (por ejemplo, `RESTAPI_Certificate=C:\cert.pem`). La interacción segura de Kaspersky Endpoint Security con el cliente de REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga de cada solicitud.
`ADMINKITCONNECTOR`	Permitir que la aplicación se administre a través de un sistema de administración. Kaspersky Security Center es uno de esos sistemas. Además de los sistemas de administración de Kaspersky, es posible utilizar soluciones de terceros. La API de Kaspersky Endpoint Security se ha diseñado para ello. Valores disponibles: • `1`: la aplicación podrá administrarse a través de un sistema de administración (valor predeterminado). • `0`: la aplicación podrá administrarse únicamente a través de su 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 madre. En algunos casos, por ejemplo, cuando se utiliza 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 cual se envía la telemetría. Para crear un Sensor ID único, debe configurar 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 garantiza un Sensor ID único. De manera predeterminada, el parámetro no está establecido. 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, el instalador intenta heredar el Sensor ID. Si el Sensor ID no se puede restaurar, la aplicación crea un nuevo Sensor ID.
`SKIPKB5007186CHECK=1`	Deshabilitar la verificación de la actualización del sistema operativo 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 más información, consulte la Base de conocimientos del Servicio de soporte técnico. Por lo tanto, el instalador anula la instalación si se detecta esta actualización. Para continuar con la instalación, configure `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). Usualmente, una licencia de prueba tiene un plazo corto. Cuando la licencia de prueba se vence, se deshabilitan todas las características de Kaspersky Endpoint Security. Para seguir 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 su versión en modo silencioso, se admite el uso de los siguientes archivos:

- setup.ini: parámetros generales para instalar la aplicación.

  Para aplicar la configuración del archivo setup.ini, colóquelo en la misma carpeta que el paquete de distribución de Kaspersky Endpoint Security.

- install.cfg: parámetros relativos al funcionamiento de Kaspersky Endpoint Security

  Para aplicar la configuración desde el 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 archivo setup.reg se escriben en el registro solo si se establece el valor de `setup.reg` 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, colóquelo en la misma carpeta que 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 puede desinstalarse a través de la línea de comandos de los siguientes modos:

- En modo interactivo usando el Asistente de instalación de la aplicación.

- En modo silencioso. Una vez que comience la desinstalación en modo silencioso, no es necesaria su participación en el proceso de eliminación (eliminación silenciosa). Para desinstalar la aplicación en modo silencioso, use los modificadores `/s` y `/qn`.

Para desinstalar la aplicación en modo silencioso:

1. Abra el símbolo del sistema (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

```
msiexec.exe /x <GUID> /qn
```

`<GUID>` es el id. único de la aplicación. Para determinar cuál es este identificador, consulte la Base de conocimientos del Servicio de soporte técnico o utilice el siguiente comando:

```
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

```
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.14.1\QB`. De manera predeterminada, la opción de guardar archivos en Copia de seguridad está deshabilitada (`SAVEQB=0`).

Ejemplo

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Recuperar la aplicación

Al recuperarse, la aplicación verifica 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 puede recuperarse a través de la línea de comandos en uno de los siguientes modos:

- En modo interactivo usando el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que comience la recuperación en modo silencioso, podrá desentenderse del proceso de recuperación.

Si el instalador de Kaspersky Endpoint Security se ejecuta en modo de recuperación y la aplicación no necesita recuperación, el instalador no realiza cambios.

Si el instalador de Kaspersky Endpoint Security se ejecuta en modo de recuperación y la aplicación no está instalada, el instalador inicia el proceso de instalación.

Para recuperar la aplicación en modo silencioso, haga lo siguiente:

1. Abra el símbolo del sistema (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. Para determinar cuál es este identificador, consulte la Base de conocimientos del Servicio de soporte técnico o utilice el siguiente comando:

     ```
     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
```

Comando de AVP

Para administrar Kaspersky Endpoint Security a través de la línea de comandos:

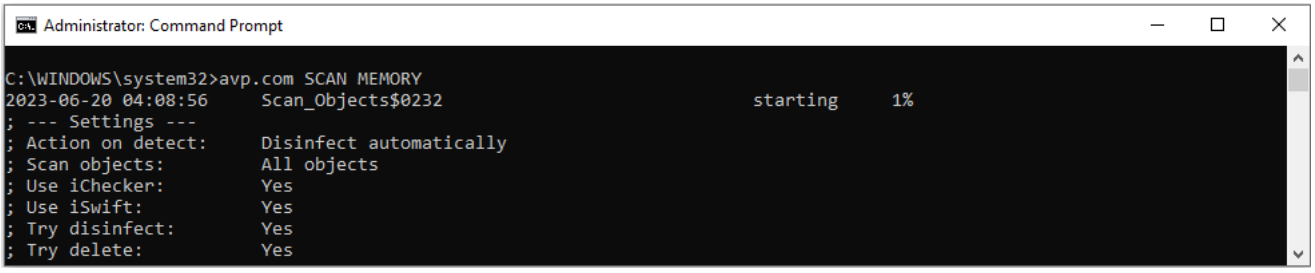
1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

   Puede agregar la ruta al 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 de malware

Ejecución de la tarea *Análisis de malware*.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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>]
```

Alcance 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`	Ejecute la tarea de *Análisis de malware*. Kaspersky Endpoint Security analiza los siguientes objetos: • Memoria del núcleo • Objetos cargados al iniciar el sistema operativo • Sectores de inicio • Copia de seguridad del sistema operativo • Todos los discos rígidos y discos extraíbles En Kaspersky Endpoint Security para Windows 12.12, se excluye el correo electrónico del alcance del análisis de la aplicación. El análisis de los mensajes de correo electrónico entrantes y salientes lo realiza el componente Protección contra amenazas de correo. Si está utilizando una versión anterior del complemento de administración, la aplicación excluye el correo electrónico del alcance del análisis, aunque la directiva lo incluya.
`/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 amenaza	
`/i0`	**Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.
`/i1`	**Desinfectar; informar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección falla, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.
`/i2`	**Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo 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 archivo	
`/fe`	**Archivos analizados según su extensión**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión.
`/fi`	**Archivos analizados según su formato**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, 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 esta configuración está habilitada, la aplicación analiza todos los archivos sin excepción (todos los formatos y las extensiones). Esta es la configuración por defecto.

Exclusiones de 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 archivo especificada. Por ejemplo: • Si utiliza la máscara `*.exe`, se excluirán del análisis 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 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
`/iSwift=on|off`	Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

La configuración avanzada	
`/C:<file with scan settings>`	Archivo con la configuración de la tarea de *Análisis de malware*. 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 bases de datos y módulos de software de la aplicación

Ejecución de la tarea *Actualización de bases de datos y módulos de la aplicación*.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

No puede ejecutar este comando si la aplicación está instalada en el 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 bases de datos y módulos de la aplicación* que se creó automáticamente después de instalar la aplicación. Puede cambiar la configuración de la tarea *Actualización de 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 *Actualización de bases de datos y módulos de la aplicación* con la configuración predeterminada o con la configuración especificada en el comando. Puede definir la configuración de la tarea de *Actualización de bases de datos y módulos de la aplicación* de la siguiente manera: • `UPDATE` inicia la tarea de *Actualización de bases de datos y módulos de la aplicación* con la configuración predeterminada: el origen de actualizaciones está en los servidores de actualizaciones de Kaspersky, la cuenta es Sistema y demás configuraciones predeterminadas. • `UPDATE local` inicia la tarea de *Actualización de bases de datos y módulos de la aplicación* que se creó automáticamente luego de la instalación (tarea predefinida). • `UPDATE <update settings>` inicia la tarea de *Actualización de bases de datos y módulos de la aplicación* con la configuración establecida manualmente (que figura 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 el origen predeterminado: Servidores de actualizaciones de Kaspersky.

Guardar eventos en un modo de archivo de informe (solo para 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.

La configuración avanzada	
/C:<file with update settings>	Archivo con la configuración de la tarea de *Actualización de 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

No puede ejecutar este comando si la aplicación está instalada en el 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 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. Seguimiento

Los archivos de seguimiento quedarán guardados en el equipo mientras la aplicación esté instalada; cuando desinstale la aplicación, los archivos se eliminarán de forma permanente. Los archivos de seguimiento, excepto los del Agente de autenticación, se almacenan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. De manera predeterminada, la función está deshabilitada.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 de los archivos de seguimiento. Valores disponibles: • `100` (crítico). Solo mensajes sobre errores graves. • `200` (alto). Mensajes sobre todos los errores, incluidos los 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.

La 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 limitado de conjuntos de archivos, que no podrán superar un tamaño máximo. 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, actualizar las bases de datos o habilitar un componente de protección).

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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. Para ver la lista de perfiles disponibles, ejecute el comando `HELP START`.

Guardar eventos en un modo de archivo de informe (solo para 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 deshabilitar un componente de protección).

Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada. El usuario debe tener los permisos **Deshabilitar componentes de protección** y **Deshabilitar componentes de control**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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. Para ver la lista de perfiles disponibles, ejecute 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 en qué estado se encuentran los perfiles de la aplicación (por ejemplo, `running` o `completed`). Para ver la lista de perfiles disponibles, ejecute 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 Servicio de soporte técnico de Kaspersky.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 ingresa 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 un perfil de la aplicación (por ejemplo, la duración de un análisis o la cantidad de amenazas detectadas). Para ver la lista de perfiles disponibles, ejecute el comando `HELP STATISTICS`.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 desde copias de seguridad

Restaurar un archivo almacenado en Copias de seguridad a su carpeta original. Si en la ruta especificada ya existe un archivo con el mismo nombre, la aplicación solicitará confirmación para reemplazar el archivo. El archivo restaurado se guarda con su nombre original.

Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada. El usuario debe tener el permiso **Restaurar objetos de Copia de seguridad**.

El depósito *Copia de seguridad* contiene copias de respaldo de los archivos que se modifican o eliminan cuando se realiza una desinfección. Una *copia de seguridad* es una copia del archivo creada antes de desinfectar o eliminar el archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. Se conceden accesos limitados a esta carpeta al usuario cuya cuenta se utilizó para instalar Kaspersky Endpoint Security.

Kaspersky Endpoint Security no brinda la capacidad de configurar permisos de acceso de usuario a copias de seguridad de archivos.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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>
```

La 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 coloca el archivo de la siguiente manera:

- Si la ruta a avp.com se agrega a la variable de sistema %PATH%, la aplicación coloca el archivo en la carpeta `C:\Windows\SysWOW64`.
- Si ejecuta el comando desde la carpeta de instalación de la aplicación, la exportación fallará debido a que la autoprotección de la aplicación bloquea la creación de un nuevo archivo en la carpeta de la aplicación. Para exportar los ajustes de configuración de la aplicación a un archivo, ingrese la ruta del archivo.

Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada. El usuario debe tener el permiso **Exportar configuración**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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. Para ver la lista de perfiles disponibles, ejecute el comando `HELP EXPORT`.

Archivo para exportar	
`<file name>`	Nombre del archivo en el que se guardarán los ajustes de configuración exportados. También puede escribir 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 ajustes de la aplicación

Importar 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 habilitada. El usuario debe tener el permiso **Configurar la aplicación**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 de clave.

Activar Kaspersky Endpoint Security con un archivo de clave. Si la aplicación ya está activada, la clave se agregará como clave de reserva.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

No puede ejecutar este comando si la aplicación está instalada en el modo de Light Agent.

Sintaxis del comando

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Archivo de clave	
`<file name>`	Nombre del archivo de clave.

Autenticación	
`/login=<user name> /password= <password>`	Credenciales de una cuenta de usuario. Estos datos solo se necesitan si la protección con contraseña está habilitada.

Ejemplo

```
avp.com ADDKEY file.key
```

LICENSE. Administración de licencias

Administrar las claves de licencia 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 habilitada. El usuario debe tener el permiso **Eliminar una clave**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

No puede ejecutar este comando si la aplicación está instalada en el 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 de clave. Si la aplicación ya está activada, la clave se agregará 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 agregará como clave de reserva.
`/REFRESH`	Actualice el estado de la licencia de Kaspersky Endpoint Security. De esta manera, la aplicación recibe información actualizada sobre el estado de la licencia de los servidores de activación de Kaspersky.
`/REFRESH <license ID>`	Actualice el estado de las licencias con el ID de la licencia. Con este comando, puede actualizar el estado de los complementos de EDR, MDR y KUMA, y de otras licencias. Puede encontrar el ID de licencia en el certificado de la licencia. De esta manera, la aplicación recibe información actualizada sobre el estado de la licencia de los servidores de activación de Kaspersky.
`/CHECK`	Obtenga información de la licencia. Kaspersky Endpoint Security muestra información sobre todas las claves de licencia agregadas, 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 la licencia: • nombre de la licencia; • identificador de la licencia; • dirección del Servidor de protección (SVM) al que está conectada la máquina virtual donde está instalada la aplicación en el modo de Light Agent; • tipo de licencia: prueba, comercial, beta, suscripción; • fecha y hora de activación de la aplicación; • fecha y hora de caducidad de la licencia; • cantidad de días hasta la fecha de caducidad de la licencia.
`/CHECK <license ID>`	Obtenga información de la licencia por Id. Puede usar este comando para obtener información de la licencia. Puede encontrar el ID de licencia en el certificado de la licencia.
`/DEL /login=<user name> /password=<password>`	Elimine la clave de licencia de la aplicación. La clave de reserva también se eliminará.
`/DEL <license ID> /login=<user name> /password=<password>`	Elimine la clave con el ID de licencia. Con este comando, puede eliminar una clave de los complementos de EDR, MDR y KUMA, y de otras licencias. Puede encontrar el ID de licencia en el certificado de la 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. Adquisición 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

No puede ejecutar este comando si la aplicación está instalada en el modo de Light Agent.

PBATESTRESET. Restablecer los resultados de la comprobación del disco antes de cifrarlo

Restablecer los resultados de la prueba de compatibilidad con el cifrado de disco completo (FDE), el cual puede estar basado en las tecnologías Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker.

Antes de aplicar el cifrado de disco completo, la aplicación realiza una serie de pruebas para verificar que el equipo pueda, efectivamente, cifrarse. Cuando se determina que el equipo no es compatible con el cifrado de disco completo, 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. Por ello, ante un cambio en el hardware del equipo, los resultados de la verificación deben descartarse y se debe volver a comprobar si el disco duro 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 habilitada. El usuario debe tener el permiso **Salir de la aplicación**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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. Deshabilitar una directiva

Deshabilitar 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 habilitada. El usuario debe tener el permiso **Deshabilitar la directiva de Kaspersky Security Center**.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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. Habilitar una directiva

Habilitar 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

DISABLE. Deshabilitar la protección

Deshabilitar el componente Protección contra archivos peligrosos en un equipo si la licencia de Kaspersky Endpoint Security caducó. 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 habilitada.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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

Seleccionar la solución de Kaspersky que se usará para determinar la reputación de los archivos y los sitios web. Kaspersky Endpoint Security da soporte a 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 detectados 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)*. A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky. 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;

  - 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar la ruta del archivo ejecutable a la variable de sistema %PATH% y ejecutar el comando sin navegar a la carpeta de la aplicación.

No puede ejecutar este comando si la aplicación está instalada en el 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. Deshabilitar la protección de la conexión con el servidor.

Ejecute la tarea *Protección de la conexión del Servidor de administración*, que elimina la contraseña de la conexión del equipo al Servidor de administración. De esta manera, la tarea deshabilita la protección de la conexión del Servidor de administración.

Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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>`	Contraseña de la cuenta de usuario de KLAdmin o contraseña de la tarea *Protección de la conexión del Servidor de administración*. Si no se especifica el parámetro, Kaspersky Endpoint Security le pedirá una contraseña en la siguiente línea.

Comando de KESCLI

Los comandos de KESCLI le permiten recibir información sobre el estado de la protección del equipo mediante el componente OPSWAT, y le permiten realizar tareas estándar como *Análisis de malware* y *Actualización de bases de datos y módulos de la aplicación*

Puede ver la lista de comandos de KESCLI a través del comando `kescli --help` o a través del comando abreviado `kescli -h`.

Para administrar Kaspersky Endpoint Security a través de la línea de comandos:

1. Abra el símbolo del sistema (cmd.exe) como administrador.

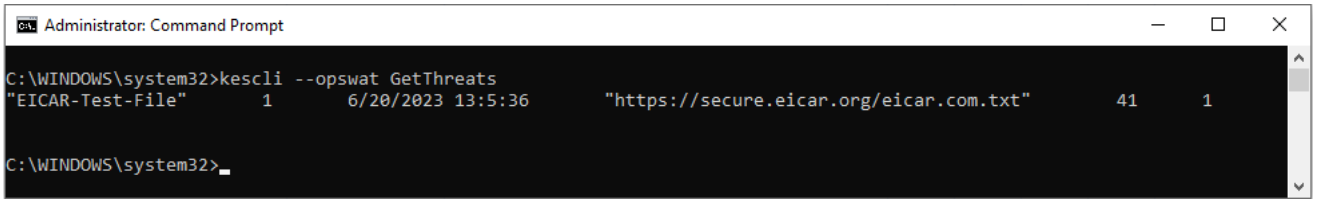
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

   Puede agregar la ruta al 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 de malware

Ejecutar la tarea *Análisis de malware* (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 encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Puede verificar el estado de la finalización de una tarea de *Análisis de malware* a través del comando `GetScanState` y ver la fecha y la hora en que se completó el análisis a través del comando `GetLastScanTime`.

Alcance del análisis	
`<scan scope>`	`;`: lista de archivos y carpetas separados. Por ejemplo, `"C:\Program Files (x86)\Example Folder"`.

Acción al detectar amenaza	
0	**Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.
1	**Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo 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 la finalización del análisis

Mostrar la información sobre el estado de la finalización de la tarea *Análisis de malware* (*Análisis completo*):

- 1: el análisis está en progreso.
- 0: el análisis no se está ejecutando.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetScanState
```

GetLastScanTime. Determinación de la hora de finalización del análisis

Mostrar información sobre la fecha y la hora de la última finalización de la tarea de *Análisis de malware* (*Análisis completo*).

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetLastScanTime
```

GetThreats. Obtención de datos sobre las amenazas detectadas

Visualización de una lista de amenazas detectadas (*Informe de amenazas*). Este informe contiene información sobre las amenazas y la actividad de los virus durante los últimos 30 días anteriores a la creación del informe.

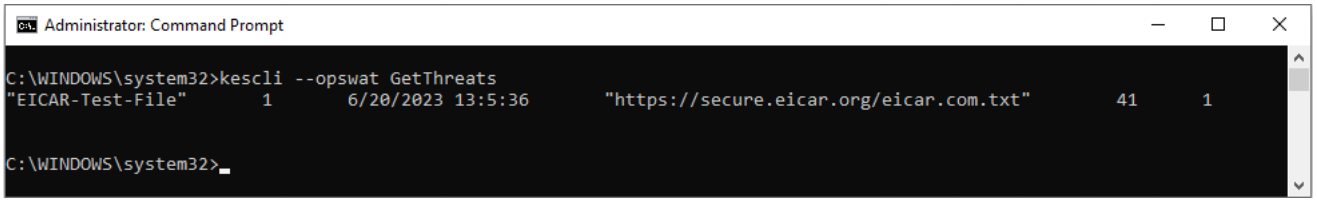
Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetThreats
```

Cuando se ejecute 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	Programa malintencionado (Malware).
4	Programas de publicidad (Adware).
5	Programas de marcador automático (Pornware).
6	Aplicaciones que podrían utilizarse por un ciberdelincuente para hacer daño en el equipo o los datos del usuario (Riskware).
7	Ejecutables comprimidos que puedan tener código malicioso oculto (Packed).
20	Objetos desconocidos (Xfiles).
21	Aplicaciones conocidas (Software).
22	Archivos ocultos (Hidden).
23	Aplicaciones que requieren atención (Pupware).
24	Comportamiento irregular (Anomaly).
30	No determinado (Undetect).
40	Anuncios publicitarios (Banner).
50	Ataque de red (Attack).
51	Acceso del registro (Registry).
52	Actividad sospechosa (Suspicion).
60	Vulnerabilidades (Vulnerability).
70	Phishing (Phishing).
80	Archivos adjuntos de correo electrónico no deseados (Attachment).
90	Malware detectado por Kaspersky Security Network (Urgent).
100	Vínculo desconocido (Suspic URL).
110	Otro malware (Behavioral).

Acción al detectar amenaza	
`0`	Desconocido (`unknown`).
`1`	Amenaza corregida (`ok`).
`2`	El objeto estaba infectado y no ha sido desinfectado (`infected`).
`5`	El objeto está en un archivo y no ha sido desinfectado (`archive`).
`9`	El objeto ha sido desinfectado (`disinfected`).
`10`	El objeto no ha sido desinfectado (`not disinfected`).
`11`	Se eliminó el objeto (`deleted`).
`13`	Se creó una copia de seguridad del objeto (`backupped`).
`15`	Se movió el objeto al depósito de copias 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`	El usuario movió el objeto al depósito de copias de seguridad (`added by user`).
`30`	El objeto se agregó a las exclusiones (`added to exclude`).
`31`	Se movió el objeto al depósito de copias 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 puede resolver la amenaza (`untreatable`).
`42`	Se restauró el objeto (`rolled back`).
`43`	El objeto se creó como resultado de una actividad de amenaza (`produced by threat`).
`44`	El objeto se restauró al reiniciar el equipo (`roll back on reboot`).
`0xffffffff`	El objeto no se procesó (`discarded`).

Nivel de peligro de la amenaza	
`0`	Desconocido
`1`	Alto
`2`	Análisis medio
`4`	Bajo
`8`	Información (menor que *Bajo*)

UpdateDefinitions. Actualización de bases de datos y módulos de software de la aplicación

Ejecución de la tarea *Actualización de bases de datos y módulos de la aplicación*. Kaspersky Endpoint Security utiliza el origen predeterminado: Servidores de actualizaciones 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security.

> No puede ejecutar este comando si la aplicación está instalada en el modo de Light Agent.

Sintaxis del comando

```
kescli --opswat UpdateDefinitions
```

Puede ver la fecha y hora de publicación de las bases de datos antivirus actuales a través del comando `GetDefinitionsetState`.

GetDefinitionState. Determinación de la fecha y hora de la última actualización de las bases de datos

Mostrar información sobre la fecha y hora de última actualización de las bases de datos antivirus en uso.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetDefinitionState
```

EnableRTP. Habilitación de la protección

Habilitar los componentes de protección de Kaspersky Endpoint Security en el equipo: Protección contra archivos peligrosos, Protección contra amenazas web, Protección contra amenazas de correo, Protección contra amenazas de red, 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat EnableRTP
```

De esta manera, los componentes de protección están habilitados incluso si prohibió la modificación de la configuración de la aplicación mediante Protección con contraseña.

Puede verificar el estado del funcionamiento de la Protección contra archivos peligrosos a través del comando `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Estado de la Protección contra archivos peligrosos

Mostrar información sobre el estado del componente de Protección contra archivos peligrosos:

- `1`: el componente está habilitado.
- `0`: el componente está deshabilitado.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Estado de cifrado del disco

Mostrar información acerca del estado de cifrado del disco:

- `1` significa que el disco está protegido con la tecnología de cifrado de disco de Kaspersky o BitLocker.
- `0` significa que el disco no está cifrado.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security.

Sintaxis del comando

```
kescli --Version
```

También puede utilizar el comando abreviado `-v`.

Comandos de administración de Detection and Response

Puede usar la línea de comandos para administrar las características integradas de las soluciones Detection and Response (por ejemplo, Kaspersky Sandbox o Kaspersky Endpoint Detection and Response Optimum). Puede administrar las soluciones Detection and Response si la administración mediante el uso de la consola de Kaspersky Security Center no es posible. Para ver la lista de comandos de administración disponibles, ejecute 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:

1. Abra el símbolo del sistema (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:

- Habilitar o deshabilitar el componente Sandbox.

  Los componentes de Sandbox proporcionan interacción con la solución Kaspersky Sandbox y el componente KATA Sandbox, que forma parte de Kaspersky Anti Targeted Attack Platform.

- Configurar el componente Kaspersky Sandbox:

  - Conectar el equipo a los servidores de Sandbox.

    Los servidores utilizan imágenes virtuales implementadas de los sistemas operativos Microsoft Windows para ejecutar objetos que necesitan ser analizados. Puede ingresar una dirección IP (IPv4 o IPv6) o un nombre de dominio completo. Para obtener más información sobre el despliegue 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.

  - Configurar el tiempo de espera de la conexión para el servidor.

    Tiempo de espera de la conexión al servidor de Sandbox (para Kaspersky Sandbox) o al 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 conexión agotado para el 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.

- Configurar una conexión de confianza 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. Luego, debe agregar el certificado al equipo mediante una directiva. También debe agregar 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 sea parte, es decir, Kaspersky Sandbox o KATA Sandbox. *Kaspersky Sandbox* es una solución independiente de Kaspersky Detection and Response. *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:

  - **Manualmente**. El usuario envía manualmente el archivo para analizarlo desde el menú contextual (**Enviar a Sandbox**).
  - **Automáticamente**. La aplicación detecta objetos y los envía a Sandbox para analizarlos de manera automática.
  - **Combinado**.

- Mostrar la configuración actual del componente.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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`	Deshabilite el componente Sandbox.
`start`	Habilite el componente Sandbox.

`set`	Configure el componente Sandbox. Puede configuración las siguientes:
	• Agregue los servidores de Sandbox (`--servers`)
	• Agregue un certificado TLS (`--pinned-certificate`)
	• Agregue un contenedor criptográfico (`--client-certificate`).
	• Especifique una contraseña para el criptocontenedor (`--client-certificate-password`);
	• Configure el tiempo de espera de la conexión al 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. Administrar la prevención de la ejecución

Deshabilitar el componente de prevención de la ejecución o mostrar la configuración actual del componente, incluida la lista de reglas de prevención de la ejecución.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 del 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 deshabilitar el componente cuando ya está deshabilitado).

ISOLATION. Administrar el aislamiento de la red

Deshabilitar el aislamiento de la red en el equipo o mostrar la configuración actual del componente. La configuración del componente también incluye una lista de conexiones de red agregadas a exclusiones.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 en 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 Cuarentena solo cuando se integra con la solución 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 habilitada. El usuario debe tener el permiso **Restaurar objetos de Copia de seguridad**.

El objeto se pone en cuarentena en la cuenta del sistema (SYSTEM).

La restauración de archivos de Cuarentena implica las siguientes consideraciones especiales:

- Si se eliminó la carpeta de destino o si el usuario no tiene derechos de acceso a esa carpeta, la aplicación coloca el archivo en la carpeta `%DataRoot%\QB\Restored`. A continuación, debe mover manualmente el archivo a la carpeta de destino.
- La aplicación distingue entre mayúsculas y minúsculas en el nombre del archivo que se está restaurando. Si no respeta las mayúsculas y las minúsculas cuando ingresa el nombre del archivo, la aplicación no podrá restaurar el archivo.
- 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. En el caso de 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 encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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>
```

La 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 del 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 una actividad que indica 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 *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta ante amenazas.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 anula después de 128 coincidencias con los indicadores de compromiso descritos en los archivos de IOC. Esto es necesario para limitar la cantidad de entradas en el informe de la tarea Análisis de IOC a fin de facilitar su observación y evitar que el informe se desborde debido a indicadores de compromiso formulados de forma imprecisa que puedan 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 de IOC	
`<full path to the IOC file>`	Ruta completa al archivo de IOC que desea utilizar para analizar. Puede especificar varios archivos de IOC separados por espacios. La ruta completa al archivo de IOC debe ingresarse 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 de IOC que desea usar para analizar. Los *Archivos de IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos de IOC deben cumplir con el estándar OpenIOC. Por ejemplo, `C:\Users\Admin\Desktop\IOC`

Tipo de datos del 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, 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 de 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 un archivo de las siguientes maneras: • `<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 de RegistryItem, 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 conjunto 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 de DnsEntryItem, 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 de 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 de ArpEntryItem, 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 de PortItem, 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 de 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 de ServiceItem, 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 de SystemInfoItem, 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 de 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 de UserItem, 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 de VolumeItem, se ignoran (se detectan como no coincidentes). Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos sobre los volúmenes 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 de EventLogItem, 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 de EventLogItem se describe en el archivo de IOC que se proporciona para el análisis.
`/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 el alcance del 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 de `TaskSettings::BaseSettings::EventLogItem::datetime` no se puede editar. La configuración se utiliza solo si el documento de IOC de 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 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 de los archivos. Si el archivo de IOC contiene términos del documento de IOC de FileItem, 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 el alcance del análisis de IOC al analizar los datos para el documento de IOC de FileItem. Puede establecer los siguientes valores para el alcance del análisis: • `<all>` para todos los alcances 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 el alcance 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 datos para el documento de IOC de FileItem (`/drives=custom`). Puede especificar varias rutas separadas por espacios.
`/retro /<number of days>`	En el modo *Análisis retrospectivo de IOC* de la tarea *Análisis de IOC*, Kaspersky Endpoint Security analiza los indicadores de vulneración mediante el uso de datos durante un período determinado. Este modo está diseñado para buscar indicadores de compromiso según la telemetría del equipo protegido, como la actividad de la red, los procesos, los archivos y otros tipos de telemetría. Puede establecer un período de 1-14 días. De forma predeterminada, la aplicación busca indicadores de vulneración durante un día.
`/network=on|off`	Análisis de datos de red (término NetworkItem).

`/url=on|off`	Análisis de datos en registros del navegador (término UrlHistoryItem). El Análisis retrospectivo de IOC examina los registros de los siguientes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versión 79 o posterior).
`/email`	Análisis de objetos de correo (término EmailItem).
`/route`	Análisis de tablas de enrutamiento y reenvío (término RouteEntryItem).

Valores de retorno del 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 con éxito (valor de retorno `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 del encabezado de la estructura del archivo de IOC (la etiqueta `<ioc id="">`)
`Name`	Descripción del archivo de IOC del 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 de MDR

Agregar el archivo de configuración de BLOB para activar Managed Detection and Response. El archivo BLOB contiene la ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. Encontrará el archivo BLOB en el archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre el archivo BLOB, consulte la Ayuda de Kaspersky Managed Detection and Response.

> Para realizar operaciones con el archivo BLOB, necesitará privilegios de administrador. También será necesario que los ajustes de Managed Detection and Response puedan editarse ( ) en la directiva.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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>	Aplicar el archivo de configuración BLOB para llevar a cabo la integración con Kaspersky Managed Detection and Response (archivo de formato P7). Solo se puede aplicar un único archivo BLOB. Si el equipo ya tiene un archivo BLOB, se lo reemplazará.
/DEL	Eliminar 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 con EDR (KATA)

Comandos para administrar el componente Endpoint Detection and Response (KATA):

- Habilitar o deshabilitar 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.

- Mostrar la configuración actual del componente.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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	Deshabilite el componente EDR (KATA).
start	Habilite el componente EDR (KATA).
set	Configure el componente EDR (KATA). Puede configuración las siguientes: • Agregue servidores de Central Node (servers=<server address>:<port>) • Agregue un certificado TLS (server-certificate=<path to the TLS certificate>) • Configure el tiempo de conexión agotado del servidor de Central Node (/timeout=<Central Node server connection timeout (s)>) • Configure 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.

KUMA. Integración con KUMA

Comandos para administrar el agente KUMA integrado:

- Habilitar o deshabilitar la integración con KUMA.

  El agente KUMA integrado proporciona interoperabilidad con la solución Kaspersky Unified Monitoring and Analysis Platform.

- Configurar la conexión a los servidores de Kaspersky Unified Monitoring and Analysis Platform.

- Mostrar la configuración actual del componente.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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	Deshabilitar la integración con KUMA.
start	Habilitar la Integración con KUMA.

`set`	Configure el agente KUMA integrado. Puede configuración las siguientes: • Agregue los servidores de KUMA (`/servers=<protocol>://<server address>:<port>`) La aplicación admite los siguientes protocolos de conexión con el servidor: `tcp`, `udp`, `http`, `https`. • Agregue un certificado TLS (`/server-certificate=<path to the TLS certificate>`) • Configure el tiempo de espera de la conexión al servidor (`/timeout=<KUMA server connection timeout (s)>`) • Agregue un contenedor criptográfico (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`). • Configure el retraso de transmisión de 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 YARA Scan

Ejecutando la tarea *Ejecutar análisis 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 de 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 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 se adhieren al 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 YARA* no es compatible con otros tipos de reglas.
- Si agregó archivos YARA que Kaspersky Endpoint Security no admite, o las reglas contienen errores de sintaxis, la tarea se anula y se muestra 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 YARA se cancela después de 128 coincidencias con los indicadores descritos en las reglas YARA. Esto es necesario para limitar la cantidad de entradas en el informe de análisis YARA de modo que sea más fácil de analizar y a fin de evitar que el informe se desborde 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 YARA puede demorar un tiempo considerable. Según el tamaño de la unidad, la configuración de la tarea y la cantidad de objetos en el disco, un análisis YARA puede tardar varios minutos o varias horas. La aplicación no muestra un indicador de progreso. No es posible detener o cancelar un análisis YARA. Recomendamos esperar hasta que los resultados del análisis 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 de YARA	
`<full path to the YARA file>`	Ruta completa al archivo de YARA que desea utilizar para analizar. Puede especificar rutas a varios archivos YARA separados con espacios. Argumento necesario si no se especifica el valor `/path=<path to the folder with YARA files>`. 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 analizar. Argumento necesario si no se especifica el valor `<full path to the YARA file>`. Ejemplo: `/path=C:\Users\Admin\Desktop\YARA`

La configuración avanzada	
`/fastScan=<on|off>`	Análisis 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 YARA rápido permite analizar archivos grandes más rápido. Si no se especifica esta configuración, la aplicación realiza un análisis YARA estándar. En este modo, la aplicación registra duplicados de indicadores detectados.
`/maxRules=<maximum number of scan rules>`	Límite del número de reglas únicas activadas que, al alcanzarse, hace que la aplicación detenga el análisis YARA. Si no se especifica el valor de esta configuración o si se especifica `0`, la aplicación realiza el análisis YARA sin limitaciones.
`/timeOut=<stop scan after the specified time in seconds>`	Cuánto tiempo puede tomar un análisis YARA, en segundos. Cuando se agota este tiempo, la aplicación detiene el análisis YARA. Si no se especifica el valor de esta configuración o si se especifica `0`, la aplicación realiza el análisis YARA sin limitaciones.
`/recursive=<on|off>`	Este argumento inicia un análisis recursivo de subcarpetas dentro del Análisis personalizado de `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Este argumento inicia un análisis YARA de archivos en la lista de carpetas especificada. Puede especificar varios valores separados por espacios. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara para una ruta de acceso a carpeta. Si no se especifica esta configuración, la aplicación realiza un análisis YARA de todos los discos locales, excepto los recursos compartidos de red, las unidades de 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 los procesos especificados. Especifique rutas completas separadas por espacios a los archivos ejecutables de los procesos. Puede usar los caracteres `*` y `?` para ingresar una máscara.
`/maxSize=<file size in bytes>`	Limitar el tamaño del archivo para el análisis YARA. La aplicación omite los archivos más grandes.

`/includes=<list of objects to be scanned>`	Edite el alcance del análisis. Puede especificar varios valores separados por espacios. Estos son los valores disponibles: • Nombre de archivo • Extensión de archivos El alcance del análisis debe especificarse con el parámetro `/scanFolders`. Ejemplo: `/scanFolders C:\*.* /includes=*.exe *.dll`: la aplicación analiza todos los archivos en el disco C que tienen las extensiones EXE y DLL.
`/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 de archivo • Máscara de la ruta del archivo Las exclusiones deben especificarse 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 del disco C.
`/scanAutoruns=<on|off>`	Análisis YARA de objetos de puntos de ejecución automática.
`/excludeAutoruns=<list of autorun point areas to skip>`	Excluir objetos de puntos de ejecución automática del alcance del análisis. Especifique rutas completas separadas por espacios a los archivos ejecutables de los procesos. Puede usar los caracteres `*` y `?` para ingresar 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 del 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 encontraron uno o más archivos con las reglas YARA especificadas en el parámetro.

Si el comando se ejecutó con éxito (valor de retorno `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 de error del error que ocurrió al ejecutar la tarea. Si no hay errores, la aplicación muestra un resultado `0x00000000`.
`Comment: <comment text>`	Descripción del error que ocurrió al ejecutar la tarea. Por ejemplo, `Operation timeout`.
`Object Name:` o `Process:` (al analizar la memoria del proceso)	El nombre del objeto o proceso en el que se activó la regla YARA.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hashes del objeto en 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 encontraron coincidencias dentro del objeto que cumplen con las condiciones de la regla YARA:
	• Desplazamiento en la memoria del proceso o 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 del proceso o en el archivo (`String data`).

TELEMETRYFILTERS. Filtrar eventos para enviar a KUMA

De manera predeterminada, el envío de eventos al servidor KUMA está deshabilitado. Para asegurarse de que KUMA funcione correctamente, debe habilitar el envío de telemetría. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*. Para mejorar el rendimiento y optimizar la transmisión de datos al servidor de KUMA, puede agregar o excluir eventos individuales de la telemetría de forma manual. 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 coloca el archivo de la siguiente manera:

- Si la ruta a avp.com se agrega a la variable de sistema %PATH%, la aplicación coloca el archivo en la carpeta `C:\Windows\SysWOW64`.
- Si ejecuta el comando desde la carpeta de instalación de la aplicación, la exportación fallará debido a que la autoprotección de la aplicación bloquea la creación de un nuevo archivo en la carpeta de la aplicación. Para exportar los ajustes de configuración de la aplicación a un archivo, ingrese la ruta del archivo.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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`	Exportar filtros de eventos que se enviarán a KUMA.
`import`	Importar filtros de eventos que se enviarán a KUMA. Si ya existen reglas de filtrado de eventos en la computadora, Kaspersky Endpoint Security las reemplaza al importar.

Archivo para exportar o importar	
`<file name>`	Nombre del archivo con los filtros de eventos que se enviarán a KUMA. También puede escribir la ruta del archivo. Puede exportar filtros para enviar a KUMA a un archivo JSON.

Comandos de administración de Light Agent

Puede administrar la aplicación en modo de Light Agent para proteger entornos virtuales en la línea de comandos. Puede administrar la aplicación en el modo de Light Agent si la administración mediante el uso de la consola de Kaspersky Security Center no es posible. Para ver la lista de comandos de administración disponibles, ejecute el comando `HELP`. Para conocer la sintaxis de un comando específico, escriba `HELP <command>`.

Para administrar la aplicación en el modo de Light Agent desde la línea de comandos:

1. Abra el símbolo del sistema (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 el modo de Light Agent es compatible con casi todos los comandos de AVP de la aplicación instalada en el modo estándar. En el modo de Light Agent, las tareas de actualización de bases de datos antivirus y las tareas de administración de claves de licencia son limitadas.

KSVLAINFO. Determinación del modo de Light Agent

Determinación del modo de Light Agent.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 de Light Agent para proteger entornos virtuales: habilitado o deshabilitado.

  Si el modo de Light Agent está habilitado, la aplicación se utiliza como parte de la solución Kaspersky Security for Virtualization Light Agent.

- Modo de protección de VDI: habilitado o deshabilitado.

  El modo de protección VDI permite optimizar el rendimiento de Kaspersky Endpoint Security en máquinas virtuales no persistentes. Si el modo de protección de VDI está habilitado, las actualizaciones que exigen el reinicio de la máquina virtual protegida no se instalan en las máquinas virtuales no persistentes. Al recibir actualizaciones que exigen un reinicio, el Light Agent instalado en una máquina virtual no persistente envía un mensaje a Kaspersky Security Center para informar 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 con el Servidor de integración

Visualización de información sobre la conexión del Light Agent con el Servidor de integración.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 la conexión del Servidor de integración.
- Fecha y hora de la última conexión del Light Agent con el Servidor de integración.

SVMINFO. Estado de la conexión del Light Agent con el Servidor de protección

Ver información sobre la conexión del Light Agent con el Servidor de protección.

Para ejecutar el comando, vaya a la carpeta en la que se encuentra el archivo ejecutable de Kaspersky Endpoint Security. También puede agregar 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 ubicación de la SVM en la infraestructura virtual relativa al Light Agent: local o no local.
- Método de detección de la SVM que utiliza el Light Agent: mediante un Servidor de integración o mediante una lista personalizada de direcciones de SVM.

- Lista de direcciones de SVM si se selecciona la lista de direcciones de SVM como el método de detección de la SVM.
- Etiqueta para conectar el Light Agent a la SVM.
- Algoritmo de selección de SVM: estándar o extendido. Si se utiliza el algoritmo de selección de SVM extendido, también se muestra el tipo de ruta de SVM en la infraestructura virtual.
- Estado de la 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'`. De forma complementaria, Kaspersky Endpoint Security puede mostrar un código como `error=8947906D` (consulte la siguiente tabla).

Códigos de error

Código de error	Descripción
09479001	Esta clave ya está en uso
0947901D	La licencia caducó. La actualización de la base de datos no está disponible
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 caducó
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	Biblioteca de licencias sin cargar
8947900F	Bases de datos dañadas o actualizadas manualmente
89479010	Las bases de datos están dañadas
89479011	No se puede usar un archivo de clave no válido para agregar 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 correspondiente a una licencia de prueba 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 se puede activar con un archivo de clave que corresponda a otra aplicación. Verifique cuál es la aplicación instalada
89479018	Clave de licencia bloqueada por Kaspersky

Código de error	Descripción
89479019	Ya se usó la licencia de prueba para esta aplicación. No se puede agregar una clave para una licencia de prueba nuevamente
8947901A	El archivo de clave está dañado
8947901B	No se encuentra la firma digital, está dañada o no corresponde con la firma digital de Kaspersky
8947901C	No se puede agregar una clave si la licencia no comercial correspondiente ha caducado
8947901E	La fecha de creación o uso del archivo de clave no es válida. Compruebe la fecha del sistema
8947901F	No se puede agregar un archivo de clave para la licencia de prueba: otra licencia de prueba ya está activa
89479020	Falta la lista de claves rechazadas o la lista existente está dañada
89479021	Descripción de la actualización dañada o faltante
89479022	La clave no es adecuada para esta aplicación
89479023	No se puede usar un archivo de clave no válido para agregar una clave de reserva
89479025	Error al enviar la solicitud del servidor de activación. Motivos probables: error de 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 el error persiste, comuníquese con su proveedor de Internet
89479026	La petición contiene un código de activación incorrecto
89479027	No se pude obtener el estado de la respuesta
89479028	Se produjo un error al guardar el archivo temporal
89479029	Se escribió un código de activación incorrecto o la fecha del sistema en el equipo no es válida. Controle la fecha del sistema en el equipo
8947902A	Clave no compatible con esta aplicación o licencia caducada
8947902B	Error al recibir el archivo de clave. Se escribió 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 su 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 para usar el proxy. Revise la configuración de red
89479033	Se agotó 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 su 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	Respuesta de puerta de enlace no válida. Compruebe la configuración de red
8947903F	Recurso no disponible temporalmente
89479040	Se agotó el tiempo de espera de la respuesta de la puerta de enlace. Compruebe la configuración de red

Código de error	Descripción
89479041	El protocolo no es compatible con el servidor
89479043	Error de HTTP desconocido
89479044	Id. de recurso no válido
89479046	URL no válida
89479047	Carpeta de destino no válida
89479048	Error de asignación de memoria
89479049	Error al convertir los parámetros a una cadena ANSI (URL, carpeta, agente)
8947904A	Error al crear subproceso de trabajo
8947904B	El subproceso de trabajo ya está en ejecución
8947904C	El subproceso de trabajo no está en ejecución
8947904D	No se encuentra el archivo de clave en el servidor de activación
8947904E	La clave está bloqueada
8947904F	Error interno del servidor de activación
89479050	Datos insuficientes en la solicitud de activación
89479053	La licencia que corresponde a la clave agregada ya ha caducado
89479054	Fecha del sistema no válida en el equipo. Controle el valor de la fecha del sistema
89479055	La licencia de prueba ha caducado
89479056	Período de activación de la aplicación caducado
89479057	Se superó la cantidad de activaciones que permite el código especificado
89479058	Proceso de activación completado con Error del sistema
89479059	No se puede utilizar una clave correspondiente a una licencia de prueba como clave para una licencia comercial
8947905C	Se requiere un código de activación
89479062	No se puede establecer conexión con el servidor de activación
89479064	El servidor de activación no está disponible. Asegúrese de que tiene conexión a Internet y vuelva a intentarlo
89479065	La licencia caducó
89479066	No se puede reemplazar la clave activa con una clave caducada
89479067	No se puede agregar una clave de reserva cuando la licencia correspondiente caduca antes que la licencia vigente
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 correspondientes a las claves activa y de reserva no coinciden
8947906D	Componente no compatible con la licencia
8947906E	No se puede agregar una clave de suscripción como clave de reserva
89479213	Error genérico de capa de transporte
89479214	No se pudo conectar al servidor de activación
89479215	La dirección web no tiene un formato válido
89479216	No se pudo convertir la dirección del servidor proxy
89479217	No se pudo convertir la dirección del servidor. Verifique la configuración de conexión a Internet
89479218	El intento de conexión con el servidor falló

Código de error	Descripción
89479219	Acceso denegado de manera remota
8947921A	Se agotó el tiempo de espera de la operación
8947921B	Error al enviar la solicitud HTTP
8947921C	Error de conexión SSL
8947921D	Operación interrumpida por devolución de llamada
8947921E	Hay demasiadas redirecciones
8947921F	Error de comprobación de destinatario
89479220	Respuesta vacía del servidor
89479221	Error a 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	Contenido de paquete de red no válido
89479227	Acceso a la cuenta denegado
89479228	Archivo de certificado SSL no válido
89479229	No se puede cerrar la conexión SSL
8947922A	Error recurrente
8947922B	Archivo no válido con certificados revocados
8947922C	Error de solicitud de certificado SSL
89479401	Error de servidor desconocido
89479402	Error interno del servidor
89479403	No hay una clave disponible para el código de activación escrito
89479404	Clave activa bloqueada
89479405	No se encuentran los 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 este programa. Kaspersky Endpoint Security para Windows no se puede activar con un archivo de clave que corresponda a otra aplicación. Verifique cuál es la aplicación instalada
89479409	Se requiere un código de activación
8947940B	Periodo de activación finalizado
8947940C	Se superó el número de activaciones con este código
8947940D	Formato de id. de solicitud no válido
8947940E	Código de activación ya 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 esta aplicación. Obtenga un código diferente para activar la versión instalada de la aplicación
89479413	El servidor de activación devolvió el error 643

Código de error	Descripción
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 necesita la versión 1.0 del servidor de activación
89479418	El formato del código de activación no es correcto
89479419	La hora del equipo no está sincronizada con la hora del servidor de activación
8947941A	Versión de la aplicación incorrecta
8947941B	La suscripción caducó
8947941C	Cantidad de activaciones superada
8947941D	Firma del vale no válida
8947941E	Se requieren datos adicionales
8947941F	Falla al comprobar los datos
89479420	Suscripción inactiva
89479421	El servidor de activación está en mantenimiento
89479501	Error inesperado
89479502	Parámetro transferido no válido. Por ejemplo, una lista vacía de direcciones de servidores 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 de servidor de activación
89479507	La solicitud de activación ha sido interrumpida
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 vía 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 contra amenazas de red
- `IntegrityCheck`: Comprobación de integridad
- `LogInspector`: Inspección de registro
- `Mail_Monitoring` o `EM`: Protección contra amenazas de correo
- `Rollback`: Reversión de la actualización (el perfil no se puede aplicar si la aplicación está instalada en el modo de Light Agent)
- `Scan_ContextScan`: Análisis desde el menú contextual
- `Scan_IdleScan`: Análisis en segundo plano
- `Scan_Memory`: Análisis de 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 el modo de Light Agent)
- `Web_Monitoring` o `WM`: Protección contra 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 Servicio de soporte técnico de Kaspersky.

Uso de la API REST para administrar la aplicación

Si lo desea, puede utilizar una solución desarrollada por un tercero para configurar los ajustes de Kaspersky Endpoint Security, realizar análisis, actualizar las bases de datos antivirus y llevar a cabo otras tareas. La API de Kaspersky Endpoint Security se ha diseñado para ello. La API REST de Kaspersky Endpoint Security funciona sobre el protocolo HTTP y consiste de una serie de métodos de solicitud-respuesta. Gracias a ello, Kaspersky Endpoint Security puede administrarse a través de soluciones de terceros, y no únicamente con la interfaz local de la aplicación o mediante la Consola de administración de Kaspersky Security Center.

Si comienza a utilizar la API REST, deberá instalar Kaspersky Endpoint Security con las opciones necesarias para permitir el uso de la API REST. El cliente de REST que utilice deberá estar instalado en el mismo equipo que Kaspersky Endpoint Security.

Para garantizar que Kaspersky Endpoint Security y el cliente de REST interactúen en forma segura, haga lo siguiente:

- Configure la protección del cliente de REST para evitar accesos sin autorización según las recomendaciones del desarrollador del cliente de REST. Configure la protección de la carpeta del cliente de REST para evitar la escritura con la ayuda de la lista de control de acceso discrecional (LCAD).
- Para ejecutar el cliente de REST, utilice una cuenta diferente con derechos de administrador. Rechace el inicio de sesión interactivo al sistema para esta cuenta.

El acceso a la API REST es a través de http://127.0.0.1 o http://localhost. La API REST no puede utilizarse para administrar Kaspersky Endpoint Security en forma remota.

ABRIR LA DOCUMENTACIÓN DE LA API REST

Habilitar el uso de la API REST al instalar la aplicación

Si desea administrar la aplicación mediante REST API, deberá habilitar la compatibilidad con dicha API al instalar Kaspersky Endpoint Security. Si opta por utilizar la API REST, no podrá administrar Kaspersky Endpoint Security a través de Kaspersky Security Center.

Preparación para instalar la aplicación a través de la API REST

La interacción segura de Kaspersky Endpoint Security con el cliente de REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga de cada solicitud.

Para crear un certificado, puede usar, por ejemplo, OpenSSL.

Ejemplo:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Use el algoritmo de cifrado RSA con una longitud de clave de 2048 bits o más.

De esta manera, obtendrá un certificado `cert.pem` y una clave privada `key.pem`.

Instalación de la aplicación a través de la API REST

Para instalar Kaspersky Endpoint Security con las opciones necesarias para usar la API REST:

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security (versión 11.2.0 o posterior).
3. Instale Kaspersky Endpoint Security con los siguientes parámetros:
   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Nombre de usuario que se utilizará para administrar la aplicación a través de la API REST. El nombre de usuario debe especificarse en formato `<DOMAIN>\<UserName>` (por ejemplo, `RESTAPI_User=COMPANY\Administrator`). La cuenta que defina aquí será la única que podrá administrar la aplicación con la API REST. El uso de la API REST está limitado a un único usuario.
   - `RESTAPI_Port=<port>`

     Puerto que se usará para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782. Asegúrese de que el puerto esté libre. Este parámetro es opcional.
   - `RESTAPI_Certificate=<path to certificate>`

     Certificado para reconocer 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 la API REST

     1. Deshabilitar Autoprotección de Kaspersky Endpoint Security

        El mecanismo de autoprotección impide que se modifiquen o se eliminen los archivos, los procesos en memoria y las entradas del Registro correspondientes a la aplicación.
     2. Vaya a la clave del registro que contiene la configuración de la API REST: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Ingrese la ruta del certificado, por ejemplo, `Certificate = C:\Folder\cert.pem`.
     4. Habilitar Autoprotección de Kaspersky Endpoint Security.
     5. Reiniciar aplicación.
   - `AdminKitConnector=1`

     Permitir que la aplicación se administre a través de un sistema de administración. Esta posibilidad está habilitada por defecto.

Los parámetros para utilizar la API REST también se pueden definir en el archivo setup.ini.

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 utilizar la REST API para administrar la aplicación. Para verificar que todo funcione correctamente, envíe una solicitud GET para ver la documentación de la API REST.

Ejemplo:
```
GET http://localhost:6782/kes/v1/api-docs
```

Si instaló la aplicación a través de la API REST, Kaspersky Endpoint Security crea automáticamente una regla de habilitación en la configuración de Control web para acceder a los recursos web (*Regla de servicio para API REST*). Esta regla es necesaria para permitir que el cliente REST acceda a Kaspersky Endpoint Security en todo momento. Por ejemplo, si restringió el acceso de los usuarios a los recursos web, esto no afectará la administración de la aplicación mediante la API REST. Se recomienda que no elimine la regla ni cambie la configuración de la *Regla de servicio de la API REST*. Si eliminó la regla, Kaspersky Endpoint Security la restaurará tras reiniciar la aplicación.

Uso de la API

La característica de protección con contraseña no puede utilizarse para restringir la capacidad de acceder a la aplicación con la API REST. Por ejemplo, no es posible impedir que una persona utilice la API REST para deshabilitar la protección. Por el contrario, la API REST sí puede utilizarse para configurar la protección con contraseña y limitar el acceso de los usuarios a la interfaz local de la aplicación.

Para administrar la aplicación a través de la REST API, deberá ejecutar un cliente de REST con la cuenta especificada al habilitar el uso de esta API durante la instalación de la aplicación. El uso de la API REST está limitado a un único usuario.

ABRIR LA DOCUMENTACIÓN DE LA API REST

El proceso para administrar la aplicación a través de la API REST se divide en los siguientes pasos:

1. Obtener los valores de configuración vigentes en la aplicación. Para ello, 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 configuración. Kaspersky Endpoint Security admite los formatos XML y JSON.

   Ejemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Modificar la configuración de la aplicación. Utilice la estructura de configuración que obtuvo en la respuesta a la solicitud GET inicial.

Ejemplo:

```
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Guarde la configuración de la aplicación (la carga) en un archivo JSON (payload.json).

5. Firme el archivo 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
   ```

   De esta manera, obtiene un archivo firmado con la carga de la solicitud (`signed_payload.pem`).

6. Modificar la configuración de la aplicación. Para hacerlo, envíe una solicitud POST y adjunte el archivo firmado con la carga de la solicitud (`signed_payload.pem`).

La aplicación aplica la nueva configuración y envía una respuesta que contiene los resultados de la configuración de la aplicación (la respuesta puede estar vacía). Puede comprobar que la configuración se actualice mediante el uso de una solicitud GET.

Fuentes de información acerca de la aplicación

Esta sección describe las fuentes de información acerca de la aplicación.

Puede seleccionar la fuente de información más conveniente dependiendo de la importancia y urgencia del tema.

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 y sus funciones y características.

La página de Kaspersky Endpoint Security contiene un vínculo a la tienda en línea. Allí puede comprar o renovar la aplicación.

Página de Kaspersky Endpoint Security en la Base de conocimientos

Base de conocimientos es una sección en el sitio web de soporte técnico.

En la página de Kaspersky Endpoint Security en la Base de conocimientos, puede leer artículos que brindan información útil, recomendaciones y respuestas a preguntas frecuentes sobre cómo comprar, instalar y usar la aplicación.

Los artículos de la base de conocimientos pueden tener respuestas 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 del soporte técnico.

Debate sobre las aplicaciones de Kaspersky en el foro

Si su pregunta no requiere una respuesta urgente, puede debatir sobre eso con los expertos de Kaspersky y otros usuarios en nuestro Foro.

En el foro, puede ver los temas existentes, publicar sus propios comentarios y crear nuevos temas de debate.

Contacto con Soporte técnico

Si no puede encontrar una solución a su problema en la documentación o en ninguna de las fuentes de información sobre Kaspersky Endpoint Security, le recomendamos que se ponga en contacto con Soporte técnico. Soporte técnico responderá sus preguntas acerca de la instalación y el uso de Kaspersky Endpoint Security.

Kaspersky se compromete a brindar asistencia técnica para Kaspersky Endpoint Security a lo largo de su ciclo de vida (el cual se detalla en esta página). Antes de ponerse en contacto con el soporte técnico, lea primero las reglas de soporte.

Puede comunicarse con el Servicio de soporte técnico de las siguientes maneras:

- Visitando el sitio web del soporte técnico
- Enviando una solicitud al Servicio de soporte técnico de Kaspersky por medio del portal de Kaspersky CompanyAccount.

Después de informar su problema a los especialistas del Servicio de soporte técnico de Kaspersky, posiblemente le soliciten que cree un *archivo de seguimiento*. El archivo de rastreo le permite hacer un seguimiento del proceso de ejecución de comandos de aplicaciones paso a paso y determinar la etapa del funcionamiento de una aplicación en la cual se produce un error.

Es posible que los especialistas del Servicio de soporte técnico también le soliciten información adicional sobre el sistema operativo, los procesos que se están ejecutando en el equipo, los informes detallados sobre el funcionamiento de los componentes de las aplicaciones.

Mientras ejecuta un diagnóstico, los representantes del Servicio de soporte técnico pueden pedirle que cambie la configuración de la aplicación por medio de las siguientes acciones:

- Activar una función que permitirá recibir información de diagnóstico extendida.
- Configurar componentes individuales de la aplicación valiéndose de configuraciones especiales a las que no se puede acceder con la interfaz de usuario estándar.
- Cambiar opciones relativas al almacenamiento de la información de diagnóstico.
- Configurar la intercepción y el registro del tráfico de red.

Los expertos del Servicio de 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 mencionadas deben llevarse a cabo solamente bajo la supervisión de especialistas del Servicio de soporte técnico siguiendo sus instrucciones. Modificar la configuración de la aplicación por cuenta propia y de maneras no indicadas en la Ayuda en línea o recomendadas por el Servicio de soporte técnico puede provocar fallos y problemas de rendimiento en el sistema operativo, reducir el nivel de protección del equipo y afectar la disponibilidad e integridad de la información procesada.

Contenidos y almacenamiento de los archivos de rastreo

> Usted tiene la responsabilidad personal de garantizar que los datos almacenados en su equipo se mantengan protegidos. En particular, es responsable de controlar y restringir el acceso a esta información hasta que se la envíe a Kaspersky.

Los archivos de seguimiento quedarán guardados en el equipo mientras la aplicación esté instalada; cuando desinstale la aplicación, los archivos se eliminarán de forma permanente.

Los archivos de seguimiento, excepto los del Agente de autenticación, se almacenan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`.

El nombre de los archivos de seguimiento sigue este formato: `KES<14.1_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Puede ver los datos guardados en los archivos de rastreo.

Todos los archivos de rastreo tienen los siguientes datos comunes:

- Hora del evento
- Número del hilo de ejecución

  > El archivo de seguimiento del Agente de autenticación no contiene esta información.

- Componente de la aplicación que causó el evento
- Gravedad del evento (evento informativo, advertencia, evento crítico, error)
- Una descripción del evento que involucra la ejecución del comando por un componente de la aplicación y el resultado de la ejecución de ese comando.

Contenido de los archivos de rastreo 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, como apellido, nombre de pila y segundo nombre, si esos datos se incluyen en la ruta a los archivos en el equipo local.
- Datos sobre el hardware instalado en el equipo (por ejemplo, datos de la BIOS o del firmware UEFI). Esta información se guarda en los archivos de seguimiento cuando se utiliza la función de cifrado de disco de Kaspersky.
- El nombre de usuario y la contraseña si se transmitieron en forma abierta. Estos datos se pueden registrar en los archivos de rastreo durante el análisis de tráfico de Internet.

- El nombre de usuario y la contraseña si están contenidos en los encabezados HTTP.
- El nombre de la cuenta de Microsoft Windows si el nombre de cuenta se incluye en el nombre del archivo.
- Su dirección de correo electrónico o una dirección web que contenga el nombre de su cuenta y contraseña si están contenidos en el nombre del objeto detectado.
- Los sitios web que visita y se redirige desde esos sitios. Estos datos se escriben en los archivos de rastreo cuando la aplicación analiza sitios web.
- Dirección del servidor proxy, nombre del equipo, puerto, dirección IP y nombre de usuario para iniciar sesión en el servidor proxy. Estos datos se escriben en los archivos de rastreo si la aplicación utiliza un servidor proxy.
- Direcciones IP remotas con las que su equipo estableció conexiones.
- Sujeto del mensaje, identificador, nombre del remitente y dirección del sitio web del remitente del mensaje en una red social. Estos datos se escriben en los archivos de rastreo si está activado el componente Control web.
- Datos sobre el tráfico de red. Esta información se guarda en los archivos de seguimiento cuando se han habilitado los componentes de monitoreo del tráfico (por ejemplo, Control web).
- Datos recibidos de los servidores de Kaspersky (por ejemplo, la versión de las bases de datos antivirus).
- Estados y datos operativos de los componentes de Kaspersky Endpoint Security.
- Datos sobre las actividades 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 los datos generales, el archivo de seguimiento `HST.log` contiene información sobre la ejecución de una tarea de actualización de la base de datos y del módulo de la aplicación.

Además de los datos generales, el archivo de seguimiento `BL.log` contiene información sobre los eventos que ocurrieron durante la operación de la aplicación, como así también de los datos necesarios para la resolución de problemas de errores de la aplicación. El archivo se crea si la aplicación se inicia con el parámetro avp.exe –bl.

Además de los datos generales, el archivo de seguimiento `Dumpwriter.log` contiene información del servicio necesaria para la resolución de errores que ocurren cuando se escribe el archivo de volcado de la aplicación.

Además de los datos generales, el archivo de seguimiento `WD.log` contiene información sobre los eventos que ocurrieron durante el funcionamiento del servicio avpsus, incluyendo los eventos de actualización de módulos de la aplicación.

Además de los datos generales, el archivo de seguimiento `AVPCon.dll.log` contiene información sobre los eventos que ocurrieron durante la operación 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 tiene este formato: `KES<14.1_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 del archivo de seguimiento del componente Protección vía AMSI

Además de los datos generales, el archivo de seguimiento `AMSI.log` contiene información sobre los resultados del análisis realizado en solicitudes de aplicaciones de terceros.

Contenidos de los archivos de seguimiento del componente Protección contra amenazas de correo

El archivo de seguimiento `mcou.OUTLOOK.EXE.log` puede contener partes de mensajes de correo electrónico, incluidas las direcciones de correo electrónico, además de datos generales.

Contenidos de los archivos de seguimiento del componente Análisis desde menú contextual

El archivo de seguimiento `shellex.dll.log` contiene información sobre la finalización de la tarea de análisis y los datos requeridos para depurar la aplicación, además de información general.

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 instaló 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 de Internet (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.

Contenido del archivo de seguimiento del Agente de autenticación

El archivo de seguimiento del Agente de autenticación se guarda en la carpeta System Volume Information y tiene el siguiente nombre: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Además de los datos generales, el archivo de seguimiento del Agente de autenticación contiene información sobre el funcionamiento del Agente de autenticación y las acciones realizadas por el usuario con el Agente de autenticación.

Seguimiento de la operación de aplicaciones

Los *archivos de seguimiento de la aplicación* contienen un registro detallado de las acciones que la aplicación realiza, así como de los mensajes sobre los eventos que ocurren cuando la aplicación está en funcionamiento. Durante el proceso de seguimiento, 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 seguimiento de la aplicación solo debe utilizarse bajo la supervisión del Servicio de soporte técnico de Kaspersky.

Para crear un archivo de seguimiento de la aplicación:

1. En la ventana principal de la aplicación haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Herramientas de soporte**.
3. Use el interruptor **Habilitar seguimiento de la aplicación** para habilitar o deshabilitar el seguimiento del funcionamiento de la aplicación.

4. En la lista desplegable **Seguimiento**, seleccione un modo de seguimiento de la aplicación:

   - **Con limitación de tamaño**. Guardar los datos de seguimiento en un número limitado de conjuntos 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 la cantidad máxima de conjuntos de archivos para la rotación y el tamaño máximo de cada archivo.

     De manera predeterminada, la aplicación guarda cinco conjuntos de archivos de seguimiento. El tamaño de cada conjunto de archivos es de 3072 MB. De esta manera, necesita 15 GB de espacio libre en disco para guardar los archivos de seguimiento.

   - **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 rastreo guarda mensajes acerca de todos los errores, advertencias, así como información acerca del funcionamiento normal de la aplicación (predeterminado).

   - **Detallado** significa que el archivo de rastreo guarda toda la información acerca del funcionamiento de la aplicación.

   Los niveles de seguimiento adicionales están disponibles si administra la configuración de seguimiento de la aplicación en la línea de comandos. En lo posible, pregúntele por el nivel de seguimiento indicado a un especialista del servicio de soporte técnico. A falta de esta información, use el nivel de seguimiento **Normal**.

   > Si se habilitó el seguimiento de la aplicación en la línea de comandos y se estableció un nivel de seguimiento diferente al **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 deshabilite el seguimiento.

> También puede crear archivos de seguimiento al instalar la aplicación; para ello, realice la instalación a través de la línea de comandos o utilice el archivo setup.ini.

Como resultado, los archivos de seguimiento de las operaciones de la aplicación se crean en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Envíe esos archivos al servicio de soporte técnico de Kaspersky.

Kaspersky Endpoint Security elimina automáticamente los archivos de seguimiento cuando se elimina la aplicación. También puede eliminar los archivos de manualmente. Para ello, debe deshabilitar el seguimiento y detener la aplicación.

Seguimiento 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 *seguimiento 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 servicio de soporte técnico de Kaspersky.

La función de seguimiento de la aplicación solo debe utilizarse bajo la supervisión del Servicio de soporte técnico de Kaspersky.

Para crear un archivo de seguimiento del rendimiento:

1. En la ventana principal de la aplicación haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Herramientas de soporte**.
3. Use el interruptor **Habilitar seguimiento del rendimiento** para habilitar o deshabilitar el seguimiento del rendimiento de las aplicaciones.
4. En la lista desplegable **Seguimiento**, 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:
   - **Básico**. Kaspersky Endpoint Security analizará los procesos del sistema operativo relacionados con el rendimiento más importantes.
   - **Detallado**. Kaspersky Endpoint Security analizará todos los procesos del sistema operativo relacionados con el rendimiento.
6. En la lista desplegable **Tipo de seguimiento**, seleccione el tipo de seguimiento:
   - **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, regrese a la ventana Herramientas de soporte y deshabilite el seguimiento.

Como resultado, se crea un archivo de seguimiento del rendimiento en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Envíe ese archivo al servicio de soporte técnico de Kaspersky.

Creación de archivos de volcado

Un archivo de volcado contiene toda información sobre la memoria operativa de los procesos de Kaspersky Endpoint Security en el momento en que se creó el archivo de volcado.

> Los archivos de volcado guardados pueden contener datos confidenciales. Usted es responsable de velar por la seguridad de estos archivos y controlar el acceso a los datos.

Los archivos de volcado se almacenan en su equipo de una forma modificada que no puede leerse mientras la aplicación está en uso y se eliminan en forma permanente cuando se desinstala la aplicación. Los archivos de volcado se almacenan en la carpeta `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`.

Cómo habilitar la escritura en archivos 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 correspondiente 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 para depuración**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, use la casilla **Habilitar escritura en archivos de volcado** para habilitar o deshabilitar la escritura en archivos de volcado de la aplicación.

6. Guarde los cambios.

Cómo habilitar la escritura en archivos 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 ficha **Configuración de la aplicación**.

4. Vaya a **Configuración general** → **Servicio de soporte técnico**.

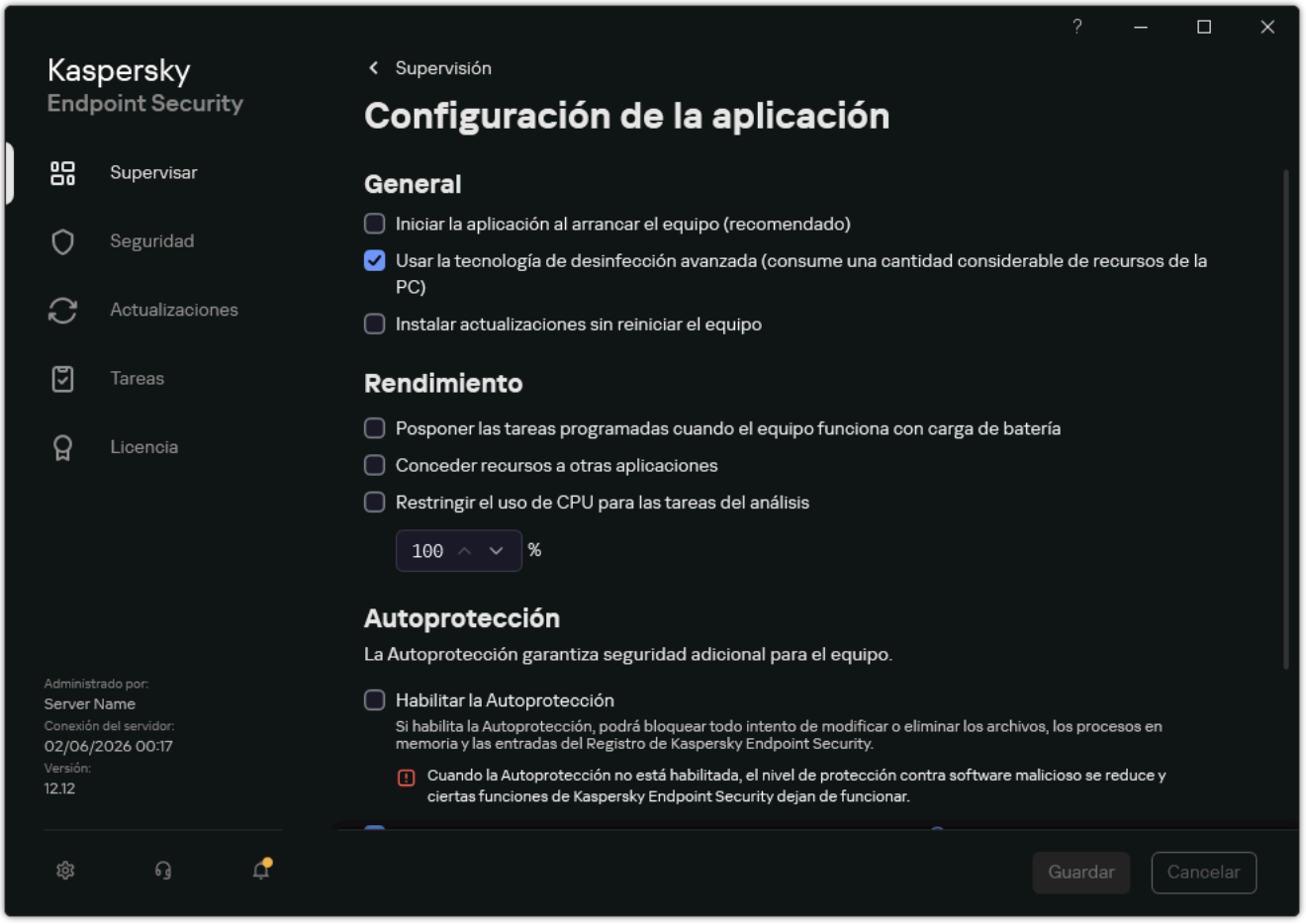
5. En el bloque **Información para depuración**, use la casilla **Escritura de volcado HABILITADA** para habilitar o deshabilitar la escritura de volcado de la aplicación.

6. Guarde los cambios.

Cómo habilitar la escritura en archivos de volcado en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 para depuración**, use la casilla **Habilitar escritura en archivos de volcado** para habilitar o deshabilitar la escritura de volcado de la aplicación.

4. Guarde los cambios.

Protección de los archivos de volcado y de seguimiento

Los archivos de volcado y los archivos de rastreo contienen la información sobre el sistema operativo y también pueden contener datos del usuario. Para evitar el acceso no autorizado a dichos datos, puede habilitar la protección de archivos de volcado y de rastreo.

Si la protección de archivos de volcado y de rastreo está activada, los siguientes usuarios podrán acceder a los archivos:

- El administrador del sistema y el administrador local, además del usuario que activó la escritura de los archivos de volcado y de rastreo pueden acceder a los archivos de volcado.

- Solo el administrador del sistema y el administrador local pueden acceder a los archivos de rastreo.

Cómo habilitar la protección de archivos de volcado y archivos de seguimiento 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 correspondiente 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 para depuración**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, use la casilla **Habilitar la protección de los archivos de volcado y de seguimiento** para habilitar o deshabilitar la protección de archivos.
6. Guarde los cambios.

Cómo habilitar la protección de archivos de volcado y archivos de seguimiento en Web Console y Cloud Console

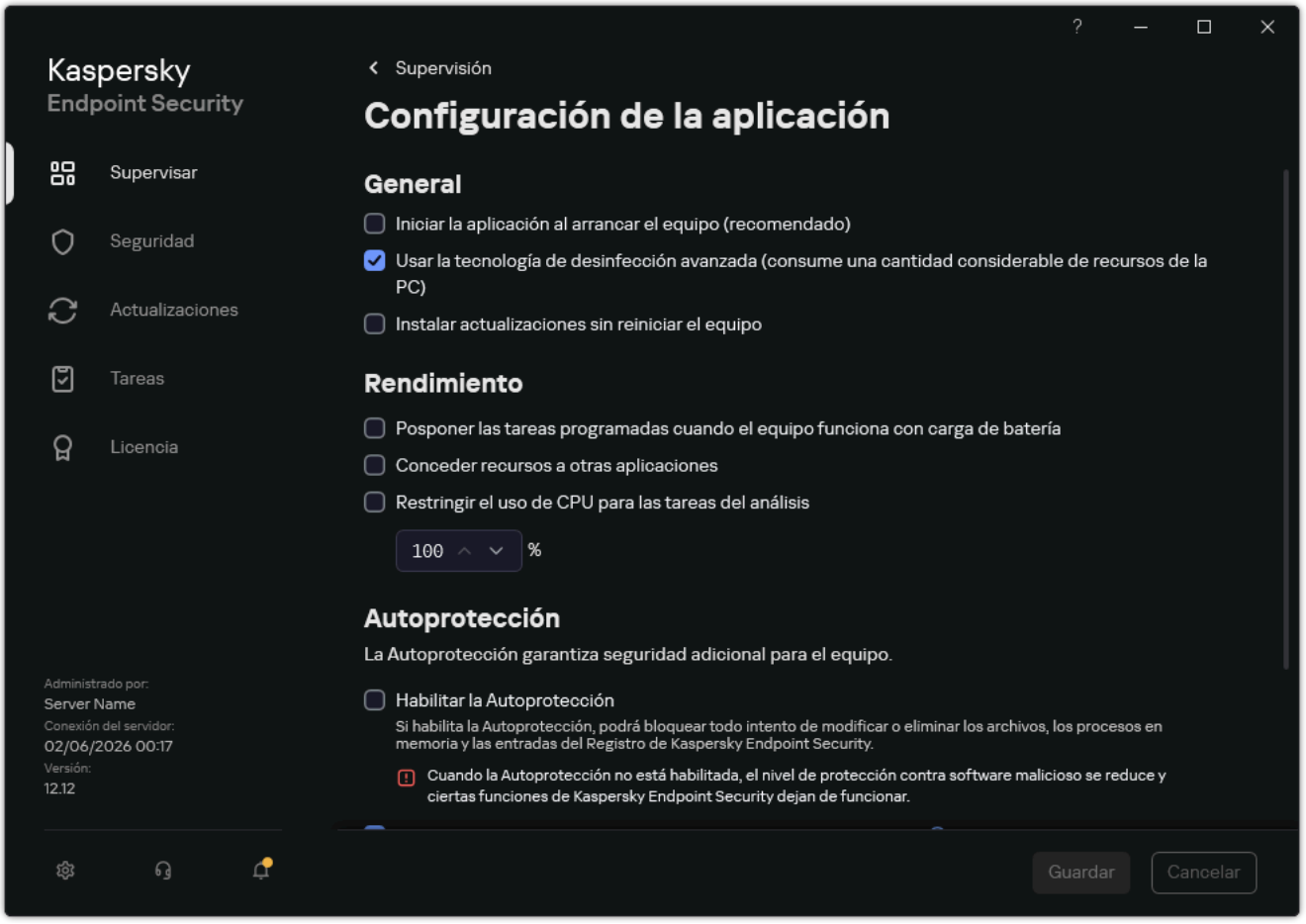
1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Servicio de soporte técnico**.
5. En el bloque **Información para depuración**, use la casilla **Protección de archivos de volcado y seguimiento HABILITADA** para habilitar o deshabilitar la protección de archivos.
6. Guarde los cambios.

Cómo habilitar la protección de archivos de volcado y archivos de seguimiento en la interfaz de la aplicación

1. En la ventana principal de la aplicación 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 para depuración**, use la casilla **Habilitar la protección de los archivos de volcado y de seguimiento** para habilitar o deshabilitar la protección de archivos.

4. Guarde los cambios.

Los archivos de volcado y de rastreo que se escribieron con la protección activa permanecen protegidos incluso luego de deshabilitar esta función.

Obtención de datos del sistema operativo (Kaspersky Get System Info)

Luego de instalar la aplicación Kaspersky Endpoint Security, es posible que el sistema operativo o alguna aplicación no funcionen de forma correcta. 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 necesita un informe de la utilidad Kaspersky Get System Info (en adelante denominada GSI). Para obtener información detallada sobre el uso de la utilidad, consulte la Base de conocimientos de Kaspersky.

Limitaciones y advertencias

Kaspersky Endpoint Security posee numerosas limitaciones que no son críticos para el funcionamiento de la aplicación.

Instalación de la aplicación

- Para obtener más información sobre el soporte técnico de los sistemas operativos Microsoft Windows 10, Microsoft Windows Server 2016 y Microsoft Windows Server 2019, consulte la Base de conocimientos del Servicio de soporte técnico.

- Para obtener más información sobre el soporte técnico de los sistemas operativos Microsoft Windows 11 y Microsoft Windows Server 2022, consulte la Base de conocimientos del Servicio de 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 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).

- Al eliminar componentes individuales de la aplicación (por ejemplo, mediante la tarea *Cambiar componentes de la aplicación*), es posible que sea necesario reiniciar el equipo.

- En las propiedades de la tarea *Cambiar componentes de la aplicación*, al cambiar el modo de instalación (**Modo separado**/**Modo combinado**), la sincronización del conjunto de componentes entre modos no es compatible. La aplicación sincroniza el conjunto de componentes entre modos una vez que vuelve a abrir las propiedades de la tarea.

- La instalación de la aplicación puede terminar con el siguiente error: *An application whose name is missing or unreadable is installed on your computer* (Una aplicación cuyo nombre falta o no se puede leer está instalada en su equipo). Esto significa que las aplicaciones no compatibles o fragmentos de ellas permanecen en su equipo. Para eliminar artefactos de aplicaciones no compatibles, envíe una solicitud con una descripción detallada de la situación al Servicio de soporte técnico de Kaspersky a través de Kaspersky CompanyAccount.

- Si canceló 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 superior. Microsoft .NET Framework 4.6.1 tiene vulnerabilidades. Si usa Microsoft .NET Framework 4.6.1, debe instalar las actualizaciones de seguridad. Para obtener más información 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 no afectar el rendimiento del sistema.

- Cuando se instala Kaspersky Endpoint Security para Windows en un servidor con las aplicaciones Kaspersky Security for Windows Server (KSWS) y Windows Defender instaladas, debe reiniciar el sistema. Es necesario reiniciar el sistema aunque haya habilitado la instalación de la aplicación sin reiniciar el sistema. Windows Defender para Windows Server está incluido en la lista de software que no es compatible con Kaspersky Endpoint Security para Windows. Antes de instalar la aplicación, el instalador elimina Windows Defender para Windows Server. La eliminación del software incompatible exige el reinicio del sistema.

- Antes de instalar Kaspersky Endpoint Security para Windows (KES) en un servidor con Kaspersky Security for Windows Server (KSWS) instalado, debe desactivar la Protección con contraseña de KSWS. Después de migrar de KSWS a KES, habilite 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 el software Veeam Backup & Replication implementado, es posible que necesite reiniciar su equipo y volver a ejecutar la instalación.

- La migración de Kaspersky Small Office Security (KSOS) a Kaspersky Endpoint Security (KES) con protección con contraseña habilitada está disponible a partir de la compilación 21.16 de KSOS.*.*. Para migrar versiones anteriores de KSOS, debe deshabilitar la protección con contraseña o eliminar KSOS manualmente. La migración de KSOS a KES sin protección con contraseña se realiza correctamente.

- No puede instalar Kaspersky Endpoint Security en una unidad extraíble de arranque. Durante la instalación, Kaspersky Endpoint Security muestra un mensaje de error: *Seleccionó una carpeta o una unidad no válida. Debe instalar la aplicación en un disco duro local*. Si logra instalar la aplicación en una unidad extraíble utilizando herramientas de terceros, esto puede hacer que el sistema operativo se bloquee (BSOD) durante el proceso de arranque. Esto significa que Kaspersky Endpoint Security no es compatible con Windows To Go ni con soluciones similares. Para analizar un equipo desde una unidad extraíble, puede usar la aplicación Kaspersky Rescue Disk.

- Debe tener consideraciones especiales al instalar Kaspersky Endpoint Security con componentes de red en un servidor de terminal con sesiones RDP de varios usuarios. El sistema operativo hace que todas las sesiones de usuario finalicen cuando finaliza la sesión del Administrador. Para conectarse al servidor de terminal, debe reiniciar el servidor o iniciar sesión en el sistema de forma local. Ese comportamiento se debe a peculiaridades de funcionamiento del 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 directivas 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 Web Console, la lista de componentes se muestra de manera incorrecta en las propiedades del paquete de instalación de Kaspersky Endpoint Security 12.11 para Windows. Un componente independiente, Anticifrador, no está disponible en esta versión de la aplicación. La funcionalidad 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 funcionalidad es un componente independiente. Al mismo tiempo, en la Consola de administración (MMC), la lista de componentes se muestra correctamente.

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 volver a una versión anterior del complemento, elimine el complemento actual e instale una versión anterior del complemento.

- Al actualizar Kaspersky Endpoint Security 11.0.0 o 11.0.1 para Windows, la configuración del programa de tareas local para las tareas *Actualización de 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 superior. Microsoft .NET Framework 4.6.1 tiene vulnerabilidades. Si usa Microsoft .NET Framework 4.6.1, debe instalar las actualizaciones de seguridad. Para obtener más información sobre las actualizaciones de seguridad de Microsoft .NET Framework, consulte el sitio web de soporte técnico de Microsoft.

- Al momento de actualizar Kaspersky Endpoint Security, la aplicación deshabilita el uso de KSN hasta que se acepte 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 usa Kaspersky Managed Detection and Response, recibirá eventos sobre violaciones a la operación de la solución. El uso de KSN es necesario para la operación de Kaspersky Managed Detection and Response. Kaspersky Endpoint Security habilita el uso de KSN después de aplicar la directiva por la que el administrador acepta los términos de uso de KSN. Una vez que se haya aceptado la Declaración de Kaspersky Security Network, Kaspersky Endpoint Security reanuda su operación.

- Después de actualizar Kaspersky Endpoint Security a la versión 11.10.0 o posterior sin reiniciar, el equipo tendrá dos aplicaciones de Kaspersky Endpoint Security instaladas. No elimine manualmente la versión anterior de la aplicación. La versión anterior se eliminará automáticamente cuando se reinicie el equipo.

- Después de actualizar Kaspersky Endpoint Security en un equipo con Microsoft Windows 11, es posible que el menú contextual del archivo muestre elementos tanto para las versiones anteriores como nuevas de la aplicación. Reinicie el 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 contra amenazas web, Protección contra amenazas de correo, Protección contra amenazas de 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 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 completó 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 con Kaspersky Security Center Cloud Console, no se permite actualizar la aplicación de manera local. Al actualizar la aplicación de manera local, no es posible aceptar el Acuerdo de procesamiento de datos para Kaspersky Security Center Cloud Console.

Compatibilidad con la arquitectura Arm

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

- El 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 es compatible con equipos basados en Arm.

- En equipos que ejecutan Windows 11 para Arm64, EDR Agent no es compatible con Bitdefender Endpoint Security Tools.

- La funcionalidad de protección de la señal de audio y la funcionalidad de protección del acceso a la cámara web no son compatibles con los equipos basados en Arm.

- En equipos basados en Arm, la extensión de Protección contra amenazas de 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 objetos destinados a la arquitectura Arm a Kaspersky Sandbox.

- El control de impresión no es compatible con equipos basados en la arquitectura Arm.

- La integración con Kaspersky Endpoint Detection and Response Expert (cloud) no es compatible con equipos basados en la arquitectura Arm.

- En equipos basados en Arm, la tarea *Análisis de IOC* solo admite archivos de correo electrónico de los siguientes clientes de correo: Versiones de 32 y 64 bits de Outlook 2016 y Outlook 2021, 2024 y 365 para Arm64.

Compatibilidad con plataformas de servidor

- En servidores con *deduplicación de datos* habilitada, debe agregar el archivo fsdmhost.exe a la lista de aplicaciones de confianza. De esta forma, se optimiza el rendimiento de la aplicación y evita una carga excesiva en la CPU.

- El sistema de archivos ReFS se admite con limitaciones:

  - Kaspersky Endpoint Security puede procesar incorrectamente los eventos de desinfección de amenazas. Por ejemplo, si la aplicación eliminó un archivo malicioso, el informe puede tener una entrada 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 contra archivos peligrosos puede omitir algunas amenazas. Al mismo tiempo, Análisis de malware funciona correctamente.

  - Una vez que se inicia la tarea *Análisis de malware*, las exclusiones agregadas con iChecker se restablecen cuando se reinicia el servidor.

  - No se admite la tecnología iSwift. Kaspersky Endpoint Security no considera las exclusiones de análisis agregadas mediante el uso de la tecnología iSwift.

  - Kaspersky Endpoint Security no detecta los archivos eicar.com y susp-eicar.com si el archivo meicar.exe existía en el equipo antes de la instalación de 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 pueden utilizarse en plataformas de servidor. Al mismo tiempo, Kaspersky Endpoint Security puede procesar incorrectamente los eventos de cifrado de datos.

- En sistemas operativos de servidor, no se muestra ninguna advertencia sobre la necesidad de una desinfección avanzada.

- Microsoft Windows Server 2008 ya no se considera compatible. La aplicación no está diseñada para instalarse en una computadora con el sistema operativo Microsoft Windows Server 2008.

- Kaspersky Endpoint Security instalado en un servidor con Microsoft Data Protection Manager (DPM) puede causar el mal funcionamiento de DPM. Esto está relacionado con las limitaciones en el funcionamiento de DPM. Para eliminar el mal funcionamiento, debe agregar las unidades del servidor local a las exclusiones para el componente Protección contra archivos peligrosos y las tareas de *Análisis de malware*.

- 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 solicitudes, 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 habilitado el modo de compatibilidad con el Estándar federal de procesamiento de información (FIPS), conecte una unidad extraíble para guardar la clave de cifrado antes de comenzar a cifrar la unidad.

Compatibilidad con plataformas virtuales

- No se admite Cifrado de disco completo (FDE) en máquinas virtuales Hyper-V.
- No se admite Cifrado de disco completo (FDE) en plataformas virtuales Citrix.
- Se admite Windows 10 Enterprise multisesión con ciertas limitaciones:
  - Kaspersky Endpoint Security desinfecta las amenazas activas sin avisarle 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.
  - El cifrado de disco completo (FDE) no es compatible.
  - La administración de BitLocker no es compatible.
  - El uso de Kaspersky Endpoint Security con unidades extraíbles no es compatible. La infraestructura de Microsoft Azure define las unidades extraíbles como unidades de red.
- No se admite la instalación y el uso de 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** habilitada. Esta opción se puede habilitar en el Asistente de instalación o con el parámetro de línea de comandos `/pCITRIXCOMPATIBILITY=1`. En caso de instalación remota, el archivo KUD debe editarse agregando el siguiente parámetro: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Antes de iniciar la clonación, debe deshabilitar Autoprotección para clonar máquinas virtuales que usan vDisk.
- Al preparar una máquina de plantilla para la imagen principal de Citrix XenDesktop con Kaspersky Endpoint Security para Windows preinstalado y el Agente de red de Kaspersky Security Center, agregue 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 se realice correctamente 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, es posible que no se logre eliminar de forma segura un disco extraíble en una máquina virtual. Intente desconectar de forma segura el dispositivo una vez más.

- Es posible que la instalación de Kaspersky Endpoint Security en máquinas virtuales con el agente de VDA Citrix resulte en un error de compatibilidad. Esto ocurre porque Citrix Provisioning Services limitó la compatibilidad con soluciones antivirus. Para consultar las mejores prácticas del uso de soluciones antivirus con Citrix Provisioning Services, vaya al 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 tales dispositivos, el sistema operativo detecta la unidad extraíble conectada como una unidad de red. En esos casos, puede utilizar la tarea *Análisis personalizado*. El comportamiento de la aplicación en el modo estándar y en el modo de Light Agent es el mismo.

- Si Kaspersky Endpoint Security está instalado en una máquina virtual en una infraestructura que utiliza la tecnología Citrix App Layering, los archivos detectados por la aplicación como infectados con el estado *El objeto se eliminará al reiniciar* no se eliminarán automáticamente cuando la máquina virtual se reinicie

  Para eliminar dichos archivos, debe montar el archivo VHDX que contiene la capa de usuario (User Layer) en el equipo del administrador de Citrix App Layering y ejecutar un análisis de malware en el disco montado.

Compatibilidad con Kaspersky Security Center

- En la versión 14.1 y versiones anteriores de Kaspersky Security Center Web Console, los nombres de las áreas funcionales de los componentes Inspección de registros y Monitor de integridad de archivos no se muestran correctamente en la sección de configuración de permisos de acceso de los usuarios de las propiedades del Servidor de administración.

- Después de reparar la aplicación, se deshabilita la protección de la conexión del equipo con el Servidor de administración. Después de reparar la aplicación, ejecute nuevamente la tarea *Protección de la conexión del Servidor de administración*.

- En la Consola de administración de Kaspersky Security Center, en la ventana **Seleccionar un usuario o un grupo de usuarios** solo se muestran los primeros 50 000 usuarios de la lista de usuarios de Kaspersky Security Center. Consulta la Ayuda de Kaspersky Security Center para obtener más detalles.

- Al buscar dispositivos administrados en la Consola de administración de Kaspersky Security Center, la pestaña **Componentes de las aplicaciones** puede mostrar simultáneamente distintas 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 podrían estar duplicados.

  Para buscar por componente, simplemente debe seleccionar una de las variantes que se muestran. Para obtener más información sobre la detección de dispositivos, consulte la Ayuda de Kaspersky Security Center.

Administración de licencias

- Si aparece el mensaje *Error al recibir los datos*, verifique que el equipo en el que está realizando la activación tenga acceso a la red o defina la configuración de activación a través del 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 de clave 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 a que, durante el proceso de instalación, la aplicación activa primero la licencia de prueba integrada. Requiere acceso a Internet.

- Durante el período de prueba, 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 a 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, debe activar manualmente la aplicación.

- Si está usando la versión 11 de Kaspersky Security Center y la versión 14.1 de Kaspersky Endpoint Security, es posible que los informes de rendimiento de los componentes no funcionen de forma correcta. Si instaló componentes de Kaspersky Endpoint Security que no se incluyen en la licencia que posee, es posible que un Agente de red envíe errores sobre el estado de los componentes al Registro de eventos de Windows. Para evitar errores, elimine los componentes que no están incluidos en la licencia que posee.

Protección contra amenazas de correo

- Al analizar el correo con la extensión Protección contra amenazas de correo para Microsoft Outlook, se recomienda utilizar el modo caché de Exchange (la opción Usar modo caché de Exchange).

- Kaspersky Endpoint Security no es compatible con la versión de 64 bits de cliente de correo Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de Microsoft Outlook (archivos PST y OST) si está instalada una versión de Microsoft Outlook de 64 bits en el equipo, incluso si el correo está incluido en el alcance del análisis.

- Kaspersky Endpoint Security no es compatible con el nuevo cliente de correo de Microsoft 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 paquetes de red o una regla de red de aplicaciones 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 controlar la actividad de la red. Por lo tanto, la aplicación convierte los nombres DNS en direcciones IP. Se recomienda usar nombres DNS en reglas solo para equipos de red LAN o servicios internos.

- Para especificar una regla para todas las direcciones IPv6, agregue el intervalo 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 aplicaciones de bloqueo 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 configuró un adaptador de red o período de vida (TTL) de paquetes para una regla de paquetes permitidos, la prioridad de esta regla es menor que la de una regla de aplicación de bloqueo. En otras palabras, si la actividad de red está bloqueada para una aplicación (por ejemplo, la aplicación está en el grupo de confianza *Restricción máxima*), no puede permitir la actividad de red de la aplicación mediante el uso de una regla del paquete con esta configuración. En todos los demás casos, la prioridad de una regla de paquete es mayor que la de una regla de red de aplicaciones.

- 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 (TTL) del paquete. Si este conjunto de parámetros generales es idéntico para varias reglas, la aplicación asigna el mismo nombre a dichas reglas o agrega una etiqueta de parámetro al nombre. De esta forma, Kaspersky Endpoint Security importa todas las reglas de paquetes, pero el nombre de las reglas que tiene una configuración general idéntica puede modificarse.

- Si habilitó la notificación de eventos de aplicación en una regla de 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 de Fiable, no tendrá restricciones de red. A continuación, habilitó la notificación de eventos para esta aplicación y la movió al grupo de confianza *No confiables*. El Firewall no aplicará las restricciones de red para esta aplicación. Se recomienda que primero mueva la aplicación al grupo de confianza correspondiente y luego habilite 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 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 del Firewall y de la Prevención de intrusiones tienen configuraciones comunes: derechos de aplicaciones y recursos protegidos. Si cambia estas configuraciones para el Firewall, Kaspersky Endpoint Security aplica automáticamente la nueva configuración a la Prevención de intrusiones. Si, por ejemplo, permitió 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 la aplicación** en el informe de 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 agregó la columna **Tipo de regla** al informe de Firewall. Cuando se activa una regla de paquete de red, el valor en la columna **Nombre de la aplicación** permanece vacío.

- Si prohibió toda la actividad de la red mediante el Firewall, el componente Protección contra amenazas de red puede detectar un ataque del tipo Análisis de puertos. Esto puede suceder porque la aplicación inicia la Protección contra amenazas de red antes que el Firewall para detectar actividad sospechosa en la red.

Prevención de ataques BadUSB

- Kaspersky Endpoint Security restablece el tiempo de espera del bloqueo del dispositivo USB cuando el equipo está bloqueado (por ejemplo, el tiempo de espera del bloqueo de la pantalla transcurrió). Es decir, si ingresa un código de autorización del dispositivo USB incorrecto varias 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 BadUSB.

- Kaspersky Endpoint Security restablece el tiempo de espera del bloqueo del dispositivo USB cuando la protección del equipo está suspendida. Es decir, si ingresa un código de autorización del dispositivo USB incorrecto varias 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 BadUSB.

Kaspersky Security Network

- Kaspersky Endpoint Security no es compatible con HTTPS cuando se conecta con KSN Proxy (la casilla **Usar HTTPS** seleccionada en la configuración de conexión de KSN Proxy) si la dirección del servidor incluye letras no pertenecientes al alfabeto latino (símbolos que no son ASCII).

- En Kaspersky Security Center, cuando se realiza el cambio de KSN Global a KSN Privada (KPSN), o viceversa, la opción de participar en Kaspersky Security Network se deshabilita en la directiva del producto específico. 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 consentimiento con la Declaración de Kaspersky Security Network. Para 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 consentimiento con la Declaración de Kaspersky Security Network. Si ya usó KSN global, primero debe deshabilitar el uso de KSN, luego volver a habilitarlo y confirmar su consentimiento con 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 archivos que pueden representar una amenaza a KSN para su análisis. 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 confiable (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 agregar más de 100 000 condiciones de inclusión y exclusión totales 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 funcione con Microsoft Windows 10.

- Solo los archivos de almacenamiento en formato ZIP son compatibles cuando se trabaja con reglas de Control de aplicaciones en Kaspersky Security Center Web Console. Los archivos de almacenamiento en otros formatos, como RAR o 7z, no son compatibles. No existe tal restricción si trabaja con reglas de Control de aplicaciones en la Consola de administración (MMC).

- Al trabajar con reglas de Control de aplicaciones en Kaspersky Security Center Web Console, el tamaño máximo admitido de un archivo cargado es de 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 bloqueo de aplicaciones, las reglas de bloqueo pueden aplicarse incorrectamente, lo que podría causar el bloqueo de aplicaciones que no están especificadas en las reglas.

- Si agregó nuevas *reglas de control de aplicaciones predefinidas* cuando actualizó 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 agregar 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 con Windows 11, el sistema operativo usa Metro Notepad ubicado en la carpeta `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. En versiones anteriores del sistema operativo, Bloc de notas está ubicado en las siguiente carpetas:

  - `C:\Windows\notepad.exe`

  - `C:\Windows\System32\notepad.exe`

  - `C:\Windows\SysWOW64\notepad.exe`

Al agregar Bloc de notas a una regla de Control de aplicaciones, puede especificar el nombre de la aplicación y el hash de archivo desde las propiedades de la aplicación en ejecución, por ejemplo.

- Al migrar la directiva de KSWS al perfil de directivas 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 los caracteres `_`. Por ejemplo, el nombre de la categoría de la aplicación `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` 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 del SISTEMA en el evento.

- El acceso a los dispositivos de impresora que se agregaron a la lista de confianza está 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, Unidades de CD/DVD. Para otros tipos de dispositivos, la aplicación no registra eventos de desconexión. La aplicación registra la operación de conectar un dispositivo a un equipo para todos los tipos de dispositivos.

- Si está agregando un dispositivo a la lista de confianza según una máscara de modelo y usa caracteres que están incluidos en el id. pero no en el nombre del modelo, estos dispositivos no se agregan. En una estación de trabajo, estos dispositivos se agregarán a la lista de confianza según una máscara de identificación.

- Cuando la aplicación se actualiza sin reiniciar el equipo, Control de dispositivos no aplica reglas de acceso a los dispositivos que se reconectan. Sin embargo, si el dispositivo estaba conectado antes de la actualización, Control de dispositivos aplica las reglas correctamente. Reinicie el equipo para que la aplicación funcione correctamente con los dispositivos que se reconectan.

- En computadoras que tengan instalada la versión 12.0 de Kaspersky Endpoint Security, el modo de acceso a la impresora **Permitir y no registrar** para el tipo de dispositivo **Impresoras de red** se denomina **Depende del bus de conexión**, si la directiva de la versión 12.1 de Kaspersky Endpoint Security se aplica en la computadora. En estos modos, la aplicación ejecuta las mismas acciones. En la versión 12.1 de Kaspersky Endpoint Security, el modo de acceso para las impresoras de red se denomina correctamente **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 la computadora. Hasta que se reinicia la computadora, Kaspersky Endpoint Security no aplica reglas de impresión y solo puede controlar el acceso a las impresoras. Si reiniciar la computadora afecta negativamente los flujos de trabajo en su organización, puede reiniciar solo el servicio spoolsv (Print Spooler). El control de impresión no es compatible con equipos basados en la arquitectura Arm.

- A partir de Kaspersky Endpoint Security 12.0 para Windows, la aplicación admite el protocolo WPA3 para dispositivos de tipo **Wi-Fi**. Si se aplica una directiva de Kaspersky Endpoint Security versión 12.2 en una computadora, el protocolo WPA2 se selecciona en computadoras con Kaspersky Endpoint Security versión 11.11.0 y anteriores. Para las versiones 12.0 a 12.1, se selecciona WPA2/WPA3; para las versiones 12.2 y posteriores, se selecciona WPA3.

- Los dispositivos Apple se clasifican como dispositivos portátiles (MTP) y dispositivos iTunes. El sistema operativo puede identificar de manera incorrecta la conexión del dispositivo Apple y no clasificar el dispositivo Apple como dispositivo portátil (MTP). Por lo tanto, el dispositivo Apple no estará disponible en el administrador de archivos, pero se podrá acceder a este en la aplicación iTunes. Como consecuencia, Kaspersky Endpoint Security controlará el acceso al dispositivo Apple solo en la aplicación iTunes. Para acceder a su dispositivo Apple como dispositivo portátil (MTP), debe ir al Administrador de dispositivos y eliminar el Controlador USB para dispositivos móviles de Apple de la lista de Controladores USB. Tras reiniciar el equipo, el sistema operativo identificará el dispositivo Apple como dispositivo portátil (MTP) y dispositivo 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 especificó 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 modifica el comportamiento del dispositivo.

- Control de dispositivos admite dispositivos Bluetooth solo a través de la pila Bluetooth de Microsoft Windows. Control de dispositivos puede funcionar de forma incorrecta con pilas Bluetooth de terceros.

- Si el dispositivo Bluetooth oculta o falsifica su Clase de dispositivo (COD), es posible que Control de dispositivos funcione de forma incorrecta.

- En equipos Windows 7 o Windows 8 con ciertos controladores del dongle Bluetooth de Realtek, quizás no sea posible permitir únicamente la conexión de dispositivos Bluetooth como dispositivos de entrada (clase de HID). Es decir, si prohíbe el acceso a dispositivos Bluetooth en la configuración de la aplicación y agrega dispositivos de entrada a las exclusiones, Control de dispositivos puede impedir el acceso a todos los dispositivos Bluetooth.

Control Web

- No se admiten los formatos OGV y WEBM.

- No se admite el protocolo RTMP.

- Control web solo es compatible con WSL1. La aplicación no controla el tráfico WSL2.

Control de anomalías adaptativo

- Se recomienda crear exclusiones automáticamente según el evento. Cuando agregue manualmente una exclusión, agregue el carácter `*` al comienzo de la ruta al especificar el objeto de destino.

- No se puede generar un informe de Reglas de control de anomalías adaptativo si la muestra incluye incluso un evento cuyo nombre contiene más de 260 caracteres.

- No se puede agregar exclusiones del Control de anomalías adaptativo que active el repositorio de reglas si las propiedades de un objeto o un proceso tienen un valor que contenga más de 256 caracteres (por ejemplo, una ruta a un objeto de destino). Puede agregar una exclusión manualmente en la configuración de directivas. También puede agregar una exclusión en el Informe en las reglas activadas del Control de anomalías adaptativo.

- Kaspersky Security Center 15.1 no puede generar un informe **Informe sobre el estado de las reglas del Control de anomalías adaptativo** para una regla específica.

Cifrado de unidad (FDE)

- El Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.
- El Cifrado de unidad BitLocker no es compatible con equipos con Windows Home.
- 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 un rendimiento óptimo del equipo después del cifrado, es necesario que el procesador sea compatible con el conjunto de instrucciones AES-NI (Nuevas Instrucciones de Cifrado Avanzado Intel). Si el procesador no es compatible con AES-NI, el rendimiento del equipo podría disminuir.
- Cuando hay procesos que intentan acceder a dispositivos cifrados antes de que la aplicación les haya otorgado acceso a dichos dispositivos, la aplicación muestra una advertencia donde se indica que dichos procesos deben terminarse. Si los procesos no se pueden terminar, vuelva a conectar los dispositivos cifrados.
- Los id. únicos 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 extraíbles 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. Desfragmente 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 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 habilitada en Microsoft Windows 8/8.1/10, el bloqueo de la hibernación evita que apague el sistema operativo.
- Los equipos con Windows 7 no permiten cambiar la contraseña durante la recuperación cuando el disco está cifrado con tecnología BitLocker. Una vez que se ingresa la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, es imposible establecer una contraseña nueva o un código PIN. Este problema se origina por las peculiaridades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.
- No se recomienda utilizar la herramienta xbootmgr.exe con los proveedores adicionales habilitados. Por ejemplo, Despachador, Red o Controladores.
- 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 al sistema de archivos NTFS.
- No pueden coexistir varios agentes de descarga en un equipo cifrado.

- Si intenta restaurar una imagen de un disco GPT de arranque en un estado no cifrado, es posible que el sistema operativo no funcione. Para evitarlo, siga estas recomendaciones:
  - Descifre completamente el disco antes de restaurar la imagen desde el respaldo.
  - 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 simultáneamente todas estas condiciones:
  - No hay conexión con el servidor de Kaspersky Security Center.
  - El usuario está intentando completar 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 cifrada.
- Es posible que el agente de autenticación no admita el descubrimiento de dispositivos USB cuando el modo xHCI para USB está habilitado 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 de Agente de autenticación basadas en cuentas de Microsoft se admite con las siguientes limitaciones:
  - No se admite la tecnología Inicio de sesión único.
  - 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 este equipo. Por ejemplo, supongamos que hay un usuario local `Ivanov` en el equipo `Ivanov`, y se creó una cuenta de agente de autenticación con el nombre `Ivanov/Ivanov` para este usuario. Si el nombre de equipo `Ivanov` se cambió por `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 utilizando la tarea de administración de cuentas locales 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 con el nombre antiguo (por ejemplo, `Ivanov/Ivanov`).

- Si a un usuario se le permite acceder a un equipo que se cifró con 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 haber restaurado el acceso al equipo cifrado. Es posible que no se guarde la contraseña que estableció el usuario al restaurar el acceso. En este caso, el usuario tendrá que completar el procedimiento para restaurar el acceso al equipo cifrado nuevamente 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 cambiado correctamente. Haga clic en Aceptar*, y el usuario reinicia el equipo. No se guarda la nueva contraseña. La contraseña anterior se debe utilizar para la autenticación posterior en el entorno de prearranque.

- El cifrado de disco no es compatible con la tecnología Intel Rapid Start.

- El cifrado de disco no es compatible 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 donde se 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 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 del Servicio 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 los 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 solo es compatible con el cifrado de archivos en dispositivos con sistemas de archivos NTFS y FAT32. Si un archivo cifrado se transfiere a una dispositivo con un sistema de archivos no compatible (como exFAT), el archivo no se cifrará en ese dispositivo y estará disponible para modificarse.

- Si un archivo cifrado se almacena en un equipo que tiene la funcionalidad de cifrado disponible y se 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 archivos con Kaspersky Endpoint Security para Windows.

- Después de cifrar un archivo, su tamaño aumenta 4 KB.

- Después de cifrar un archivo, se establece el atributo *Archivo* en las propiedades del archivo.

- Al copiar el archivo descifrado, por ejemplo, a un medio extraíble, es posible que el archivo permanezca 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 encuentra el hash, Kaspersky Endpoint Security deja el archivo cifrado. Para evitarlo, debe borrar la lista del proceso. El sistema operativo borra automáticamente la lista del proceso a medida que se completa. La lista también se puede vaciar manualmente. Para hacerlo, puede reiniciar el equipo, reiniciar el proceso que está utilizando para obtener acceso al archivo (por ejemplo, explorer.exe), o puede usar un administrador de archivos diferente que no haya usado para acceder al archivo cifrado.

- Si un archivo descomprimido desde un archivo cifrado tiene el mismo nombre que un archivo que ya existe en el equipo, el nuevo archivo descomprimido desde un archivo cifrado sobrescribirá al anterior. No se notifica al usuario sobre la operación de sobrescritura.

- Antes de descomprimir un archivo cifrado, asegúrese de tener suficiente espacio en disco libre para alojar los archivos descomprimidos. Si no tiene suficiente espacio en disco, la descompresión del archivo puede completarse, pero los archivos pueden estar dañados. 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 está instalado en el equipo.

  - No se realizó el cifrado de datos (FDE o FLE) en el equipo.

  El acceso no es posible 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 las reglas de restricción de acceso a los archivos cifrados de algunas aplicaciones. Esto se debe a que algunas operaciones de archivo se realizan mediante una aplicación de terceros. Por ejemplo, la copia de archivos la realiza el administrador de archivos y no la aplicación. De este modo, si se deniega el acceso a los archivos cifrados al cliente de correo de Outlook, Kaspersky Endpoint Security permitirá que el cliente de correo acceda al archivo cifrado, siempre y cuando el usuario haya copiado los archivos en el mensaje de correo electrónico a través del portapapeles o mediante la función de arrastrar y soltar. Se realizó la operación de copia a través de un administrador de archivos, para el cual no se especifican las reglas de restricción de acceso a los archivos cifrados, es decir, el acceso está permitido.

- Cuando las unidades extraíbles están cifradas con el modo portátil, el control de antigüedad de la contraseña no se puede deshabilitar.

- 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 al trabajar 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 sin conexión mediante Client-Side Caching (CSC). El cifrado de archivos sin conexión o la tecnología Branch Caching con SMB para servidores tampoco es compatible. Se recomienda prohibir la administración sin conexión de recursos compartidos en el nivel de directiva de grupo. Los archivos que están en modo sin conexión se pueden editar. Después de la sincronización, es posible que se pierdan los cambios realizados en un archivo sin conexión.

- No se admite la creación de un archivo 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 otro origen 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 entrada de contraseña para un archivo autoextraíble cifrado. Para resolver este problema, cierre la ventana de ingreso de contraseña, cambie a la distribución de teclado en su sistema operativo y vuelva a ingresar la contraseña para el archivo 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. A estos fines, 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 cifrados.

- No se admiten procesos Pico.

- 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 iniciarse. 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 a través de la red bajo reglas FLE mediante 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 donde 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 su nombre. Kaspersky Endpoint Security también bloquea la copia de archivos cifrados en carpetas de OneDrive si esos archivos no se agregan a la regla de descifrado.

- Cuando se instala el componente de cifrado de archivos, la administración de usuarios y grupos no funciona en modo WSL (Windows Subsystem for Linux).

- Cuando está instalado el componente Cifrado de archivos, no se admite POSIX (Portable Operating System Interface) para cambiar el nombre de archivos y eliminarlos.

- No se recomienda cifrar archivos temporales, ya que esto puede ocasionar pérdidas de datos. Por ejemplo, Microsoft Word crea archivos temporales al procesar un documento. Si los archivos temporales están cifrados, pero el archivo original no lo está, es posible que el usuario reciba el error *Acceso denegado* al intentar guardar el documento. Además, aunque Microsoft Word pueda guardar el archivo, es posible que no se pueda abrir el documento la próxima vez y se pierdan los datos. Para evitar la pérdida de datos, debe excluir la carpeta de archivos temporales de las reglas de cifrado.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- No puede analizar un objeto en cuarentena como resultado de la tarea *Poner archivo en cuarentena*.

- No se puede mover a cuarentena una Alternate Data Stream (ADS) de más de 4 MB.
  Kaspersky Endpoint Security omite los ADS de este tamaño sin notificar al usuario.

- Kaspersky Endpoint Security no ejecuta tareas de *Análisis de IOC* en unidades de red si la ruta de acceso a carpeta en las propiedades de la tarea comienza con una letra de unidad. Kaspersky Endpoint Security admite únicamente el formato de ruta UNC para tareas de *Análisis de IOC* en unidades de red. Por ejemplo, `\\server\shared_folder`.

- Para asegurarse de que la tarea *Análisis de IOC* que utiliza los términos Emailltem funcione correctamente, el complemento web de Kaspersky Endpoint Security debe actualizarse a la última versión.

- En equipos basados en Arm, la tarea *Análisis de IOC* solo admite archivos de correo electrónico 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 la aplicación termina en un error cuando la configuración de integración con Kaspersky Sandbox se encuentra habilitada en el archivo de configuración. Antes de exportar la configuración de la aplicación, deshabilite Kaspersky Sandbox. Luego, realice el procedimiento de exportación/importación. Una vez finalizada la importación del archivo de configuración, habilite 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 de EDR Agent. Para que EDR Agent 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 la tarea de *Análisis de IOC*, la aplicación envía un archivo a cuarentena solo para el término Fileltem. No se admite la cuarentena de un archivo para otros términos.

- Se requiere el complemento web de Kaspersky Endpoint Security para Windows 11.7.0 o posterior a fin de administrar los detalles de las alertas. Los detalles de las alertas son necesarios al trabajar con Endpoint Detection and Response (EDR Optimum y EDR Expert). Los detalles de la alerta solo están disponibles 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] termine 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 de [KES+KEA+agente integrado] no es compatible. Esa configuración interrumpe la interacción entre las aplicaciones y la solución de Detección y respuesta que se implementa en su organización. Además, el uso de Kaspersky Endpoint Agent y el agente integrado en la misma computadora puede provocar la duplicación de la telemetría y una mayor carga en la computadora y la red. Después de migrar a la configuración [KES+agente integrado], asegúrese de que Kaspersky Endpoint Agent se haya eliminado de la computadora. Si Kaspersky Endpoint Agent sigue funcionando después de la migración, desinstale la aplicación manualmente (por ejemplo, con la tarea *Desinstalar aplicación de forma remota*).

  El instalador le permite implementar Kaspersky Endpoint Agent en una computadora con Kaspersky Endpoint Security y el agente integrado instalados. Kaspersky Endpoint Agent y el agente integrado también se pueden instalar en una computadora 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 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 incorporado, 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 deshabilitar 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 incorporados de EDR (KATA), EDR Optimum y EDR Expert no son compatibles entre sí. Por lo tanto, se puede omitir la activación del agente incorporado de EDR con una licencia independiente del complemento Kaspersky Endpoint Detection and Response si activó Kaspersky Endpoint Security con una funcionalidad de EDR diferente. Por ejemplo, la activación del agente incorporado de EDR (KATA) con una licencia independiente se omite si activó Kaspersky Endpoint Security con la licencia de [KES+EDR Optimum].

- En la versión 12.1 de Kaspersky Endpoint Security, el agente incorporado de EDR (KATA) 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 agregó compatibilidad para estos metarchivos a la versión 12.2 de Kaspersky Endpoint Security.

- Al migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para la solución Kaspersky Anti Targeted Attack Platform (EDR), es posible que surjan errores al conectar el equipo a los servidores de Central Node. Esto se debe a que el asistente de migración de Web Console omite la siguiente configuración de directiva y no la migra:

  - Prohibición de modificación de 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 al equipo. Debe prohibir la modificación de la configuración y cerrar el "candado".

  - Contenedor cifrado.

    Si utiliza autenticación de dos factores para conectarse a los servidores de Central Node, debe volver a agregar el contenedor cifrado. El asistente de migración migra correctamente el certificado TLS del servidor.

  El Asistente de migración de la tarea y la directiva de la Consola de administración (MMC) migra toda la configuración de la solución Kaspersky Anti Targeted Attack Platform (EDR).

- No se muestra correctamente el estado de activación de la aplicación cuando 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. Tras la descarga del archivo BLOB, se muestra un estado incorrecto en el área de notificaciones de la barra de tareas de Windows: *La aplicación no está activada*. Sin embargo, se muestra el estado de activación correcto en la interfaz de la aplicación. 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 son pertinentes respecto de la visualización del estado de los componentes para interactuar con Kaspersky Anti Targeted Attack Platform:

  - En el caso del complemento de administración 12.0 y las versiones anteriores, en la aplicación se muestra el estado actual de **Sensor de Endpoint**. 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.

  - En el caso del complemento de administración 12.1 y versiones posteriores, en la aplicación se muestra el estado general de **Endpoint Detection and Response (KATA)**, que puede hacer referencia al estado de Endpoint Sensor o 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 12.6 y versiones posteriores, ni Kaspersky Security Center Web Console 14.2 ni las versiones anteriores 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)**, en la aplicación se 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 15.1 y versiones posteriores, en la aplicación se muestra el nombre correcto 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 a 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 la versión 14.0 de Kaspersky Security Center. 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 posterior. 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 objetos destinados a la arquitectura Arm a Kaspersky Sandbox.

- La integración con Kaspersky Endpoint Detection and Response Expert no es compatible con equipos basados en 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 transferirán de la directiva a los dispositivos administrados que ejecuten Kaspersky Endpoint Security versión 14.0 o anterior si se excede el límite admitido para las reglas de filtrado almacenadas. La aplicación mostrará una advertencia correspondiente.

Otras limitaciones

- Los sistemas operativos Windows, a partir de la versión 11 24H2, admiten la tecnología UDP Receive Segment Coalescing Offload (URO). La tecnología se habilita de manera predeterminada si se instalan una tarjeta de red y controladores compatibles en el equipo. Deshabilitar URO en el equipo de un usuario puede reducir de manera significativa el rendimiento de la aplicación.

- Kaspersky Endpoint Security es compatible con el subsistema WSL (Windows Subsystem for Linux) con las siguientes restricciones:

  - WSL 1 La aplicación supervisa el tráfico de la red y detecta amenazas a través de HTTP/HTTPS. Debido a que Kaspersky Endpoint Security usa su propio certificado para analizar conexiones HTTPS seguras, es posible que se interrumpa el funcionamiento de algunas aplicaciones de terceros.

  - WSL 2 La aplicación no es compatible con WSL 2.

- Si la aplicación devuelve errores o se cuelga durante la operación, se puede reiniciar en forma automática. Si la aplicación encuentra errores recurrentes que causan que la aplicación se cierre, la aplicación realiza las siguientes operaciones:

  1. Deshabilita las funciones de control y protección (la función de cifrado permanece activa).

  2. Notifica al usuario que las funciones se han deshabilitado.

  3. Intenta restaurar la aplicación a un estado funcional tras actualizar las bases de datos antivirus o aplicar actualizaciones a los módulos de la aplicación.

- Las direcciones web que se agregan a la lista de confianza pueden procesarse incorrectamente.

- En la consola de Kaspersky Security Center, no se puede guardar un archivo en el disco desde la carpeta **Avanzado** → **Repositorios** → **Amenazas activas**. Para guardar el archivo, se debe desinfectar el archivo infectado. Al desinfectarlo, la aplicación guarda una copia del archivo en Copia de seguridad. Ahora se puede guardar el archivo en el disco desde la carpeta **Avanzado** → **Repositorios** → **Copia de seguridad**.

- La opción de heredar la configuración de la transferencia de datos al Servidor de administración (**Configuración general** → **Informes y repositorios** → **Transferencia de datos al Servidor de administración**) se diferencia de la opción de heredar de otras configuraciones. Si permitió cambiar la configuración de la transmisión de datos en la directiva (el "candado" está abierto), esta configuración se restablecerá a los valores predeterminados en las propiedades del equipo local en la consola si no se definieron previamente. Si esta configuración se definió previamente, sus valores se restaurarán. Al eliminar una directiva, la configuración se hereda de la misma manera. En estos casos, otras configuraciones en las propiedades del equipo local se heredan de la directiva.

- 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 tráfico HTTP, la aplicación bloquea esta conexión para evitar la descarga de los archivos maliciosos de Internet.

- Kaspersky Endpoint Security evita la comunicación a través del protocolo QUIC. Los navegadores utilizan el protocolo de transporte estándar (TLS o SSL) independientemente de si la compatibilidad con QUIC está habilitada en el navegador o no.

- Pueden ocurrir errores de conexión TLS cuando el software de terceros funciona con la biblioteca Libcurl. Esto puede estar relacionado con el certificado de Kaspersky que usa Kaspersky Endpoint Security para analizar conexiones cifradas. Para seguir trabajando, puede deshabilitar la validación de certificados para software de terceros (no recomendado) o agregar un cuerpo de certificado de Kaspersky al almacén de certificados de cURL. Para obtener más información, consulte la Base de conocimientos 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. Posteriormente, la aplicación firmada digitalmente se incluirá en el grupo correcto.

- Durante un nuevo análisis de un objeto malicioso 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 de servidor o en estaciones de trabajo en las que no está instalado el componente Control de dispositivos.

- No es posible habilitar la visualización de todas las entradas de informes en Kaspersky Security Center Web Console. En Web Console, solamente se puede cambiar la cantidad de entradas que se muestran en los informes. De forma predeterminada, Kaspersky Security Center Web Console muestra 1000 entradas de informes. Se puede habilitar la visualización de todas las entradas de informes en la Consola de administración (MMC).

- No se puede configurar la visualización de más de 1000 entradas de informes en Kaspersky Security Center Console. Si configura un valor superior a 1000, Kaspersky Security Center Console mostrará solamente 1000 entradas de informes.

- 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 editar si la directiva principal prohíbe la modificación de esa configuración.

- Debe habilitar Auditar inicio de sesión en la configuración del sistema operativo para garantizar el correcto funcionamiento de las exclusiones para la protección de las carpetas compartidas contra el cifrado externo.

- Si la protección de carpetas compartidas está habilitada, 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 agregado 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 agregó a las exclusiones y que se iniciaron antes del inicio de Kaspersky Endpoint Security para Windows, finalice y vuelva a establezca 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 un origen 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 en Windows.

- No podemos garantizar que Control de audio funcionará hasta después del primer reinicio posterior a la instalación de la aplicación.

- En la Consola de administración (MMC), en la configuración de Prevención de Intrusiones de la ventana para configurar los permisos de las aplicaciones, el botón **Quitar** no está disponible. Puede eliminar una aplicación del 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 y los recursos protegidos de la aplicación 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 de Kaspersky Security Center Console.

- Cuando los archivos de seguimiento rotados están habilitados, no se crean seguimientos para el componente AMSI y el complemento de Outlook.

- El seguimiento del rendimiento no se puede recopilar manualmente en Windows Server 2008.

- No se admite Seguimiento del rendimiento para el tipo de seguimiento "Reiniciar".

- El registro de volcado no es compatible con los procesos Pico.

- Desactivar la opción "**Deshabilitar 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` a partir de 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 de carpetas personalizadas 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 hay Software Restriction Policies (SRP) activas en el equipo, puede que tenga problemas para cargar el sistema y vea una pantalla en negro. Para evitar un mal funcionamiento, es necesario permitir el uso de bibliotecas de aplicaciones en las propiedades de las SRP. En las propiedades de las SRP, agregue la regla con el nivel de seguridad **Sin restricciones** para el archivo khkum.dll (elemento del menú **Nueva regla Hash**). El archivo está ubicado en la carpeta `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.1\klhk\klhk_x64\`. Si seleccionó este método, además debe desmarcar la casilla **Descargar actualizaciones de módulos de la aplicación** en la configuración de la tarea *Actualizaciones* para Kaspersky Endpoint Security. Para más información sobre las directivas de restricción de software, consulte la documentación de Microsoft.

  También puede deshabilitar las SRP y utilizar el componente Control de aplicaciones de Kaspersky Endpoint Security para controlar el uso de las aplicaciones.

- Si el equipo pertenece a un dominio en un objeto de directiva de grupo (Group Policy Object, GPO) de Windows y el parámetro DriverLoadPolicy está configurado con un valor de 8 (Good only), reiniciar el equipo con Kaspersky Endpoint Security instalado causa un bloqueo (BSOD). Para evitar una falla, el parámetro Early Launch Antimalware (ELAM) en la directiva de grupo debe configurarse con un valor de 1 (Good and unknown). La configuración de ELAM se encuentra en la directiva bajo: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- No se admite la administración de la configuración del complemento de Outlook a través de la API REST.

- 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 de acuerdo con 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 la utilidad definió por última vez. 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 la protección con contraseña no permite cambiar el nombre de la cuenta del administrador (KLAdmin, de forma predeterminada). Para cambiar el nombre de la cuenta del administrador, debe deshabilitar la protección con contraseña, luego habilitar la protección con contraseña y especificar un nuevo nombre para la cuenta del 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 se instaló Kaspersky Endpoint Security en un servidor del DBMS SQL Server, la aplicación envía solicitudes a la instancia del servidor. Esto es necesario para analizar los trabajos de agente SQL Server y evitar que se ejecuten trabajos maliciosos. Kaspersky Endpoint Security utiliza la cuenta de usuario de SQL Server para analizar trabajos. La aplicación envía solicitudes al servidor cuando analiza la memoria del sistema y después de actualizar las bases de datos antivirus.

- La compatibilidad del software Kaspersky Endpoint Security y Secret Net Studio es limitada:

  - La aplicación Kaspersky Endpoint Security no es compatible con el componente antivirus del software Secret Net Studio.

    La aplicación no se puede instalar en un equipo en el que 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 Secret Net Studio.

    La aplicación no se puede instalar en un equipo en el que se implementa Secret Net Studio con el componente Protección de disco y cifrado de datos. Para que la interoperabilidad sea posible, debe eliminar el componente Protección de 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 operar 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 coexistir reglas con id. idénticos, por ejemplo, si editó manualmente los archivos XML de reglas exportados. Si los id. de las reglas son únicos, pero los nombres de las reglas son iguales, Kaspersky Endpoint Security agrega `(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 está abierta en un grupo secundario en Web Console. Web Console también muestra una advertencia: *Esta es una directiva heredada. Su configuración solo puede modificarse en el grupo de administración en el que se la creó*.

- Las notificaciones emergentes de más de 256 caracteres no se muestran en la Consola de administración (MMC).

- Los nombres de los componentes en la directiva y en el paquete de instalación pueden ser diferentes. Por ejemplo, Endpoint Detection and Response Expert (on-premises) puede llamarse 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 portátiles

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 para pasar el proceso de autenticación para acceder a los discos duros cifrados y cargar el sistema operativo una vez que se cifró el disco duro del sistema.

Agente de red

Un componente de Kaspersky Security Center que habilita 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 para todas las aplicaciones de Kaspersky que se ejecutan en Windows. Las versiones dedicadas de Agente de red sirven para aplicaciones que se ejecutan en otros sistemas operativos.

Alcance de la protección

Los objetos que la Protección básica contra amenazas analiza constantemente cuando está en ejecución. Los alcances de la protección de diferentes componentes tienen diferentes propiedades.

Alcance del análisis

Los objetos que analiza Kaspersky Endpoint Security cuando realiza una tarea de análisis.

Archivo de almacenamiento

Uno o varios archivos empaquetados en un solo archivo comprimido. Se necesita 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 usado por intrusos como "contenedor" para almacenar y propagar código malicioso. Por lo general, son archivos ejecutables con extensiones de archivo tales como .com, .exe y .dll. Existe un riesgo bastante alto de intrusión de código malicioso en estos archivos.

Archivo infectado

Archivo que contiene código malicioso (código de malware conocido que se detectó al analizar el archivo). Kaspersky no recomienda utilizar estos archivos, ya que podrían infectar el equipo.

Autenticación Kerberos

Mecanismo de autenticación mutua por parte del cliente y el servidor antes de establecer una conexión entre ellos, que permite comunicarse a través de redes inseguras. El mecanismo se basa en un vale, que el usuario obtiene de un centro de autenticación de confianza.

Base de datos de direcciones web fraudulentas

Lista de las direcciones de correo electrónico que los especialistas de Kaspersky han definido como relacionadas con phishing. La base de datos se actualiza periódicamente y forma parte del kit de distribución de las aplicaciones de Kaspersky.

Base de datos de direcciones web malintencionadas

Lista de direcciones web cuyo contenido se puede considerar peligroso. Los especialistas de Kaspersky crean la lista. Se actualiza periódicamente y se incluye en el kit de distribución de las aplicaciones de Kaspersky.

Bases de datos de antivirus

Las bases de datos que contienen información sobre las amenazas conocidas de seguridad al equipo por parte de Kaspersky como de la fecha de lanzamiento de la base de datos antivirus. Las firmas de la bases de datos antivirus ayudan a detectar código malicioso en los objetos analizados. Los especialistas de Kaspersky crean las bases de datos de antivirus y las actualizan a cada hora.

Certificado de licencia

Un documento que transfiere Kaspersky al usuario junto con el archivo de clave o código de activación. Incluye información sobre la licencia otorgada al usuario.

Clave activa

Clave que está utilizando la aplicación.

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, Microsoft Office 365. Los servicios en la nube se agrupan en categorías, por ejemplo, *Uso compartido de archivos*, *Mensajería*, *Correo electrónico*.

Desinfección

Método de procesamiento de objetos infectados cuyo resultado es la recuperación completa o parcial de los datos. No todos los objetos infectados se pueden desinfectar.

Emisor de certificado

El centro de certificación que emitió el certificado.

Falsa alarma

Una falsa alarma se produce cuando la aplicación de Kaspersky indica que un archivo desinfectado está infectado debido a que 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 del recurso web que se obtiene a través de una normalización. La *normalización* es un proceso por medio del cual la representación textual de la dirección de un recurso web cambia según reglas específicas (por ejemplo: exclusión del nombre de usuario, de la contraseña y del puerto de conexión de la representación textual de la dirección del recurso web; además, la dirección del recurso web se modifica de caracteres en mayúscula a caracteres en minúscula).

En el contexto de funcionamiento de los componentes de protección, el fin de la normalización de direcciones de recursos web es evitar el análisis de las direcciones de sitios web que, más de una vez, pueden diferir en la sintaxis pero ser físicamente equivalentes.

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 tienen funciones en común y el conjunto de aplicaciones de Kaspersky instaladas en ellos. Los dispositivos se agrupan de manera tal que se puedan administrar fácilmente como una unidad. En un grupo, se pueden incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada aplicación instalada en el grupo.

IOC

Indicador de compromiso. Un conjunto de datos acerca de una actividad o un objeto malicioso.

Light Agent

Componente Kaspersky Endpoint Security for Virtualization Light Agent. Se instala en cada máquina virtual que necesita protección.

Máscara

Representación del nombre de un archivo y de su extensión utilizando comodines.

Las máscaras de archivos puede contener cualquier carácter permitido en nombres de archivos, incluidos comodines:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto 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 de análisis.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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

Se desarrolló un microchip para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Suele haber un Módulo de plataforma segura instalado en la placa madre del equipo y este módulo interactúa con todos los demás componentes del sistema a través del bus de hardware.

Objeto OLE

Un archivo adjunto o un archivo integrado en otro archivo. Las aplicaciones de Kaspersky permiten analizar objetos OLE en busca de virus. Por ejemplo: si incrusta una tabla de Microsoft Office Excel® en un documento de Microsoft Office Word, la tabla se analiza como un objeto OLE.

OpenIOC

Estándar abierto de las descripciones del Indicador 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 se instala 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

En esta sección encontrará contenidos que complementan la información principal del documento.

Apéndice 1. Configuración de la aplicación

Puede utilizar una directiva, tareas o la interfaz de la aplicación para configurar Kaspersky Endpoint Security. La información detallada sobre componentes de la aplicación se proporciona en las secciones correspondientes.

Protección contra archivos peligrosos

El componente Protección contra archivos peligrosos le permite evitar la infección del sistema de archivos del equipo. De manera predeterminada, el componente Protección contra amenazas de archivo reside permanentemente en la memoria RAM del equipo y analiza en tiempo real todos los archivos abiertos, guardados y ejecutados. El componente analiza archivos en todas las unidades de la computadora, incluidas las unidades conectadas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

El componente analiza los archivos a los que acceden tanto el usuario como las aplicaciones. Cuando se detecta un archivo malintencionado, Kaspersky Endpoint Security bloquea la operación del archivo. El archivo entonces se elimina o se desinfecta, dependiendo de cómo se ha configurado el componente.

Si intenta acceder a un archivo cuyo contenido está almacenado en la nube de OneDrive, Kaspersky Endpoint Security descargará el contenido y lo analizará.

Parámetros del componente Protección contra amenazas de archivos

Parámetro	Descripción
Nivel de seguridad *(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)*	Para Protección contra archivos peligrosos, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*: • **Alto**. Si se selecciona este nivel de seguridad de archivos, el componente Protección contra amenazas de archivos realiza el control más estricto de todos los archivos abiertos, guardados e iniciados. El componente Protección contra amenazas de archivos analiza todos los tipos de archivo en todos los discos duros, unidades extraíbles y unidades de red del equipo. También analiza archivos de almacenamiento, paquetes de instalación y objetos OLE integrados. • **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección contra amenazas de archivos solo analiza los formatos de archivo especificados en todos los discos duros, unidades extraíbles y unidades de red del equipo, y en los objetos de OLE incorporados. El componente Protección contra amenazas de archivos no analiza paquetes de instalación ni archivos. • **Bajo**. La configuración de este nivel de seguridad de archivos garantiza la máxima velocidad de análisis. El componente Protección contra amenazas de archivos analiza solamente los archivos con las extensiones especificadas en todos los discos duros, unidades extraíbles y unidades de red del equipo. El componente Protección contra amenazas de archivos no analiza 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 esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones). **Archivos analizados según su formato**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, 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 según su extensión**. Si esta configuración está habilitada, la aplicación analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión.

Parámetro	Descripción
Alcance del análisis	Contiene objetos que son analizados por el componente Protección contra archivos peligrosos. Los objetos de análisis pueden ser discos duros, unidades extraíbles o de red, carpetas, archivos individuales o máscaras que engloben varios archivos. De manera predeterminada, el componente Protección contra amenazas de archivos analiza los archivos iniciados en discos duros, unidades extraíbles o unidades de red. El alcance de protección de estos objetos no puede modificarse ni eliminarse. Solo es posible excluir un objeto (por ejemplo, unidades extraíbles) 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 aprendizaje automático y análisis de firmas usa las bases de datos de Kaspersky Endpoint Security que contienen descripciones de las amenazas conocidas y las formas para neutralizarlas. La protección que usa este método proporciona el nivel de seguridad mínimo aceptable. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado.
Análisis heurístico *(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)*	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo. **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación bloquea este archivo. **Bloquear**. Si esta opción está seleccionada, la aplicación bloquea automáticamente todos los archivos infectados sin intentar desinfectarlos. 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 si se puede desinfectar en el futuro.
Analizar solo 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 compuestos.
Analizar archivos de almacenamiento	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos de Microsoft Office	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.
Analizar archivos de formato de correo electrónico	Analiza archivos de formato de correo electrónico. La aplicación analiza archivos MSG y EML. Los objetos OLE y los archivos MHT también se consideran archivos de formato de correo electrónico. Kaspersky Endpoint Security analiza los archivos en formato correo electrónico con un tamaño inferior a 1 MB independientemente de si la casilla está seleccionada o no.
No desempaquetar archivos compuestos de gran tamaño	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada o no.

Parámetro	Descripción
Descomprimir archivos compuestos en segundo plano	Si esta casilla de verificación está seleccionada, la aplicación proporciona acceso a los archivos compuestos que son más grandes que el valor especificado antes de que se analicen estos archivos. En este caso, Kaspersky Endpoint Security descomprimirá y analizará los archivos compuestos en segundo plano. La aplicación proporciona acceso a los archivos compuestos que son más pequeños que este valor solo después de descomprimir y analizar estos archivos. Si esta casilla de verificación no está seleccionada, la aplicación proporciona acceso a archivos compuestos solo después de descomprimir y analizar los archivos, independientemente de su 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 contra archivos peligrosos analiza un objeto en función de las operaciones realizadas sobre ese objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo. **Ante operaciones de acceso y modificación**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos siempre que haya un intento de abrirlos o modificarlos. **Ante operaciones de acceso**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos solo después de un intento de abrirlos. **Ante operaciones de ejecución**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos después de un intento de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de 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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Pausar Protección contra amenazas de archivo *(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)*	Esto suspende temporal y automáticamente la operación de Protección contra archivos peligrosos a la hora especificada o al trabajar con las aplicaciones especificadas.
Análisis de las operaciones sobre 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 contra amenazas de archivo. **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 se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado. **No analizar las operaciones sobre archivos ejecutadas en contenedores de Windows**. Si esta casilla está seleccionada, la aplicación analiza el contenedor solo al inicio. Si no se selecciona la casilla, la aplicación analiza el contenedor continuamente en tiempo real.

Protección contra amenazas web

El componente Protección contra amenazas web está diseñado para bloquear sitios web maliciosos y fraudulentos e impedir la descarga de archivos dañinos de Internet. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Kaspersky Endpoint Security analiza tráfico HTTP, HTTPS y FTP. La aplicación analiza tanto direcciones URL como direcciones IP.

Para usar la Protección contra amenazas web, debe completar la configuración inicial de la aplicación:

- Para que la aplicación pueda supervisar el tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitada de manera predeterminada).
- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación controla todos).
- Seleccione las aplicaciones cuyo tráfico desee que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya figuran en la lista de aplicaciones que recomienda Kaspersky. Si el navegador que utiliza no está en la lista, agréguelo.
- Recomendamos inyectar un script de interacción de página web en el tráfico web (la inyección de script está deshabilitada de forma predeterminada). Esta secuencia de comandos permite el registro de eventos de Protección contra amenazas web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

Cuando un usuario intente abrir un sitio web malicioso o fraudulento, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia.

Configuración del componente Protección contra 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 contra amenazas web, la aplicación puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*: • **Alto**. El nivel de seguridad con el cual el componente Protección contra amenazas web realiza el análisis máximo del tráfico web que recibe el equipo a través de los protocolos HTTP y FTP. El componente Protección contra amenazas web analiza en detalle todos los objetos de tráfico web mediante el uso de todas las bases de datos de la aplicación y realiza el análisis heurístico más avanzado posible. • **Recomendado**. Este es el nivel de seguridad que proporciona el equilibrio óptimo entre el rendimiento de la aplicación y la seguridad del tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de 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 asegura la máxima velocidad de análisis de tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de análisis superficial.
Acción al detectar una amenaza	**Bloquear**. Cuando 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**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web permite que el objeto se descargue al equipo, pero agrega información sobre el mismo a la lista de amenazas activas.
Comprobar si la dirección web está 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)*	Analizar los vínculos para determinar si están incluidos en la base de datos de direcciones web malintencionadas le permite rastrear sitios web que estén en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web malintencionadas, la que se incluye en el paquete de instalación de la aplicación y se actualiza durante las actualizaciones de las bases 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)*	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

Parámetro	Descripción
Comprobar si la dirección web está en la base de datos de direcciones web fraudulentas *(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 los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases de datos de Kaspersky Endpoint Security.
No analizar el tráfico web de las direcciones web de confianza	Si se selecciona esta opción, el componente Protección contra amenazas web no analiza el contenido de las páginas o los sitios web cuyas direcciones están incluidas en la lista de direcciones web de confianza. Puede agregar a esta lista 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 contra amenazas web, Protección contra amenazas de correo y Control web están haciendo su trabajo.

Protección contra amenazas de correo

El componente Protección contra amenazas de correo analiza los archivos adjuntos a los mensajes de correo entrantes y salientes para detectar virus y otras amenazas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

La Protección contra amenazas de 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 agregar el certificado de Kaspersky al almacén de certificados y seleccionar su almacén de certificados propios.

La Protección contra amenazas de correo no es compatible con otros protocolos y clientes de correo.

Es posible que la Protección contra amenazas de correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, la Protección contra amenazas de correo incluye una extensión para Microsoft Office Outlook. La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2010, 2013, 2016, 2019, 2021, 2024 y 365. En equipos basados en Arm, la extensión de Protección contra amenazas de correo es compatible con las versiones de 32 y 64 bits de Outlook 2016, Outlook 2021, Outlook 2024 y Outlook 365 para Arm64.

Si utiliza un navegador para acceder a su cliente de correo electrónico, el componente Protección contra amenazas de correo no analizará sus mensajes.

Cuando se detecta un archivo malicioso en un archivo adjunto, Kaspersky Endpoint Security agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[El mensaje ha sido procesado] <asunto del mensaje>*.

Configuración del componente Protección contra amenazas de 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 contra amenazas de correo, la aplicación puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*: • **Alto**. Cuando este nivel de seguridad del correo electrónico se selecciona, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico más detalladamente. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico profundo. El nivel de seguridad de correo Alto se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo gratuito desde una red doméstica sin protección centralizada del correo. • **Recomendado**. Este es el nivel de seguridad del correo electrónico que proporciona el equilibrio óptimo entre el rendimiento de la aplicación y la seguridad del correo electrónico. El componente Protección contra amenazas de 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 del tráfico de correo. • **Bajo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo solo analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza los archivos adjuntos a los mensajes de correo electrónico. En este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico con una velocidad máxima y utiliza lo mínimo de los recursos del sistema operativo. Se recomienda utilizar el nivel de seguridad de correo Bajo en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una red LAN empresarial con protección de correo electrónico centralizada.
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*. **Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. Si el objeto no puede desinfectarse, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error. **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.
Alcance de la protección *(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)*	El *Alcance de la 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 el envío de archivos infectados. También puede activar el análisis de mensajes salientes si desea evitar el envío de archivos en formatos particulares, como archivos de audio y video, por ejemplo.
Analizar el tráfico POP3, SMTP, NNTP e IMAP	El componente Protección contra amenazas de correo analiza el tráfico que utiliza los protocolos POP3, SMTP, NNTP e IMAP.
Conectar extensión 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 planea analizar el correo con la extensión para Microsoft Outlook, recomendamos que 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.
Análisis heurístico *(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)*	Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

Parámetro	Descripción
Analizar archivos de almacenamiento adjuntos	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento). Si, durante el análisis, la aplicación detecta una contraseña de un archivo de almacenamiento 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 guarda. Durante el análisis, el archivo de almacenamiento se descomprime. Si la aplicación genera un error durante el proceso de descompresión, 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	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.
No analizar archivos de almacenamiento de más de N MB	Si esta casilla está seleccionada, el componente Protección contra amenazas de correo excluye del análisis los archivos adjuntos en los mensajes de correo electrónico si el tamaño excede el valor especificado. Si se desactiva la casilla, el componente Protección contra amenazas de correo analiza los archivos adjuntos de correo de cualquier tamaño.
Limitar el tiempo para analizar archivos a N segundos	Si la casilla está seleccionada, el tiempo asignado al análisis de archivos adjuntos en los mensajes de correo se limita al período especificado.
Filtro de datos adjuntos	El filtro de documentos adjuntos no se aplica a mensajes de correo electrónico salientes. **Deshabilitar el filtrado**. Si selecciona esta opción, el componente Protección contra amenazas de correo no filtrará los archivos adjuntos de los mensajes de correo electrónico. **Cambiar el nombre de los archivos adjuntos de los tipos seleccionados**. Si selecciona esta opción, Protección contra amenazas de correo reemplazará el último carácter de extensión encontrado en los archivos adjuntos de los tipos especificados con el carácter de guion bajo (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo. **Eliminar archivos adjuntos de los tipos seleccionados**. Si selecciona esta opción, el componente Protección contra amenazas de correo eliminará de los mensajes de correo electrónico los tipos de archivos adjuntos que especifique. Puede especificar los tipos de archivos adjuntos para eliminar de los mensajes de correo electrónico en la lista de máscaras de archivos.

Protección contra amenazas de red

El componente *Protección contra amenazas de red* (también llamado 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 ataque de red contra el equipo del usuario, bloquea la conexión al equipo agresor. Las distintas clases de ataques de red sobre las que se tiene registro, así como las maneras de combatirlos, se describen en las bases de datos de la aplicación. La lista de ataques de red que detecta el componente Protección contra amenazas de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación.

Parámetro	Descripción
Tratar los análisis de puertos e inundaciones de red como ataques	Ataques de *saturación de red*, con los cuales se busca afectar los recursos de red (por ejemplo, los servidores web) de una organización. En esta clase de ataque, se realiza una gran cantidad de solicitudes con el fin de sobrecargar el ancho de banda disponible para los recursos de red. La saturación impide el acceso a los recursos de la organización. Ataques de *análisis de puertos*, en los cuales se realiza un sondeo de los puertos UDP, los puertos TCP y los servicios de red del equipo. El escaneo de puertos permite determinar qué tan vulnerable es un equipo; suele estar seguido por algún tipo de ataque más peligroso. Esto también revela el sistema operativo del equipo, lo que permite elegir el ataque de red más apropiado. Si activa esta casilla, Kaspersky Endpoint Security buscará indicios de estas clases de ataques en el tráfico de red. 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 tomar acciones de respuesta ante amenazas de forma oportuna. Si alguna de sus aplicaciones autorizadas realiza operaciones que son típicas de estas clases de ataques, puede deshabilitar las funciones de detección pertinentes. Con ello evitará las falsas alarmas.
Bloquear dispositivos atacantes durante N min	Si se habilita esta opción, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección. 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 acceder a la lista de equipos bloqueados a través de la ventana del Monitor de red. La lista de equipos bloqueados se vacía cada vez que Kaspersky Endpoint Security se reinicia o cuando se modifica la configuración de Protección contra amenazas de red.
Exclusiones	La lista contiene las direcciones IP de las que la Protección contra amenazas de red no bloquea los ataques de 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 suplantación de MAC	Ataques de *suplantación de MAC*, que consisten en cambiar la dirección MAC de un dispositivo (tarjeta) de red. Al realizar este cambio, un atacante puede redirigir los datos destinados a un dispositivo a otro dispositivo diferente y, de ese modo, obtener acceso a la información. Kaspersky Endpoint Security le permite saber si se detecta uno de estos ataques y bloquearlo.

Firewall

El componente Firewall impide que se establezcan conexiones no autorizadas cuando el equipo está conectado a una red local o a Internet. Firewall también controla la actividad de red de las aplicaciones instaladas en el equipo. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el servicio de nube Kaspersky Security Network y las *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. El firewall crea automáticamente las reglas de red necesarias para que la aplicación y el Agente de red funcionen. Como resultado, el firewall abre varios puertos en la computadora. Los puertos que se abren dependen de la función de la computadora (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en la computadora, consulte la Ayuda de Kaspersky Security Center.

Reglas de red

Las reglas de red se pueden configurar en distintos niveles:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security incluye una serie de reglas predefinidas, con permisos configurados según las recomendaciones de los expertos de Kaspersky.

- *Reglas de red de aplicaciones*. Las reglas de red de la aplicación imponen restricciones en la actividad de la red de una aplicación específica. Tienen en cuenta no solo las características del paquete de red, sino también la aplicación específica a la cual se dirige este paquete de red o que los emitió.

Controlar el acceso de las aplicaciones a los datos personales, a los procesos y a los recursos del sistema operativo es tarea del componente Prevención de intrusiones en el host, que utiliza los *derechos* asignados a las aplicaciones para tal fin.

Cuando una aplicación se ejecuta por primera vez, Firewall realiza las siguientes acciones:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.

2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Firewall, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima* o *No confiables*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea la actividad de red de la aplicación si su grupo de confianza así lo requiere. Por ejemplo, las aplicaciones del grupo *Restricción máxima* no tienen permitido usar ninguna conexión de red.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Si la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están definidas para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más arriba en la lista se encuentra una regla, mayor es su prioridad. Cuando un mismo tipo de actividad de red se describe en varias reglas, Firewall se basa en la regla de mayor prioridad para regular la actividad.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si las reglas de paquetes de red y las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se procesa según las reglas de paquetes de red.

Las reglas de red para las aplicaciones funcionan de una manera particular. La regla de red para las aplicaciones incluye reglas de acceso según el estado de la red: *Red pública*, *Red local*, *Red de confianza*. Las aplicaciones del grupo de confianza *Restricción máxima*, por ejemplo, no tienen permitido realizar ninguna clase de actividad de red, independientemente de que el equipo esté conectado a una red pública, local o de confianza. Cuando se crea una regla de red para una aplicación individual (aplicación principal), dicha regla afecta también a los procesos secundarios de otras aplicaciones. Cuando no existe una regla de red para una aplicación, los procesos secundarios quedan sujetos a la regla de acceso de red correspondiente al grupo de confianza de la aplicación.

Supóngase, por ejemplo, que se prohíbe el tráfico en redes de cualquier estado para todas las aplicaciones, a excepción del navegador X. El navegador X (aplicación principal) se utiliza luego para iniciar la instalación de un navegador Y (proceso secundario). En este caso, el instalador del navegador Y tendrá acceso a la red y podrá descargar los archivos que hagan falta. Tras la instalación, sin embargo, Firewall no permitirá que el navegador Y establezca conexiones de red. Para que el instalador del navegador Y no pueda acceder a la red valiéndose de su condición de proceso secundario, será necesario agregar una regla de red que cubra ese programa específico.

Tipos de las conexiones de red

Firewall puede controlar la actividad de red basándose en el tipo de la conexión. Kaspersky Endpoint Security obtiene el tipo de la conexión del sistema operativo. El tipo informado por el sistema operativo es el que el usuario configura cuando la conexión se establece por primera vez. Si lo desea, puede cambiar el tipo de la conexión de red en la configuración de Kaspersky Endpoint Security. El Firewall controlará la actividad de red según el tipo de red especificado en la configuración de Kaspersky Endpoint Security, y no en el sistema operativo.

Están disponibles los siguientes tipos de conexión de red:

- **Red pública**. Una red que no está protegida por una aplicación antivirus, un filtro o un firewall (un ejemplo podría ser la red Wi-Fi de una cafetería). Cuando el usuario opera un equipo conectado a una red de ese tipo, el Firewall bloquea el acceso a archivos e impresoras de este equipo. Los usuarios externos tampoco tienen acceso a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella.

  De forma predeterminada, Firewall asigna el tipo *Red pública* a Internet. No puede cambiar el tipo de Internet.

- **Red local**. Una red en la que los usuarios tienen restricciones para acceder a los archivos y las impresoras del equipo (un ejemplo podría ser una LAN corporativa u hogareña).

- **Red de confianza**. Una red segura, en la que el equipo no está expuesto a ningún ataque o a intentos no autorizados de acceder a los datos que contiene. Firewall permite cualquier actividad de red dentro de las redes con este estado.

Configuración del componente Firewall

Parámetro	Descripción
Reglas de paquetes	Tabla con una lista de reglas para paquetes de red. Las reglas de paquetes de red sirven para imponer restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. La tabla enumera reglas de paquetes de red preconfiguradas recomendadas por Kaspersky para la protección óptima del tráfico de red de equipos que se ejecutan en sistemas operativos Microsoft Windows. Firewall define la prioridad de ejecución 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 a abajo. Cuando se detecta una conexión de red, el componente 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 conexiones de red detectadas por el Firewall en el equipo. El estado asignado por defecto a la Internet es *Red pública*. No puede cambiar el estado de Internet.
Reglas para aplicaciones	**Aplicación**. Tabla de aplicaciones controladas por el componente Firewall. Cada aplicación está asignada a un grupo de confianza. Los grupos de confianza determinan los derechos en los que Kaspersky Endpoint Security se basa para controlar la actividad de red de las aplicaciones. Puede elegir una aplicación de una lista única en la que se recogen todas las aplicaciones instaladas en los equipos sujetos a una directiva y agregarla a un grupo de confianza. **Reglas de red**. Tabla con las reglas de red que se han definido para las aplicaciones de un grupo de confianza. Las reglas le indican a Firewall cómo debe regular la actividad de red de las aplicaciones. La tabla contiene reglas de red predefinidas y recomendadas por los especialistas de Kaspersky. Dichas reglas se han incluido porque permiten proteger el tráfico de red de los equipos con Windows del mejor modo posible. Las reglas de red predefinidas no se pueden eliminar.

Prevención de ataques BadUSB

Algunos virus modifican el firmware de los dispositivos USB para hacer que el sistema operativo considere que el dispositivo USB es un teclado. De esta manera, el virus puede ejecutar comandos en su cuenta de usuario para descargar malware, por ejemplo.

El componente Prevención de ataques BadUSB impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo.

Cuando un dispositivo USB se conecta a un equipo y el sistema operativo lo identifica como un teclado, la aplicación le solicita al usuario que ingrese un código numérico generado por la aplicación desde ese teclado o con un Teclado en pantalla, si está disponible (vea la siguiente imagen). Este procedimiento se conoce como autorización del teclado.

Si el código se ingresa correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al que se conectó) en la lista de teclados autorizados. No es necesario repetir la autorización del teclado cuando el teclado vuelve a conectarse o después del reinicio del sistema operativo.

Si el teclado autorizado se conecta a otro puerto USB del equipo, la aplicación mostrará otra vez una solicitud de autorización para este teclado.

Si se ha ingresado incorrectamente el código numérico, la aplicación genera un nuevo código. Puede configurar el número de intentos ingresando el código numérico. Si el código numérico se ingresa incorrectamente varias veces o se cierra la ventana de autorización del teclado (vea la siguiente imagen), la aplicación bloquea la entrada desde este teclado. Cuando transcurre el tiempo de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación le solicita al usuario que lleve a cabo nuevamente la autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea un teclado que no haya sido autorizado.

El componente Prevención de ataques BadUSB no se instala por defecto. Si desea utilizarlo, agréguelo en las propiedades del paquete de instalación antes de instalar la aplicación. Si la aplicación ya está instalada, modifique la selección de componentes disponibles.

Autorización del teclado

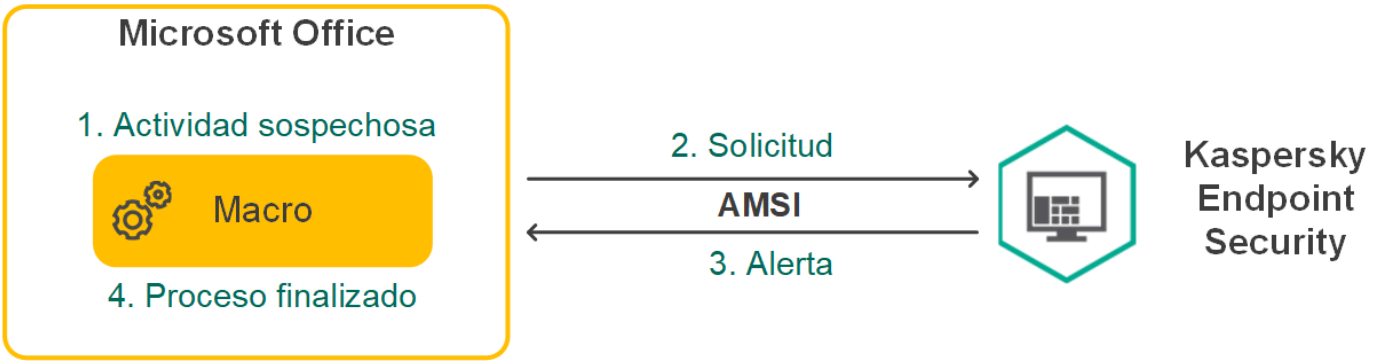
Configuración del componente Prevención de ataques BadUSB

Parámetro	Descripción
No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB	Si el interruptor está activado, la aplicación bloquea el uso del Teclado en pantalla para la autorización de un dispositivo USB desde el cual no se puede ingresar un código de autorización.
Prohibición del uso del código de barra para la autorización de dispositivos USB	Si el interruptor está habilitado, la aplicación no muestra el código de barras en la notificación de autenticación del lector de códigos de barras.
Número máximo de intentos de autorización del dispositivo USB	Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite cinco intentos para ingresar el código de autorización, la aplicación bloquea el dispositivo USB después del quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, volverá a tener 5 intentos para ingresar el código de autorización.
Tiempo de espera al alcanzar el número máximo de intentos	Duración del bloqueo del dispositivo USB después de la cantidad especificada de intentos fallidos de ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

Protección vía AMSI

El componente Protección vía AMSI está diseñado para admitir la Antimalware Scan Interface de Microsoft. La *interfaz de análisis antimalware AMSI* permite que las aplicaciones de terceros envíen a Kaspersky Endpoint Security aquellos objetos que precisan analizar (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 obtener más detalles sobre AMSI, consulte la documentación de Microsoft.

La Protección vía AMSI únicamente puede detectar amenazas y notificárselo a la aplicación. La aplicación de terceros después de recibir una notificación de una amenaza no le permite realizar acciones maliciosas (por ejemplo, la finaliza la acción).



Ejemplo del funcionamiento de AMSI

El componente Protección vía AMSI puede rechazar una solicitud de una aplicación de terceros, por ejemplo, si esta aplicación excede 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 vía AMSI no rechaza las solicitudes de aquellas aplicaciones de terceros para las cuales la integración continua con el componente de protección vía AMSI está habilitado.

La Protección vía 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
- Windows Server 2016 Essentials/Standard/Datacenter (se incluye el modo Server Core)
- Windows Server 2019 Essentials/Standard/Datacenter (se incluye el modo Server Core)
- Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition (se incluye modo Server Core)
- Windows Server 2025 Standard / Datacenter.

Configuración de Protección vía AMSI

Parámetro	Descripción
Analizar archivos de almacenamiento	Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
Analizar paquetes de distribución	Análisis de paquetes de distribución de aplicaciones de terceros.
Analizar archivos de Microsoft Office	Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. La aplicación analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla se seleccionó o no.
No desempaquetar archivos compuestos de gran tamaño	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada 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. Por ejemplo, los exploits pueden utilizar un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malintencionado. 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 podrían representar una amenaza para la seguridad del equipo. La aplicación recibe información sobre dichos procesos y las bases de datos antivirus.

Configuración del componente Prevención de exploits

Parámetro	Descripción
Al detectarse un exploit	**Bloquear**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit. **Informar**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security, registra una entrada con información del exploit y agrega información sobre este exploit a la lista de amenazas activas.
Habilitar la protección de la memoria de 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 del equipo y transmite esta información a los demás componentes de protección para mejorar su rendimiento. El componente Detección de comportamiento utiliza firmas de patrones de comportamiento para aplicaciones. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Endpoint Security realiza la acción de respuesta especificada. Las funcionalidades de Kaspersky Endpoint Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo.

El componente Detección de comportamiento también supervisa los puertos de red en busca de procesos de aplicaciones que podrían representar una amenaza para la seguridad del equipo. La aplicación recibe información sobre dichos procesos y las bases de datos antivirus.

Parámetros del componente Detección de comportamiento

Parámetro	Descripción
Acción al detectar actividad de malware	**Eliminar**. Si se elige esta opción, cuando se detecta actividad malintencionada, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación perjudicial y crea una copia de seguridad del archivo en Copia de seguridad. **Bloquear**. Si se elige esta opción, cuando se detecta actividad malintencionada, Kaspersky Endpoint Security finaliza la aplicación. **Informar**. Si se elige esta opción, cuando se detecta actividad malintencionada de parte de una aplicación, Kaspersky Endpoint Security permite que la aplicación se siga ejecutando, pero agrega información sobre la actividad malintencionada de esta aplicación a la lista de amenazas activas.

Prevención de intrusiones en el host

El componente Prevención contra intrusos impide que las aplicaciones realicen acciones que puedan ser peligrosas para el sistema operativo y garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus y el servicio de nube Kaspersky Security Network.

Para controlar el funcionamiento de las aplicaciones, el componente se basa en los *derechos* que estas tienen asignados. Los siguientes parámetros de acceso son algunos de esos derechos:

- Acceso a los recursos del sistema operativo (claves del Registro, opciones de ejecución automática, etc.)
- Acceso a datos personales (archivos, aplicaciones, etc.)

Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

Cuando una aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host hace lo siguiente:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.
2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Prevención de intrusiones en el host, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los grupos de confianza: *De confianza*, *Restricción mínima*, *Restricción máxima* o *No confiables*.

   Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea las acciones de la aplicación tomando como referencia el grupo de confianza al que pertenece. Por ejemplo, las aplicaciones del grupo *Restricción máxima* no pueden acceder a los módulos del sistema operativo.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

Configuración del componente Prevención de intrusiones en el host

Parámetro	Descripción
Derechos de aplicaciones	Tabla de aplicaciones controladas por el componente Prevención de intrusiones en el host. Cada aplicación está asignada a un grupo de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Puede elegir una aplicación de una lista única en la que se recogen todas las aplicaciones instaladas en los equipos sujetos a una directiva y agregarla a un grupo de confianza. Los derechos de acceso de las aplicaciones se recogen 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. • **Derechos**. Tabla de derechos de acceso a procesos y recursos del sistema operativo para aplicaciones pertenecientes al grupo de confianza. • **Reglas de red**. Tabla con las reglas de red que se han definido para las aplicaciones de un grupo de confianza. Las reglas le indican a Firewall cómo debe regular la actividad de red de las aplicaciones. La tabla contiene reglas de red predefinidas y recomendadas por los especialistas de Kaspersky. Dichas reglas se han incluido porque permiten proteger el tráfico de red de los equipos con Windows del mejor modo posible. Las reglas de red predefinidas no se pueden eliminar.
Recursos protegidos	La tabla contiene recursos del equipo clasificado. El componente Prevención de intrusiones en el host supervisa los intentos de otras aplicaciones de tener acceso a los recursos de la tabla. Un recurso puede ser una categoría de registro, archivo, carpeta o clave de registro.
Grupo de confianza para las aplicaciones que se ejecuten antes que Kaspersky Endpoint Security	Grupo de confianza en el que se colocarán 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 con firma digital	Si activa esta casilla, el componente Prevención de intrusiones en el host colocará las aplicaciones que tengan la firma digital de un proveedor de confianza en el grupo *De confianza*. Se considera proveedor de confianza a todo aquel proveedor de software en el que confía Kaspersky. De ser necesario, puede agregar manualmente el certificado de un proveedor al almacén de certificados de confianza. Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que tales aplicaciones sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.
Eliminar reglas de aplicaciones que no se iniciaron por más de N días (entre 1 y 90)	Si esta casilla está activada, Kaspersky Endpoint Security eliminará automáticamente la información (grupo de confianza y derechos de acceso) de una aplicación para la que se cumplan las siguientes condiciones: • El grupo de confianza o los derechos de acceso de la aplicación se definieron manualmente. • La aplicación no se inició en ningún punto del período definido. Cuando el grupo de confianza y los derechos de una aplicación se determinaron automáticamente, Kaspersky Endpoint Security elimina la información de esa aplicación luego de 30 días. El plazo de almacenamiento de la información no se puede modificar, y tampoco es posible desactivar la eliminación automática. Cuando vuelva a iniciar una aplicación cuya información se haya eliminado, Kaspersky Endpoint Security la analizará como si fuera la primera vez que se la ejecuta.
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 confiables**.

Motor de reparación

El componente Motor de reparación permite a Kaspersky Endpoint Security deshacer acciones que han sido realizadas por el malware en el sistema operativo.

Al revertir la actividad del malware en el sistema operativo, Kaspersky Endpoint Security gestiona los siguientes tipos de actividad de malware:

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto 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 eliminado o modificado.

- **Actividad del sistema**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Finaliza los procesos iniciados por el malware.
  - Finaliza los procesos en los cuales ha penetrado una aplicación malintencionada.
  - No reanuda procesos que el malware haya suspendido.

- **Actividad de la 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 las acciones del malware puede iniciarse durante un análisis de malware o a pedido de los componentes Protección contra archivos peligrosos o Detección de comportamiento.

La reversión de las operaciones del malware afecta a un conjunto de datos estrictamente definido. La reversión no tiene efectos negativos en el sistema operativo ni en la integridad de los datos de su 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 el software 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 los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, los servicios KSN proporcionan a Kaspersky Endpoint Security información sobre la reputación de las direcciones web analizadas, así como información sobre la categoría y la reputación de los archivos analizados. Para obtener más detalles sobre la configuración del acceso a KSN, consulte la Ayuda de Kaspersky Security Center.

El uso de Kaspersky Security Network es voluntario. La aplicación invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios pueden iniciar o discontinuar 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. Encontrará el texto de la Declaración de Kaspersky Security Network en el archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación.

La infraestructura de las bases de datos de reputación de Kaspersky

Kaspersky Endpoint Security da soporte a 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 detectados 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).* A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky. 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;

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
Habilitar el modo KSN extendido	El *modo KSN extendido* es un modo por el cual Kaspersky Endpoint Security remite información adicional a Kaspersky. Kaspersky Endpoint Security utiliza KSN para detectar amenazas independientemente del estado del interruptor.
Habilitar 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 bases de datos antivirus durante la siguiente actualización después de que la casilla se seleccionó. 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 bases de datos antivirus durante la siguiente actualización después de que la casilla se desactivó.
Estado del equipo cuando los servidores de KSN no estén disponibles *(disponible solo en la Consola de Kaspersky Security Center)*	Con los elementos de esta lista desplegable, puede indicar qué estado tendrá un equipo en Kaspersky Security Center cuando los servidores de KSN no estén disponibles.
Usar el 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.
Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté 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 de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network).

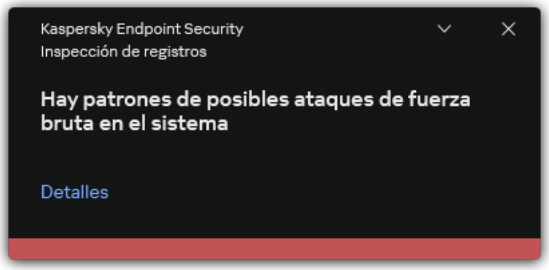
Inspección de registros

Para que pueda usar este componente, Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores. El componente no estará disponible si Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo.

A partir de la versión 11.11.0, Kaspersky Endpoint Security para Windows incluye el componente de Inspección de registros. Inspección de registro monitorea la integridad del entorno protegido en función del análisis del registro de eventos de Windows. Cuando la aplicación detecta indicios de un comportamiento atípico en el sistema, informa al administrador, ya que este comportamiento puede indicar un intento de ciberataque.

Kaspersky Endpoint Security analiza los registros de eventos de Windows y detecta las infracciones de acuerdo con las reglas. El componente incluye reglas predefinidas. Las reglas predefinidas funcionan con análisis heurístico. También puede agregar sus propias reglas (reglas personalizadas). Cuando se activa una regla, la aplicación crea un evento con el estado *Crítico* (consulte la imagen a continuación).

Si desea utilizar Inspección de registros, asegúrese de que la seguridad de la directiva de auditoría esté configurada y que el sistema registre los eventos relevantes (para obtener información, consulte el sitio web de Soporte técnico de Microsoft).



Notificación de Inspección de registro

Configuración de Inspección de registro

Parámetro	Descripción
Reglas predefinidas	Lista de reglas de Inspección de registro. Las reglas predefinidas incluyen plantillas de actividad anormal en el equipo protegido. La actividad anormal puede implicar un intento de ataque.
Reglas personalizadas	Lista de reglas de Inspección de registro que agregó el usuario. Puede establecer sus propios criterios de activación de las reglas de Inspección de registro. Para hacerlo, debe ingresar un ID de evento y seleccionar una fuente de evento. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*. También puede especificar el registro de una aplicación de terceros.

Anticifrador

El componente Anticifrador analiza la actividad en las carpetas compartidas. Cuando la actividad coincide con una firma de patrones de comportamiento que suele verse en actos de cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.

Kaspersky Endpoint Security evita el cifrado externo de solo esos archivos que se localizan en medios que tienen el sistema de archivos NTFS y no están cifrados por el sistema EFS.

Parámetro	Descripción
Exclusiones por nombre o dirección IP	**Exclusiones por nombre o dirección IP**. La lista de equipos desde los cuales los 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 habilitar 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 habilitada. Para obtener más información sobre la directiva de auditoría de seguridad de Windows, visite el sitio web de Microsoft . **Exclusiones por máscara**. Exclusiones del alcance de la protección. Excluir una carpeta del alcance de la protección puede reducir la cantidad de falsos positivos si su organización utiliza el cifrado de datos cuando se intercambian archivos utilizando carpetas compartidas. Por ejemplo, Detección de comportamiento puede generar falsos positivos cuando el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Dicha actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, agregue esa carpeta a las exclusiones. Usar máscaras: • El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. • `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 esta opción está seleccionada, al detectar un intento de modificar archivos en carpetas compartidas, Kaspersky Endpoint Security agrega información sobre este intento a la lista de amenazas activas, agrega una entrada a los informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center. • **Bloquear conexión por (min) N min**. Si se elige esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados. Si el componente Motor de reparación se habilita y la opción **Bloquear conexión por (min) N minutos** se selecciona, los archivos modificados se restauran desde copias de seguridad.
Alcance de la protección	El *alcance de la 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 ingresar una máscara. De manera 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. Esto permite reducir el tráfico y el uso inadecuado del tiempo de trabajo. Cuando un usuario intente abrir un sitio web restringido por Control web, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia (vea la siguiente imagen).

Para utilizar Control web, debe completar la configuración inicial de la aplicación:

- Para que la aplicación pueda supervisar el tráfico HTTPS, habilite el análisis de conexiones cifradas (habilitada de manera predeterminada).

- Seleccione los puertos que Kaspersky Endpoint Security debe supervisar (de forma predeterminada, la aplicación controla todos).

- Seleccione las aplicaciones cuyo tráfico desee que Kaspersky Endpoint Security supervise. La mayoría de los navegadores ya figuran en la lista de aplicaciones que recomienda Kaspersky. Si el navegador que utiliza no está en la lista, agréguelo.

- Recomendamos inyectar un script de interacción de página web en el tráfico web (la inyección de script está deshabilitada de forma predeterminada). Esta secuencia de comandos 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. Puede impedir que sus usuarios accedan a sitios catalogados como *Redes sociales*, por ejemplo, o a otras categorías.

- **Tipo de datos**. Puede restringir el acceso a ciertos tipos de datos y, por ejemplo, ocultar las imágenes de un sitio web. 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 de almacenamiento* 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 la 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.

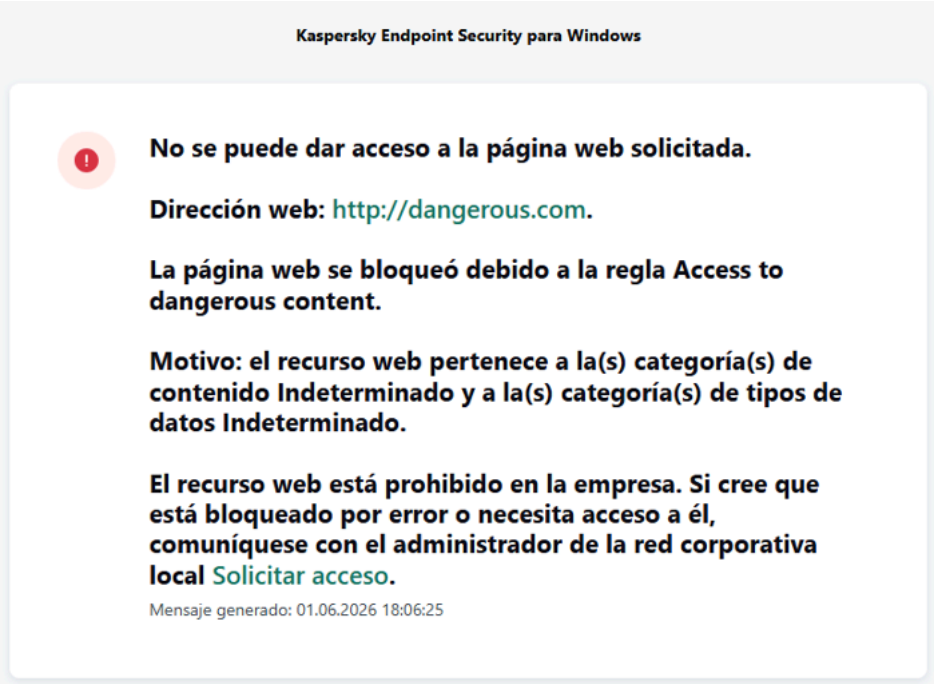
  Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.

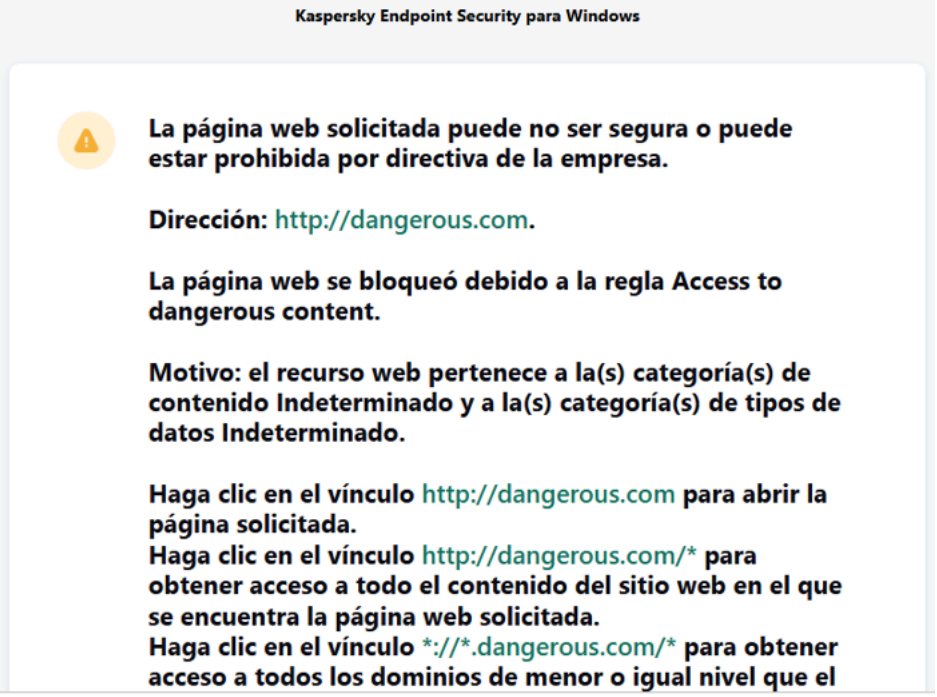
- Programación de la regla.

  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 arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado 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 arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado 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. Las siguientes opciones están disponibles: • **Permitir todo lo que no esté en la lista de reglas**, también denominado modo de lista de rechazados para sitios web prohibidos. • **Denegar todo lo que no esté en la lista de reglas**, también denominado modo de lista de admitidos para sitios web permitidos.
Finalizar las sesiones de navegador activas después de aplicar la regla	Si se selecciona la casilla, Control web finaliza la conexión a los recursos web bloqueados inmediatamente después de que se aplica la directiva. El navegador deja de descargar datos de la página web inmediatamente. Cuando actualiza la página web o accede a otra página web prohibida, la aplicación muestra una advertencia. Control web permite la desconexión inmediata de los recursos web solo en los navegadores web. Para otras aplicaciones, Control web solo restringe las nuevas conexiones. Si anula la selección de la casilla, Control web solo restringe las conexiones nuevas a los recursos web prohibidos. Control web no finaliza las conexiones activas.
Plantillas	**Advertencia**. El campo de entrada consiste en una plantilla del mensaje que se muestra si se activa una regla de advertencia acerca de intentos para acceder a un recurso web no deseado. **Mensaje para bloqueos**. El campo de entrada contiene la plantilla del mensaje que se muestra si se activa una regla que bloquea el acceso a un recurso web. **Mensaje para el administrador**. Plantilla del mensaje que se enviará al administrador de LAN si el usuario considera que se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del acceso a una página web para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 las plantillas de mensajes (por ejemplo, `%USER_NAME%`). Las variables permiten utilizar una única plantilla de mensajes para diferentes equipos.
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 compatibles con la función de monitoreo: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. El monitoreo de la actividad del usuario 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

El Control de dispositivos administra el acceso de los usuarios a los dispositivos que se instalan o se conectan al equipo (por ejemplo, discos duros, cámaras o módulos Wi-Fi). Esto impide la infección del equipo cuando se conectan dichos dispositivos y evita las pérdidas o fugas de datos.

Si el componente Control de dispositivos está habilitado, 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

El 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 de la siguiente manera:

  - Permitir – ✓.
  - Bloquear – ⊘.
  - Por reglas (solo impresoras y dispositivos portátiles) – .
  - Depende del bus de conexión (excepto Wi-Fi) – .
  - Bloquear con excepciones (solo Wi-Fi) – .

- **Bus de conexión**. El *bus de conexión* es una interfaz utilizada 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 de la siguiente manera:

  - 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 completo en todo momento.

  Puede agregar dispositivos de confianza en función de los siguientes datos:

  - **Dispositivos por Id**. Cada dispositivo tiene un identificador único (id. de hardware, también denominado HWID). Puede ver el Id. en las propiedades del dispositivo usando las herramientas del sistema operativo. Un Id. de dispositivo típico podría ser: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id.

  - **Dispositivos por modelo**. Cada dispositivo tiene un id. de proveedor (VID) y un id. de producto (PID). Puede ver los ID. en las propiedades del dispositivo usando las herramientas del sistema operativo. Los valores VID y PID deben especificarse en este formato: `VID_1234&PID_5678`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.

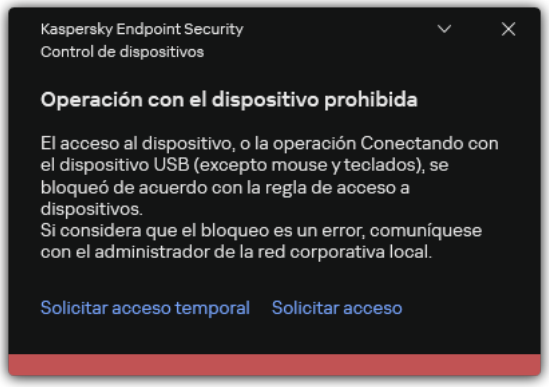
  - **Dispositivos por máscara de id**. Si está usando varios dispositivos con Id. similares, puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `WDC_C*`.

  - **Dispositivos por máscara de modelo**. Si está usando varios dispositivos con VID o PID similares (por ejemplo, dispositivos del mismo fabricante), puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `VID_05AC&PID_*`.

El Control de dispositivos regula el acceso de los usuarios a los dispositivos usando *reglas de acceso*. El Control de dispositivos también le permite guardar eventos relacionados con la 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 los eventos relacionados con la conexión/desconexión de dispositivos, autorice el acceso al tipo de dispositivo correspondiente (estado) o agregue el dispositivo a la lista de dispositivos de confianza.

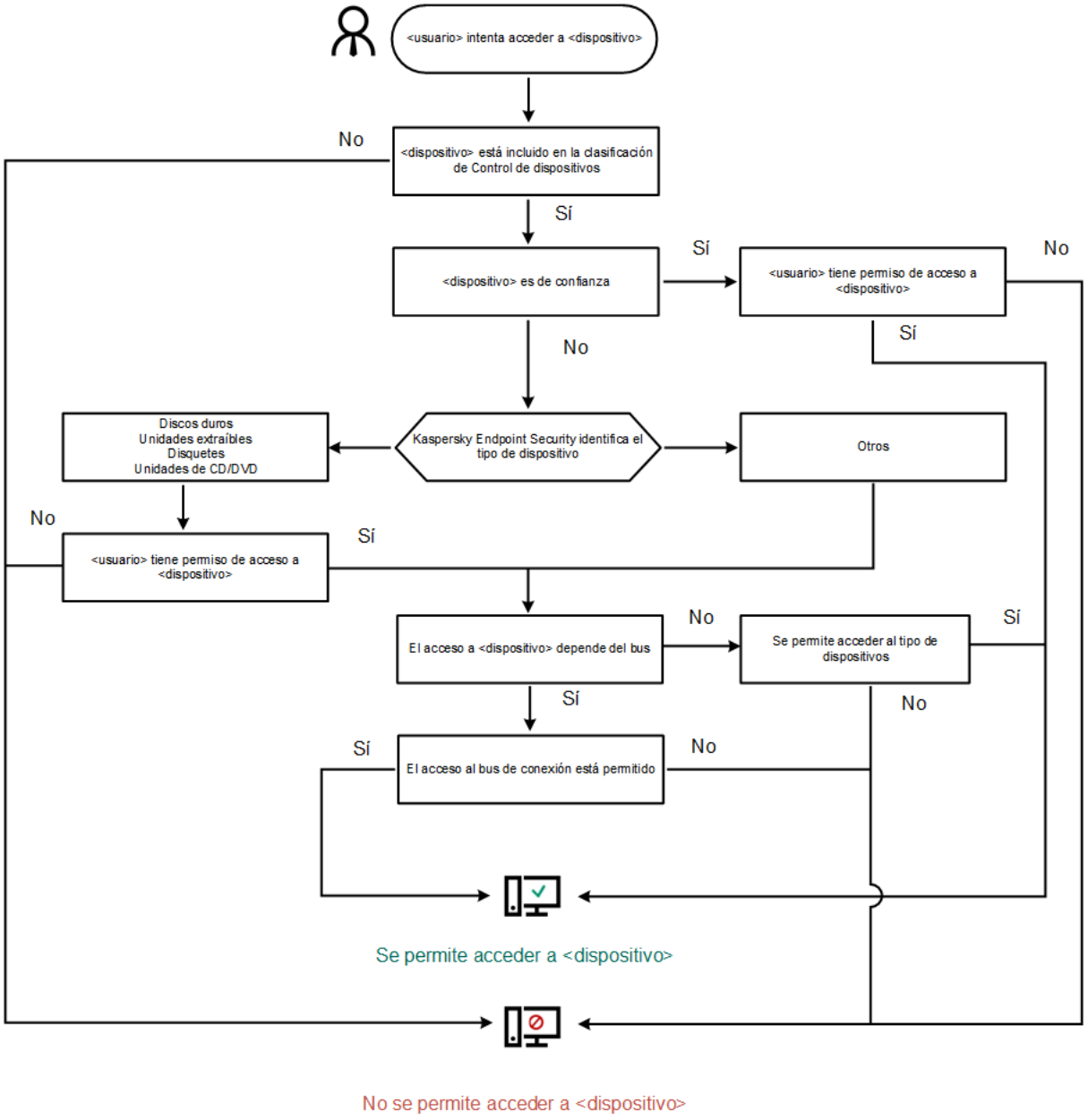
Cuando se conecta al equipo un dispositivo que está bloqueado por el Control de dispositivos, Kaspersky Endpoint Security bloqueará el acceso y mostrará que una notificación (consulte la figura a continuación).



Notificación del Control de dispositivos

Algoritmo de funcionamiento del Control de dispositivos

Kaspersky Endpoint Security decide si permitirá el acceso a un dispositivo después de que el usuario conecta el dispositivo al equipo de la siguiente imagen.



Algoritmo de funcionamiento del 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 un sistema de archivos se bloqueará solo la próxima vez que el dispositivo se conecte.

Si un usuario del equipo con Kaspersky Endpoint Security instalado debe solicitar acceso a un dispositivo que cree fue bloqueado por error, 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, el botón **Solicitar acceso** estará 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 Wi-Fi	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 a los dispositivos según el tipo de bus de conexión si se selecciona el modo **Depende del bus de conexión**.
Dispositivos de confianza	Una lista con los dispositivos de confianza y los usuarios que tienen acceso a esos dispositivos.
Combinar 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 está seleccionada, los elementos de la lista de la directiva principal de Kaspersky Security Center se mostrarán en las directivas secundarias. Así 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. Si lo necesita, podrá agregar, editar y eliminar elementos de la lista en directivas de menor jerarquía. 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 esta casilla no está seleccionada, los elementos de las listas no se fusionarán cuando una directiva de Kaspersky Security Center herede la configuración de otra. Esta funcionalidad también permite fusionar listas en perfiles de directivas. Para fusionar listas, en el perfil de mayor prioridad, habilite la herencia de la configuración de un perfil de menor prioridad. Para obtener más detalles sobre las prioridades del perfil 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, Wi-Fi), 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 Wi-Fi), 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, Wi-Fi y módem.
Plantillas de mensajes	**Mensaje para bloqueos**. 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**. Plantilla del mensaje que se envía al administrador de la red de área local cuando el usuario considera que el acceso a un dispositivo se ha bloqueado por error o, de manera similar, que la posibilidad de realizar una operación con el contenido de un dispositivo se ha bloqueado por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del acceso a un dispositivo para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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 componente Control de aplicaciones se utiliza para gestionar la ejecución de aplicaciones en los equipos de los usuarios. Permite, con ello, implementar una directiva de seguridad corporativa que regule el uso de aplicaciones. Gracias a las restricciones de acceso, el componente también ayuda a reducir el riesgo de que los equipos se infecten.

Los pasos para configurar Control de aplicaciones son los siguientes:

1. Creación de categorías de aplicaciones.

   El administrador crea categorías con las aplicaciones que desea controlar. Las categorías de aplicaciones impactan en todos los equipos de una red corporativa, independientemente del grupo de administración al que pertenecen. Las categorías se crean sobre la base de distintos criterios: categoría KL (por ejemplo, *Navegadores* u otra categoría), hash del archivo, proveedor de la aplicación y otros.

2. Creación de reglas de Control de aplicaciones.

   El administrador crea reglas de Control de aplicaciones dentro de la directiva asignada a un grupo de administración. Las reglas contienen las distintas categorías de aplicaciones y el estado de ejecución (inicio permitido o bloqueado) asignado a las aplicaciones de esas categorías. El administrador puede crear la cantidad de reglas que desee. Una aplicación puede coincidir con los criterios de varias reglas. La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. Kaspersky Endpoint Security comprueba si una aplicación coincide con una regla cada vez que se inicia. Kaspersky Endpoint Security compara de forma secuencial la aplicación con todas las reglas de Control de aplicaciones.

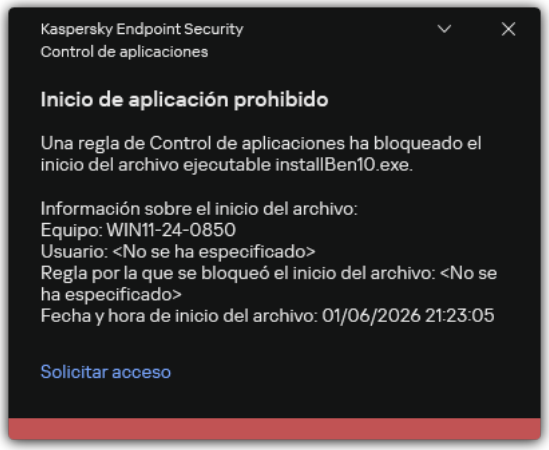
3. Selección del modo de Control de aplicaciones.

   El administrador decide el modo para trabajar con aplicaciones que no están contempladas en ninguna de las reglas (lista de autorización y de bloqueo).

Cuando un usuario intenta ejecutar una aplicación prohibida, Kaspersky Endpoint Security se lo impide y le muestra una notificación (vea la imagen de más abajo).

Existe un *modo de prueba*, diseñado para verificar la configuración de Control de aplicaciones. Cuando se utiliza este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite que se ejecute cualquier aplicación, esté o no prohibida.
- Muestra una notificación cuando se inicia una aplicación prohibida y agrega el evento al informe almacenado en el equipo del usuario.
- Transfiere información sobre la ejecución 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 permite que los usuarios inicien cualquier aplicación, excepto por las que se hayan prohibido a través de las reglas de Control de aplicaciones.

  Este modo de Control de aplicaciones está habilitado por defecto.

- **Lista de admitidos**. En este modo, Control de aplicaciones no permite que ningún usuario inicie ninguna aplicación, excepto por las que se hayan permitido (y no prohibido) a través de las reglas de Control de aplicaciones.

  Si se configuran completamente las reglas de autorización del Control de aplicaciones, el componente bloquea el inicio de todas las aplicaciones nuevas que no han sido verificadas por el administrador de la red LAN, mientras que permite el funcionamiento del sistema operativo y de las aplicaciones de confianza de las que dependen los usuarios para hacer su trabajo.

  Puede leer las recomendaciones sobre cómo configurar las reglas de control de aplicaciones en el modo de lista de autorización.

El Control de aplicaciones se puede configurar para funcionar en estos modos, tanto a través de la interfaz local de Kaspersky Endpoint Security como por medio de 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 necesarias para las siguientes tareas:

- Creación de categorías de aplicaciones.

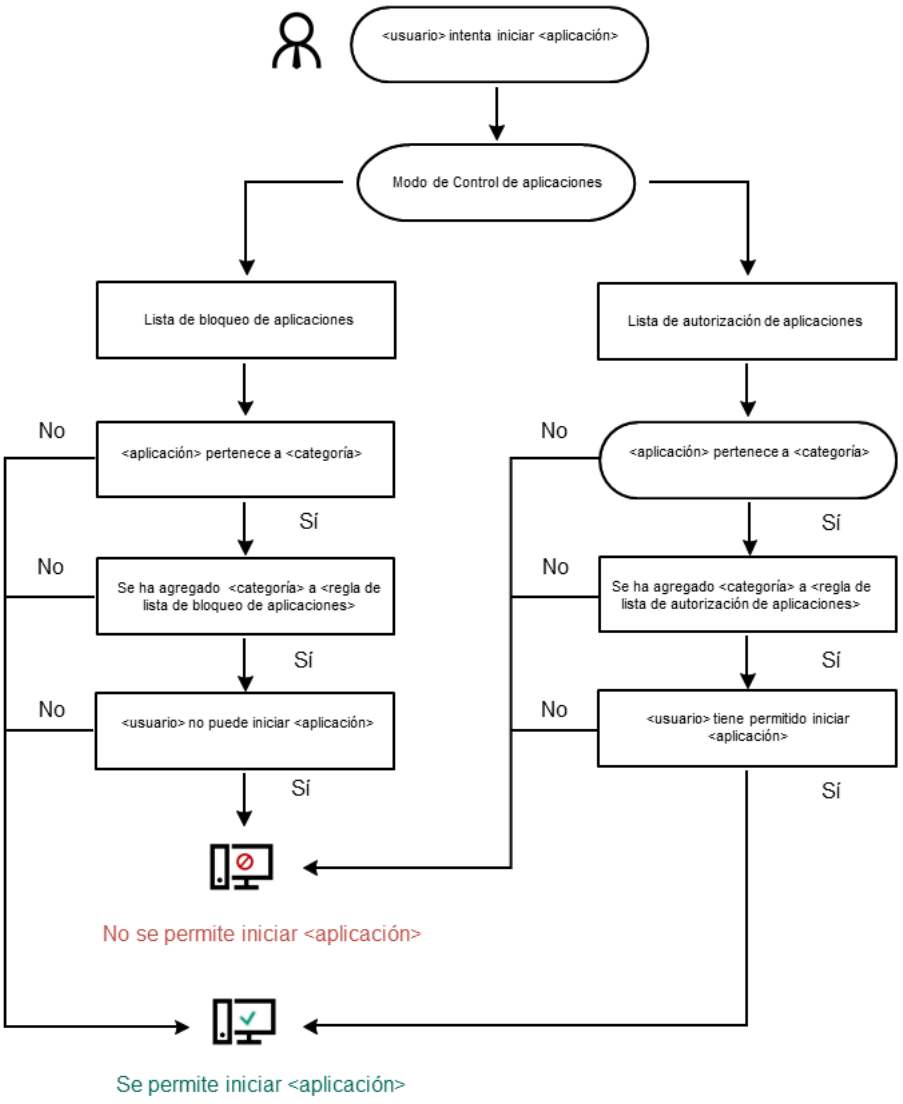
  Las reglas de Control de aplicaciones creadas en la Consola de administración de Kaspersky Security Center se basan en sus categorías de aplicaciones personalizadas, y no en condiciones de inclusión y exclusión como es el caso de la interfaz local de Kaspersky Endpoint Security.

- Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN.

Por este motivo se recomienda utilizar 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 decidir si una aplicación podrá iniciarse (vea la siguiente imagen).



Algoritmo de funcionamiento de Control de aplicaciones

Parámetro	Descripción
Acción al iniciar aplicaciones bloqueadas por las reglas	**Aplicar reglas**. Kaspersky Endpoint Security controla el inicio de las aplicaciones según el modo seleccionado. **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 aplicaciones	Puede seleccionar una de las siguientes opciones: • **Lista de rechazados**. Si se selecciona esta opción, el Control de aplicaciones permite que todos los usuarios inicien cualquier aplicación, excepto en casos en que las aplicaciones cumplan con las condiciones de las reglas de bloqueo de Control de aplicaciones. • **Lista de admitidos**. Si se selecciona esta opción, el Control de aplicaciones bloquea a todos los usuarios de iniciar alguna aplicación, excepto en casos en que las aplicaciones cumplen con las condiciones de reglas de habilitación del Control de aplicaciones. Cuando se selecciona el modo **Lista de admitidos**, se crean automáticamente dos Reglas de control de aplicaciones: • **Imagen de oro**. • **Actualizadores de confianza**. No puede modificar la configuración ni eliminar las reglas creadas automáticamente. Puede habilitar o deshabilitar estas reglas.
Supervisar la carga de módulos DLL	Si se selecciona la casilla, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. En el informe se registra información acerca del módulo de DLL y la aplicación que cargó el mismo. Si planea supervisar la carga de controladores y módulos DLL, asegúrese de que una de las siguientes reglas esté habilitada en la configuración de Control de aplicaciones: la **Imagen de oro** predeterminada u otra regla que contenga la categoría KL "**Imagen de oro\Certificados de confianza**" y que garantice que los módulos DLL y los controladores de confianza se carguen antes del arranque de Kaspersky Endpoint Security. Habilitar la supervisión de la carga de módulos DLL y controladores cuando la regla **Imagen de oro** está deshabilitada puede causar inestabilidad en el sistema operativo. Kaspersky Endpoint Security solamente supervisa los módulos DLL y los controladores cargados desde que se seleccionó la casilla. Después de seleccionar la casilla, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y los controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.
Usar verificación estricta de firma digital	Puede seleccionar un certificado como condición de activación para una regla de Control de aplicaciones. Si se selecciona esta casilla, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas con certificados solo del almacén de confianza de certificados del sistema. Las aplicaciones firmadas con dicho certificado también se consideran de confianza para los componentes de protección, por ejemplo, la tarea *Análisis de malware*. Sin embargo, si especifica un certificado de un almacén diferente en una regla de Control de aplicaciones, Kaspersky Endpoint Security no aplica dicha regla. Si la casilla no está seleccionada, Kaspersky Endpoint Security aplica las reglas a las aplicaciones firmadas por un certificado del Almacén de certificados raíz de confianza de Windows. Estas aplicaciones no forman parte de la zona de confianza. Los componentes de protección controlan la actividad de tales aplicaciones.
Plantillas de mensajes sobre el bloqueo de la aplicación	**Mensaje para bloqueos**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación. **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo del inicio de una aplicación para el administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha 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 conectados a una red corporativa. Para ello utiliza una serie de reglas, diseñadas para buscar comportamientos que no se consideran típicos (por ejemplo, la regla *Inicio de Microsoft PowerShell desde una aplicación de ofimática*). Los especialistas de Kaspersky crean estas reglas basándose en casos característicos de actividad maliciosa. La manera en que el Control de anomalías adaptativo responde ante cada regla es configurable; esto significa que, por ejemplo, es posible permitir la ejecución de scripts de PowerShell que se hayan creado para automatizar ciertos aspectos de un flujo de trabajo. Las reglas se actualizan junto con las bases de datos de Kaspersky Endpoint Security. No obstante, las actualizaciones para las reglas deben confirmarse manualmente.

Configuración del Control de anomalías adaptativo

Los pasos para configurar el Control de anomalías adaptativo son los siguientes:

1. Usar el modo de aprendizaje del Control de anomalías adaptativo.

   Una vez que el Control de anomalías adaptativo se habilita, sus reglas entran en un *modo de aprendizaje*. Mientras dicho modo está activo, el Control de anomalías adaptativo monitorea la activación de las reglas y envía los eventos de activación a Kaspersky Security Center. El tiempo de aprendizaje varía según la regla. Quienes definen la duración son los expertos de Kaspersky. Lo normal es que el modo de aprendizaje esté activo por dos semanas.

   Si una regla no se activa en lo absoluto durante el período de aprendizaje, el componente considerará que las acciones asociadas con la regla son atípicas. En consecuencia, Kaspersky Endpoint Security bloqueará cualquier acción vinculada con esa regla.

   Si una regla se activa durante el período de aprendizaje, Kaspersky Endpoint Security dejará constancia de los eventos en el informe de activación de las reglas y en el repositorio **Activación de reglas en el estado Aprendizaje inteligente**.

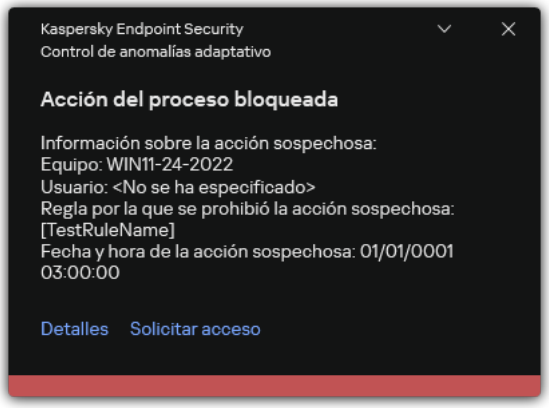
2. Analizar el informe de activación de las reglas.

   El administrador analiza el informe de activación de reglas o el contenido del repositorio **Activación de reglas en el estado Aprendizaje inteligente**. A continuación, selecciona cómo reaccionará el Control de anomalías adaptativo cuando se active una regla; las opciones posibles son permitir y bloquear. El administrador también puede optar por seguir controlando el funcionamiento de la regla y extender la duración del modo de aprendizaje. Si el administrador no realiza ninguna acción, la aplicación seguirá operando en modo de aprendizaje. El plazo de aprendizaje se reiniciará.

Control de anomalías adaptativo se configura en tiempo real mediante los siguientes canales:

- El Control de anomalías adaptativo comienza a bloquear automáticamente las acciones asociadas con las reglas que nunca se activaron en el modo de aprendizaje.
- Kaspersky Endpoint Security agrega reglas nuevas o elimina las que han quedado obsoletas.
- El administrador configura el funcionamiento de Control de anomalías adaptativo tras revisar el informe de activación de reglas y el contenido del repositorio **Activación de reglas en el estado Aprendizaje inteligente**. Recomendamos consultar el informe sobre la activación de reglas y el contenido del almacenamiento **Activación de reglas en el estado Aprendizaje inteligente**.

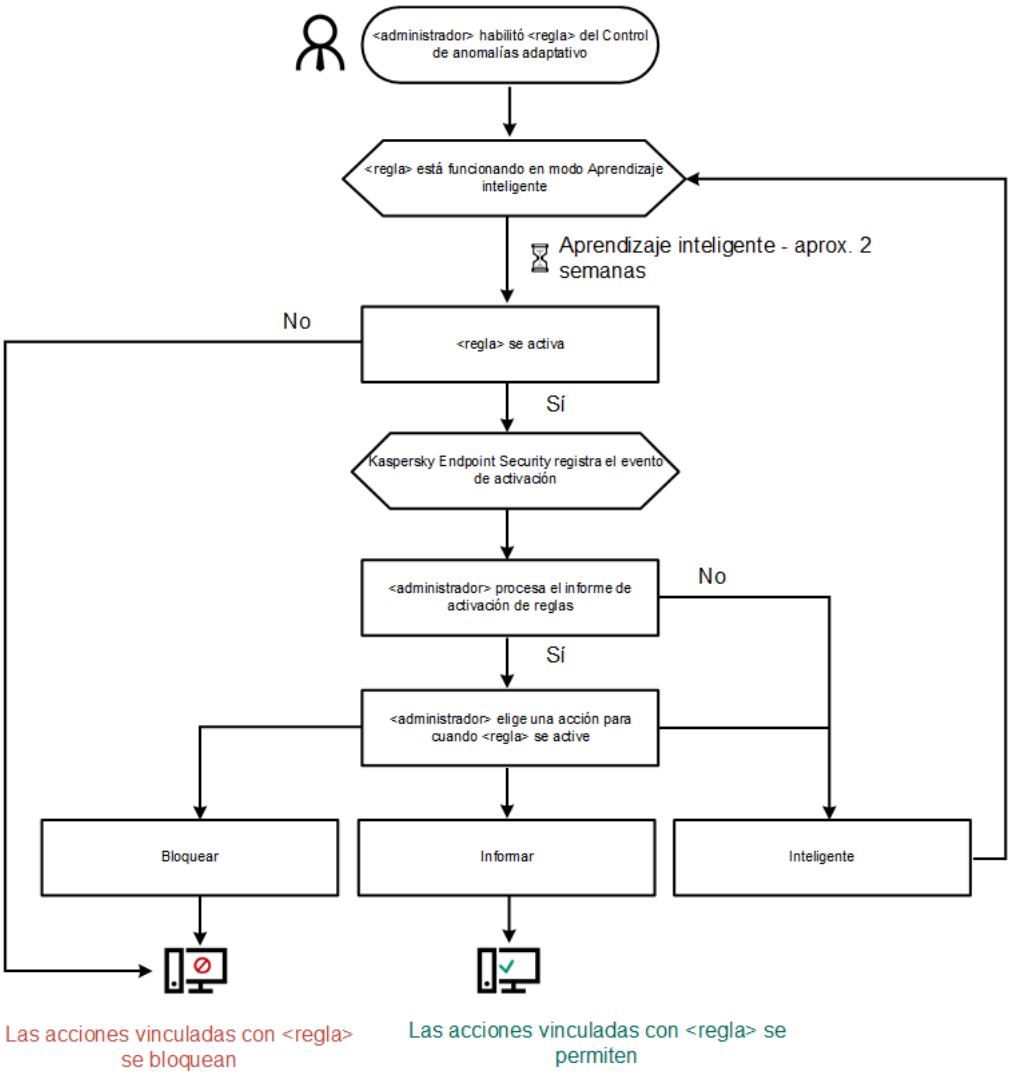
Cuando una aplicación maliciosa intente realizar una acción, Kaspersky Endpoint Security bloqueará el intento y mostrará una notificación (consulte la siguiente imagen).



Notificación del Control de anomalías adaptativo

Algoritmo de funcionamiento del Control de anomalías adaptativo

Para determinar si una acción asociada a una regla debe permitirse o bloquearse, Kaspersky Endpoint Security usa el algoritmo de la siguiente imagen.



Algoritmo de funcionamiento del Control de anomalías adaptativo

Parámetros del componente Control de anomalías adaptativo

Parámetro	Descripción
Informe sobre el estado de las reglas del Control de anomalías adaptativo *(disponible solo en la Consola de Kaspersky Security Center)*	Informe sobre el estado asignado a las reglas de detección del Control de anomalías adaptativo (por ejemplo, *Deshabilitado* o *Bloquear*). El informe se genera para todos los grupos de administración.
Informe sobre las reglas activadas del Control de anomalías adaptativo *(disponible solo en la Consola de Kaspersky Security Center)*	Informe sobre las acciones atípicas detectadas por el Control de anomalías adaptativo. El 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 estas reglas basándose en casos característicos de actividad maliciosa.
Plantillas	**Mensaje para bloqueos**. Plantilla del mensaje que se le mostrará al usuario cuando se active una regla del Control de anomalías adaptativo para bloquear una acción atípica. **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la red local corporativa si considera que una acción se bloqueó por error. Después de que el usuario solicita proporcionar acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje de bloqueo de actividad de aplicación enviado al administrador**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center a través de la selección de eventos predefinida **Solicitudes de usuario**. 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

Para que pueda usar este componente, Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores. El componente no estará disponible si Kaspersky Endpoint Security debe estar instalado 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 del registro y la conexión de los dispositivos externos.

El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que podrían indicar filtraciones de seguridad en el equipo. Cuando se detectan dichos cambios, Kaspersky Endpoint Security genera los eventos y las alertas correspondientes, y las envía al administrador. Control de integridad del sistema puede operar en tiempo real y también puede realizar controles de integridad del sistema a pedido.

Control de integridad del sistema en tiempo real

En el modo de tiempo real, Control de integridad del sistema realiza un seguimiento de los cambios en los objetos que incluyó en el alcance del componente (el *alcance del monitoreo*). Además, Control de integridad del sistema permite bloquear el acceso no autorizado a dichos objetos en tiempo real.

Comprobación de integridad del sistema a pedido

Comprobación de integridad del sistema a pedido es una tarea que se puede ejecutar manualmente o según una programación. Para ejecutar la tarea *Comprobación de integridad del sistema*, debe configurar el alcance del componente (el *alcance del monitoreo*) y crear una línea de base. Una *línea de base* es un estado registrado de los objetos en el sistema que la aplicación usa como referencia cuando se compara con el estado actual.

Configuración de Control de integridad del sistema

Parámetro	Descripción
Modo de funcionamiento de las reglas de bloqueo	• **Bloquear**. En este modo, Control de integridad del sistema bloquea las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente. • **Informar**. En este modo, Control de integridad del sistema permite las acciones con archivos y claves del registro del alcance del monitoreo y genera un evento correspondiente.

Parámetro	Descripción
Control de integridad del sistema en tiempo real	En el modo de tiempo real, Control de integridad del sistema realiza un seguimiento de los cambios en los objetos que incluyó en el alcance del componente (el *alcance del monitoreo*). Además, Control de integridad del sistema permite bloquear el acceso no autorizado a dichos objetos en tiempo real.
Supervisar dispositivos	Control de integridad del sistema supervisa la conexión y desconexión de dispositivos externos.
Supervisar archivos y el registro	Control de integridad del sistema supervisa los cambios en los archivos, las carpetas y el registro.
Comprobación de integridad del sistema	Comprobación de integridad del sistema a pedido es una tarea que se puede ejecutar manualmente o según una programación. Para ejecutar la tarea *Comprobación de integridad del sistema*, debe configurar el alcance del componente (el *alcance del monitoreo*) y crear una línea de base. Una *línea de base* es un estado registrado de los objetos en el sistema que la aplicación usa como referencia cuando se compara con el estado actual.

Endpoint Sensor

Endpoint Sensor no forma parte de Kaspersky Endpoint Security 11.4.0.

Para administrar el componente Endpoint Sensor, puede usar Kaspersky Security Center Web Console o la Consola de administración de Kaspersky Security Center. No es posible usar Kaspersky Security Center Cloud Console para administrar Endpoint Sensor.

Endpoint Sensor es un componente diseñado para interactuar con Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* es una solución que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. 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 adquirir todas las unidades funcionales o las unidades funcionales individuales por separado. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

La capacidad de administrar el componente Endpoint Sensor está sujeta a ciertas restricciones:

- Los ajustes de Endpoint Sensor pueden configurarse utilizando una directiva si el equipo tiene instalado Kaspersky Endpoint Security versiones 11.0.0 a 11.3.0. Si necesita información adicional para configurar los ajustes de Endpoint Sensor a través de una directiva, consulte los artículos de ayuda correspondientes a las versiones anteriores de Kaspersky Endpoint Security.
- Los ajustes de Endpoint Sensor no pueden configurarse a través de una directiva si el equipo tiene instalado Kaspersky Endpoint Security 11.4.0 o una versión posterior.

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 los siguientes 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 incluye un agente incorporado para la integración con la solución 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 los objetos en servidores especiales con imágenes virtuales implementadas de los sistemas operativos Microsoft Windows (servidores de Sandbox). Para obtener más información sobre 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 de Kaspersky Sandbox, el componente KATA Sandbox permite analizar archivos no solo de forma automática, sino también manualmente desde el menú contextual del archivo.

KATA Sandbox requiere la implementación de Kaspersky Anti Targeted Attack Platform 7.0 o una versión posterior.

El componente se puede administrar solo mediante el uso de Kaspersky Security Center Web Console. No puede administrar este componente mediante el uso de 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 el 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: • **Manualmente**. El usuario envía manualmente el archivo para analizarlo desde el menú contextual (**Enviar a Sandbox**). • **Automáticamente**. La aplicación detecta objetos y los envía a Sandbox para analizarlos de manera automática. • **Combinado**.
Configuración de conexión con el servidor	**Tiempo de espera (ms)**. Tiempo de espera de la conexión al servidor de Sandbox (para Kaspersky Sandbox) o al 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 conexión agotado para el 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 solicitudes**. 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 la cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Sandbox deja de agregar 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. Luego, debe agregar el certificado al equipo mediante una directiva. También debe agregar 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña.
Conexión a servidores de Sandbox	**Kaspersky Sandbox**. Configuración de la conexión del servidor de Sandbox. Los servidores utilizan imágenes virtuales implementadas de los sistemas operativos Microsoft Windows para ejecutar objetos que necesitan ser analizados. Puede ingresar 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 esta opción está seleccionada, 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 Cuarentena. **Ejecutar análisis de áreas críticas**. Si esta opción está seleccionada, Kaspersky Endpoint Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del kernel, los procesos en ejecución y los sectores de inicio del disco. **Crear tarea de Análisis de IOC**. Si esta opción está seleccionada, Kaspersky Endpoint Security crea automáticamente la tarea *Análisis de IOC (tarea de análisis de IOC independiente)*. Para esta tarea, puede configurar el modo de ejecución, el alcance del análisis y la acción que se realizará al detectar un IOC (*Mover la copia a la Cuarentena, eliminar objeto* o *Ejecutar análisis de áreas críticas*). Para modificar otros opciones de la tarea *Análisis de IOC*, vaya a la configuración de la tarea.
Alcance del Análisis de IOC	**Áreas críticas del archivo**. Si esta opción esta seleccionada, Kaspersky Endpoint Security realiza un análisis de IOC solo en áreas críticas del archivo del equipo: memoria del núcleo y sectores de inicio. **Áreas de archivos en la unidad del sistema del equipo**. Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC en la unidad del sistema del equipo.
Ejecute la tarea de Análisis de IOC	**Manualmente**. Modo de ejecución en el que puede iniciar la tarea de *Análisis de IOC* manualmente en el momento que sea conveniente para usted. **Automáticamente**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta automáticamente la tarea *Análisis de IOC* después de que se detecta una amenaza. **Ejecutar solo cuando el equipo esté inactivo**. Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea de *Análisis de IOC* si el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security pone la tarea en pausa. 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 usa datos de telemetría recibidos de puntos de conexión y aprendizaje automático. MDR envía los datos de los incidentes a los expertos de Kaspersky. A continuación, los expertos pueden procesar el incidente y, por ejemplo, agregar una nueva entrada a las bases de datos antivirus. Alternativamente, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener más detalles sobre el funcionamiento de 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 la ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. Encontrará el archivo BLOB en el archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre el 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 lo sucesivo, también denominada "EDR Optimum"). A partir de la versión 11.8.0, Kaspersky Endpoint Security para Windows incluye un agente incorporado para la solución Kaspersky Endpoint Detection and Response Expert (en lo sucesivo, también denominada "EDR Expert"). *Kaspersky Endpoint Detection and Response* es una variedad de soluciones para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. Las funcionalidades de las soluciones combinan la detección automática de las amenazas con la capacidad para reaccionar a estas amenazas para contrarrestar los 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 antes 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 revisa y analiza el desarrollo de las amenazas y proporciona al *personal de seguridad* o al *Administrador* la información sobre el posible ataque necesaria para una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana independiente. Una *alerta* es un evento en la infraestructura de TI corporativa que la aplicación identificó como inusual o sospechoso y que puede representar una amenaza para la seguridad de la infraestructura de TI corporativa. *Detalles de la alerta* es una herramienta para ver la totalidad de la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, 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 la consola web y en la consola en la nube. La configuración del componente Endpoint Detection and Response Expert (cloud) solo está disponible en Cloud Console.

Parámetro	Descripción
Habilitar el registro avanzado de la actividad del sistema	La telemetría extendida mejora la precisión en la detección de IOC, pero utiliza más recursos del equipo. Recomendamos habilitar la telemetría extendida en el equipo para realizar el análisis retrospectivo de IOC. En el modo *Análisis retrospectivo de IOC* de la tarea *Análisis de IOC*, Kaspersky Endpoint Security analiza los indicadores de vulneración mediante el uso de datos durante un período determinado. Este modo está diseñado para buscar indicadores de compromiso según la telemetría del equipo protegido, como la actividad de la red, los procesos, los archivos y otros tipos de telemetría. Si la telemetría extendida está deshabilitada, Kaspersky Endpoint Security puede rotar la información sobre los indicadores de vulneración detectados.
Aislamiento de la red	Aislamiento automático del equipo de la red en respuesta a amenazas detectadas. Cuando el aislamiento de la 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 la 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)	Aislamiento de la red se puede desactivar de forma automática después de un tiempo especificado o manualmente. De forma predeterminada, Kaspersky Endpoint Security desactiva el aislamiento de la red 5 horas después del inicio del aislamiento.
Exclusiones de aislamiento de la red	Lista de reglas para las exclusiones del aislamiento de la red. Las conexiones de red que coinciden con las reglas no se bloquean en los equipos cuando el aislamiento de la red está activado. Para configurar las exclusiones de aislamiento de la red, puede utilizar una lista de *perfiles de la red estándar*. De forma predeterminada, las exclusiones incluyen perfiles de red que contienen reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles del cliente DNS/DHCP. También puede modificar la configuración de los perfiles de la red estándar o definir las exclusiones manualmente. Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de la 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 la 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 los archivos ejecutables y scripts y la apertura de archivos en formato de Office. Por ejemplo, puede evitar la ejecución de aplicaciones que se consideran inseguras en el equipo seleccionado. La prevención de la ejecución es compatible con un conjunto de extensiones de archivos de Office y un conjunto de intérpretes de script. Para usar el componente Prevención de ejecución, debe agregar reglas de prevención de ejecución. La opción *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 los algoritmos hash MD5 y SHA256.
Acción ante operaciones de ejecución o apertura de un objeto prohibido	**Bloquear y agregar al 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 de Kaspersky Security Center. **Agregar a registros 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	La opción *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 los algoritmos hash MD5 y SHA256.

Parámetro	Descripción
Cloud Sandbox	*Cloud Sandbox* es una tecnología que le permite detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Cloud Sandbox para su análisis. Cloud Sandbox ejecuta estos archivos en un entorno aislado para identificar actividades maliciosas y decide sobre su reputación. Luego, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Cloud Sandbox detectó un archivo malicioso, Kaspersky Endpoint Security realiza la acción adecuada para eliminar esta amenaza en todos los equipos donde se detecte este archivo. La tecnología Cloud Sandbox está habilitada de forma permanente y está disponible para todos los usuarios de Kaspersky Security Network, independientemente del tipo de licencia que utilicen. Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security activará el contador de amenazas detectadas mediante Cloud Sandbox en la ventana principal de la aplicación, en **Tecnologías de detección de amenazas**. Kaspersky Endpoint Security también indicará la tecnología de detección de amenazas Cloud Sandbox en los eventos de la aplicación y en *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 la solución de Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* es una solución de ciberseguridad para empresas que incluye las aplicaciones de Kaspersky que le permiten a una organización defenderse contra la mayoría de los tipos de riesgos de ciberseguridad y cubrir los escenarios de propagación de amenazas más importantes. Los componentes de EDR Expert (on-premises) se implementan en Open Single Management Platform (OSMP). Esta plataforma ejecuta escenarios de múltiples plataformas en una única interfaz y permite integrar aplicaciones de Kaspersky con aplicaciones de terceros en un sistema integral de seguridad.

Uno de los elementos principales de la solución es *SIEM*. SIEM supervisa eventos provenientes de todos los componentes y los correlaciona entre sí mediante reglas que definen el proveedor y el usuario. EDR Expert (on-premises) analiza la telemetría y los registros recibidos de la infraestructura corporativa para detectar ataques de forma automática y permite investigar incidentes mediante un gráfico de investigación unificado que combina todos los eventos recopilados en EDR Expert (on-premises), incluidos los eventos de las aplicaciones de Kaspersky y de productos de seguridad de terceros.

Para responder ante incidentes avanzados, EDR Expert (on-premises) utiliza escenarios predefinidos y definidos por el usuario. También puede aplicar acciones de respuesta de aplicaciones de terceros y escenarios de respuesta que implican múltiples aplicaciones.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security para Windows admite 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 que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. 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 adquirir todas las unidades funcionales o las unidades funcionales individuales por separado. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

La aplicación Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y monitorea de forma continua los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos del 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. Luego, el agente incorporado se administra mediante la consola de Kaspersky Anti Targeted Attack Platform, incluidas las tareas en ejecución, 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 recopilación de telemetría	Un *servidor de recopilación de telemetría* es un servidor que forma parte de una solución SIEM y que recopila, normaliza, correlaciona, analiza y almacena información sobre los eventos que ocurren en el equipo. Configure los siguientes parámetros para conectarse a los servidores de colección de telemetría (KUMA): • **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en Open Single Management Platform (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 habilitarla en la configuración del servidor y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Después de configurar el servidor, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña. El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Dirección y **Puerto** (servidores de colección de telemetría)	Configuración para conectarse a servidores de recopilación de telemetría. Puede ingresar una dirección IP (IPv4 o IPv6). Puede agregar varias direcciones de servidores de colección de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 recolección de telemetría	Esta funcionalidad le permite desactivar por completo el envío de telemetría al servidor de KATA. Por ejemplo, si está usando Kaspersky Anti Targeted Attack Platform junto con otra solución que también usa telemetría, puede desactivar el envío de telemetría para KATA (EDR). Esto le permite optimizar la carga del servidor para estas soluciones. Si tiene implementada la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Respuesta ante amenazas en KATA (EDR). • **Enviar telemetría solo con IOA**. Esto permite optimizar la telemetría y enviar solo telemetría con IOA. El *indicador de ataque (IOA)* es una regla que contiene una descripción de comportamiento sospechoso en el sistema que podría señalar un ataque dirigido. La aplicación compara el comportamiento regular en el sistema con estas reglas y registros de eventos que son indicativos de un ataque dirigido. La aplicación usa la tecnología de *análisis de transmisión*, que permite dar seguimiento a estos eventos en tiempo real. • **Retraso máximo de transmisión de eventos (s)**. La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos. • **Limitar la cantidad de paquetes de eventos por transmisión**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. La configuración predeterminada es de 1024 eventos. Esta función permite deshabilitar el almacenamiento en búfer de eventos previo a la sincronización con el servidor.
Habilitar regulación de solicitudes	Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. Configure la telemetría: • **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada 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 las tareas y la configuración de la aplicación modificada.

Parámetro	Descripción
Conexión a servidores de respuesta	Un *servidor de respuesta* es un servidor que recibe y analiza datos, estudia el comportamiento de los objetos y publica los resultados de dichos estudios. Configure los siguientes parámetros para la conexión a los servidores de respuesta: • **Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor. Puede obtener un certificado TLS en Open Single Management Platform (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 habilitarla en la configuración del servidor y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un criptocontenedor en Open Single Management Platform (consulte las instrucciones en la Ayuda de Kaspersky Endpoint Detection and Response Expert (on-premises)). Después de configurar el servidor, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña.
Dirección y **Puerto** (servidores de respuesta)	Configuración para conectarse a servidores de respuesta. Puede ingresar una dirección IP (IPv4 o IPv6). Puede agregar varias direcciones de servidores de colección de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 las tareas y la configuración de la aplicación modificada.
Conexión a servidores KATA	Configure los siguientes parámetros para la conexión al servidor de Central Node: • **Tiempo de espera (s)**. 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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Dirección y **Puerto** (servidores de KATA)	Configuración para conectarse a servidores de Kaspersky Anti Targeted Attack Platform. Ingrese la dirección IP (IPv4 o IPv6) y el puerto del servidor de Central Node para conectarse. Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 de KATA. Por ejemplo, si está usando Kaspersky Anti Targeted Attack Platform junto con otra solución que también usa telemetría, puede desactivar el envío de telemetría para KATA (EDR). Esto le permite optimizar la carga del servidor para estas soluciones. Si tiene implementada la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Respuesta ante amenazas en KATA (EDR). Configure la telemetría: • **Retraso máximo de transmisión de eventos (s)**. La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos. • **Cantidad máxima de paquetes de eventos**. La aplicación se sincroniza con el servidor cuando el búfer se llena de eventos. La configuración predeterminada es de 1024 eventos.

Parámetro	Descripción
Habilitar regulación de solicitudes	Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. Configure la telemetría: • **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada es 15 %.

Network Detection and Response (KATA)

Kaspersky Endpoint Security para Windows admite 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 que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. 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 adquirir todas las unidades funcionales o las unidades funcionales individuales por separado. Para obtener más información sobre la solución, consulte la Ayuda de Kaspersky Anti Targeted Attack Platform.

La aplicación Kaspersky Endpoint Security se instala en equipos individuales en la infraestructura de TI corporativa y monitorea de forma continua los procesos, las conexiones de red abiertas y los archivos que se modifican. La información sobre los eventos del 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. Luego, el agente incorporado se administra mediante la consola de Kaspersky Anti Targeted Attack Platform, incluidas las tareas en ejecución, la administración de objetos en cuarentena, la visualización de informes y otras acciones.

Parámetro	Descripción
Configuración de conexión del servidor	**Tiempo de espera (s)**. 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). **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 habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un *contenedor criptográfico* es un archivo de almacenamiento 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). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.
Dirección y **Puerto**	Configuración para conectarse a servidores de Kaspersky Anti Targeted Attack Platform. Ingrese la dirección IP (IPv4 o IPv6) y el puerto del servidor de Central Node para conectarse. Puede agregar varias direcciones de servidor de Nodo central. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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 de NDR cada (min)	Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre las tareas y la configuración de la aplicación modificada.
Retraso máximo de transmisión de eventos (s)	La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos.
Habilitar regulación de solicitudes	Esta función permite optimizar la carga en el servidor. Si esta funcionalidad está habilitada, la aplicación restringe la transmisión de eventos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos.
Cantidad máxima de eventos por hora	La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia 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 de eventos	La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande. La configuración predeterminada es 15 %.

Integración con KUMA

Kaspersky Endpoint Security para Windows es compatible con la solución Kaspersky Unified Monitoring and Analysis Platform. La solución *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* administra eventos e información de seguridad (SIEM) en la infraestructura informática de las organizaciones. KUMA permite detectar, analizar y mitigar las amenazas de seguridad antes de que puedan hacer daño.

Parámetro	Descripción
Retraso máximo al enviar eventos (s)	La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización. La configuración predeterminada es de 30 segundos.
Conexión a servidores KUMA	**Tiempo de espera (s)**. Tiempo de espera máximo de respuesta del servidor de KUMA. 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 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 modo TLS **With verification** (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 Kaspersky Endpoint Security y KUMA. Para usar la autenticación bidireccional, en la consola de KUMA, en la configuración del conector TCP, debe seleccionar el modo TLS **Custom PFX** (consulte la configuración del conector de tipo TCP en la Ayuda de Kaspersky Unified Monitoring and Analysis Platform). Luego, debe obtener un contenedor criptográfico y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Después de configurar los ajustes de KUMA, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe tener protección 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 ingresar una dirección IP (IPv4 o IPv6). Puede agregar varias direcciones de servidores de KUMA. Kaspersky Endpoint Security intenta conectarse al servidor utilizando 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

El Cifrado de disco de Kaspersky no es compatible con equipos basados en Arm.

Una vez cifrados los discos duros del sistema, la próxima vez que se inicie el equipo, el usuario deberá superar la autenticación por medio del Agente de autenticación para poder acceder a los discos duros y cargar el sistema operativo. El usuario puede autenticarse de dos maneras: puede escribir la contraseña de un token o de una tarjeta inteligente que conecte al equipo, o puede introducir el nombre de usuario y la contraseña de la cuenta del Agente de autenticación que el administrador de la red de área local haya creado con la tarea de *Administrar cuentas del Agente de autenticación*. Estas cuentas se basan en las cuentas de Microsoft Windows con las que el usuario inicia sesión en el sistema operativo. También existe la posibilidad de usar la tecnología Single Sign-On (SSO), que le permite iniciar sesión en el sistema operativo automáticamente con el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

La autenticación de usuarios en el Agente de autenticación se puede realizar de dos formas:

- Ingrese el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red LAN que está utilizando las herramientas de Kaspersky Security Center.
- Ingrese la contraseña de un token o tarjeta inteligente conectados al equipo.

> El uso de un token o de una tarjeta inteligente está disponible solo si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, se rechazará la adición del archivo de certificado electrónico al comando.

Cifrado de Unidad BitLocker

BitLocker es una tecnología de cifrado que forma parte de los sistemas operativos Windows. Kaspersky Endpoint Security le permite controlar y administrar BitLocker a través de la infraestructura de Kaspersky Next. La tecnología BitLocker está diseñada para cifrar volúmenes lógicos. No puede utilizarse para cifrar unidades extraíbles. Para más información sobre BitLocker, puede consultar la documentación de Microsoft.

> Al cifrar el disco, BitLocker coloca el cargador de arranque y otros archivos auxiliares en system partition. Esta partición no está cifrada. El sistema operativo crea la partición del sistema automáticamente durante la instalación de Windows. Si todo el disco está particionado antes de instalar Windows, el sistema operativo no podrá crear una partición del sistema. En este caso, cuando inicie el cifrado de disco BitLocker, el sistema operativo le pide al usuario 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 BitLocker.

Las claves de acceso de BitLocker pueden almacenarse de manera segura utilizando un TPM (módulo de plataforma segura). Un *Trusted Platform Module (TPM)* es un microchip que proporciona funciones de seguridad básicas (entre ellas, la capacidad de almacenar claves de cifrado). Por lo general, el TPM forma parte de la placa madre del equipo e interactúa con los demás componentes del sistema a través de un bus físico. Es la opción más segura para almacenar las claves de acceso de BitLocker porque permite verificar la integridad del sistema antes del arranque. La ausencia de un TPM no es impedimento para cifrar las unidades de un equipo. En tal caso, se utiliza una contraseña para cifrar la clave de acceso. BitLocker permite emplear los siguientes métodos de autenticación:

- TPM.
- PIN y TPM.
- Contraseña.

Cuando la unidad del sistema está cifrada, el usuario debe superar la autenticación de BitLocker para iniciar el sistema operativo. Después de la autenticación, BitLocker permite que el usuario inicie sesión. BitLocker no es compatible con la tecnología de inicio de sesión único (SSO).

Cuando se cifra una unidad, BitLocker crea una clave de recuperación. Kaspersky Endpoint Security envía la clave de recuperación a Kaspersky Security Center; ello le permitirá restaurar el acceso al disco si, por ejemplo, un usuario olvida su contraseña.

Si un usuario cifra un disco con BitLocker, Kaspersky Endpoint Security enviará la clave de recuperación y la información sobre el cifrado de disco a Kaspersky Security Center.

Si utiliza directivas de grupo de Windows, deshabilite el control de BitLocker en las mismas. Las directivas de Windows pueden interferir con las de Kaspersky Security Center. Tales interferencias pueden derivar en errores de cifrado.

Parámetros del componente Cifrado de disco de Kaspersky

Parámetro	Descripción
Modo de cifrado	**Cifrar todos los discos duros**. Si se selecciona esta opción, cuando se aplique la directiva, la aplicación cifrará todos los discos duros. Si el equipo tiene varios sistemas operativos instalados, después del cifrado podrá solo cargar el sistema operativo que tenga la aplicación instalada. **Descifrar todos los discos duros**. Si se selecciona esta opción, cuando se aplique la directiva, la aplicación descifrará todos los discos duros que se encuentren cifrados. **Dejar sin modificar**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación no modificará el estado de las unidades. Si la unidad se cifra, permanece cifrada. Si la unidad se descifra, permanece descifrada. Este elemento está seleccionado por defecto.
Durante el cifrado, crear automáticamente cuentas de Agente de autenticación para los usuarios de Windows	Cuando esta casilla está activada, la aplicación crea cuentas del Agente de autenticación para las cuentas de usuario de Windows disponibles en el equipo. De manera predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario haya iniciado sesión en el sistema operativo en los treinta días anteriores.
Configuración de la creación de cuentas del Agente de autenticación	**Todas las cuentas del equipo**. Todas las cuentas del equipo que estuvieron activas en cualquier momento. **Todas las cuentas de dominio del equipo**. Todas las cuentas del equipo que pertenecen a algún dominio y que estuvieron activas en algún momento. **Todas las cuentas locales del equipo**. Todas las cuentas locales del equipo que estuvieron activas en cualquier momento. **Cuenta del servicio con una contraseña de un solo uso**. La cuenta del servicio es necesaria para acceder al equipo (por ejemplo, cuando el usuario olvida la contraseña). También puede utilizar la cuenta del servicio como cuenta de reserva. Debe ingresar el nombre de la cuenta (de manera predeterminada, `ServiceAccount`). Kaspersky Endpoint Security crea una contraseña automáticamente. Puede encontrarla 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. De manera predeterminada, el rol de administrador del equipo no está definido (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 de Agente de autenticación para todos los usuarios de este equipo al iniciar sesión	Si activa esta casilla de verificación, la aplicación analizará las cuentas de Windows disponibles en el equipo antes de que se inicie el Agente de autenticación. Si detecta que una cuenta de Windows no tiene su correspondiente cuenta para el Agente de autenticación, crea esa cuenta para que el usuario pueda acceder a las unidades cifradas de su equipo. La nueva cuenta del Agente de autenticación tendrá las siguientes opciones por defecto: inicio de sesión con contraseña únicamente y cambio de contraseña obligatorio tras el primer inicio de sesión. Gracias a esta función, ya no necesitará agregar cuentas del Agente de autenticación manualmente con la tarea *Administrar cuentas del Agente de autenticación* para los equipos que ya tengan sus unidades cifradas.
Guardar el nombre de usuario utilizado 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 que ingrese el nombre de la cuenta la próxima vez que intente completar la autorización en el Agente de Autenticación bajo la misma cuenta.

Parámetro	Descripción
Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)	Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado. Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado. Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se agregan. Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente. Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De manera predeterminada, la casilla está desactivada.
Usar Legacy USB Support (no recomendado)	Esta casilla habilita/deshabilita la funcionalidad Legacy USB Support. *Legacy USB Support* es una función de la BIOS o UEFI que permite utilizar dispositivos USB (por ejemplo, tokens de seguridad) durante el arranque del equipo, en la etapa anterior al inicio del sistema operativo (modo BIOS). La funcionalidad Legacy USB Support no afecta la capacidad de usar dispositivos USB después de iniciar el sistema operativo. Si la casilla se selecciona, la compatibilidad con dispositivos USB durante el primer inicio del equipo se habilitará. Si habilita la función Legacy USB Support y el Agente de autenticación se instaló en modo BIOS, no podrá usar tokens USB. Se recomienda usar esta opción solo cuando hay un problema de compatibilidad del hardware y solo para esos equipos en los cuales el problema ocurrió.
Configuración de contraseñas	Parámetros relativos a los requisitos de seguridad con los que deben cumplir las contraseñas de las cuentas del Agente de autenticación. Si opta por usar la tecnología SSO, el Agente de autenticación no tendrá en cuenta los requisitos que puedan haberse definido en Kaspersky Security Center para controlar la seguridad de las contraseñas. Para controlar la seguridad de las contraseñas, utilice las opciones del sistema operativo.
Usar tecnología de inicio de sesión único (SSO)	La tecnología SSO hace posible usar las mismas credenciales de cuenta para acceder a discos duros cifrados e iniciar sesión en el sistema operativo. Si activa la casilla, será necesario introducir las credenciales de cuenta para acceder a los discos duros cifrados, pero el inicio de sesión en el sistema operativo se realizará automáticamente. 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.
Cifrar proveedores de credenciales de terceros	Kaspersky Endpoint Security es compatible con el proveedor de credenciales de terceros ADSelfService Plus. Cuando se trabaja con proveedores de credenciales de terceros, el Agente de autenticación intercepta la contraseña antes de que se inicie el sistema operativo. Esto significa que un usuario debe ingresar una contraseña solo una vez al iniciar sesión en Windows. Después de iniciar sesión en Windows, el usuario puede utilizar las capacidades de un proveedor de credenciales de terceros para, por ejemplo, autenticar servicios corporativos. Los proveedores de credenciales de terceros también permiten a los usuarios restablecer su propia contraseña de forma independiente. En este caso, Kaspersky Endpoint Security actualizará automáticamente la contraseña del 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 el funcionamiento de la tecnología de inicio de sesión único.
Ayuda	**Autenticación**. Texto que se muestra en la ventana del Agente de autenticación al momento de introducir las credenciales de cuenta. **Cambiar contraseña**. Texto que se muestra en la ventana del Agente de autenticación cuando se intenta cambiar la contraseña de la cuenta del Agente de autenticación. **Recuperar contraseña**. Texto que se muestra en la ventana del Agente de autenticación cuando se intenta 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, cuando se aplique la directiva, la aplicación cifrará todos los discos duros. Si el equipo tiene varios sistemas operativos instalados, después del cifrado podrá solo cargar el sistema operativo que tenga la aplicación instalada. **Descifrar todos los discos duros**. Si se selecciona esta opción, cuando se aplique la directiva, la aplicación descifrará todos los discos duros que se encuentren cifrados. **Dejar sin modificar**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación no modificará el estado de las unidades. Si la unidad se cifra, permanece cifrada. Si la unidad se descifra, permanece descifrada. Este elemento está seleccionado por defecto.
Habilitar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en tabletas	Usar la autenticación que requiere el ingreso de datos en un entorno previo al inicio del sistema, aun si la plataforma no tiene la capacidad de ingreso previo al inicio del sistema (por ejemplo, con teclados de pantalla táctil en tabletas). La pantalla táctil de las tabletas no está disponible en el entorno previo al inicio. Para completar la autenticación de BitLocker en tabletas, el usuario debe, por ejemplo, conectar un teclado USB. Si se selecciona la casilla de verificación, se permite el uso de la autenticación que requiere ingreso previo al inicio del sistema. Se recomienda usar esta configuración solo para dispositivos que tienen herramientas alternativas de ingreso de datos en un entorno previo al inicio del sistema, como ser, un teclado USB además de teclados de pantalla táctil. Para poder usar la tecnología Cifrado de unidad BitLocker en una tableta, esta casilla debe estar activada.
Usar cifrado de hardware (Windows 8 y versiones posteriores)	Si se selecciona la casilla de verificación, la aplicación implementa cifrado del hardware. Esto le permite aumentar la velocidad de cifrado y usar menos recursos del equipo.
Cifrar solo el espacio de disco usado (Windows 8 y versiones posteriores)	Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado. Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado. Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se agregan. Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente. Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables. De manera predeterminada, la casilla está desactivada.

Parámetro	Descripción
Método de autenticación	**Solo contraseña (Windows 8 y versiones posteriores)** Si se selecciona esta opción, Kaspersky Endpoint Security le solicita al usuario una contraseña cuando intenta acceder a una unidad cifrada. Esta opción se puede seleccionar cuando no se está utilizando un Módulo de plataforma segura (TPM). **Módulo de plataforma segura (TPM)** Si se selecciona esta opción, BitLocker usa un Módulo de plataforma segura (TPM). Un *Trusted Platform Module (TPM)* es un microchip que proporciona funciones de seguridad básicas (entre ellas, la capacidad de almacenar claves de cifrado). Suele haber un Módulo de plataforma segura instalado en la placa madre del equipo y este módulo interactúa con todos los demás 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 se pueden descifrar con el dispositivo. Un Módulo de plataforma segura cifra claves de cifrado con su propia clave de almacenamiento raíz. La clave de almacenamiento raíz se almacena dentro del Módulo de plataforma segura. Esto proporciona un nivel adicional de protección contra intentos de ataque a 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: • **Usar PIN para TPM**. Si activa esta casilla, los usuarios podrán usar un código PIN para obtener acceso a una clave de cifrado almacenada en un módulo de plataforma segura (TPM). Si desactiva esta casilla, los usuarios no podrán usar un código PIN. Para acceder a la clave de cifrado, deberán utilizar una contraseña. • **Módulo de plataforma segura (TPM), o contraseña si el TPM no se encuentra disponible**. Si se selecciona esta opción, el usuario puede usar una contraseña para obtener acceso a claves de cifrado cuando un módulo de plataforma segura (TPM) no está disponible. Si desactiva esta casilla y no hay un módulo TPM disponible, la función de cifrado de disco completo no se iniciará. El método de autenticación seleccionado debe configurarse mediante la especificación de requisitos de contraseña o PIN: • **Longitud mínima de PIN (caracteres)**. • **Longitud mínima de la contraseña (caracteres)**. • **Limitar el periodo de validez de la contraseña o del PIN para el TPM (días)**. • **Usar un PIN mejorado (letras y números)**. El *código PIN mejorado* permite usar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.
Recrear automáticamente clave de recuperación (días)	Actualice automáticamente la contraseña para restaurar el acceso a una unidad protegida con BitLocker. Si se selecciona la casilla de verificación, especifique el período de validez de la contraseña con clave de recuperación. Esto ayuda a prevenir la reutilización de la contraseña con clave de recuperación.

Cifrado de archivos

El cifrado de archivos no es compatible con equipos basados en Arm.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

Puede compilar listas de archivos por extensión o grupo de extensiones y listas de carpetas almacenadas en discos locales del equipo, además de crear reglas para cifrar archivos que son creados por aplicaciones específicas. Luego de que se aplique una directiva, Kaspersky Endpoint Security cifrará y descifrará los siguientes archivos:

- archivos agregados individualmente a listas para cifrado y descifrado;
- archivos almacenados en carpetas agregadas a listas para cifrado y descifrado;
- Archivos creados por aplicaciones por separado.

La característica de cifrado de archivos está sujeta a las siguientes consideraciones especiales:

- Kaspersky Endpoint Security cifrará o descifrará archivos en las carpetas predefinidas únicamente para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifrará ni descifrará ningún archivo que se encuentre en una carpeta redirigida o en las carpetas predefinidas de un perfil de usuario móvil, un perfil de usuario obligatorio o un perfil de usuario temporal.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo y las aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas están en la lista de exclusiones de cifrado:
  - %WINDIR%
  - %PROGRAMFILES% y %PROGRAMFILES(X86)%
  - Archivos de registro de Windows.

  No es posible ver ni modificar la lista de exclusiones de cifrado. Aunque los archivos y carpetas de esta lista pueden agregarse a la lista de cifrado, la característica de cifrado de archivos nunca cifrará esos objetos.

Parámetros del componente Cifrado de archivos

Parámetro	Descripción
Modo de cifrado	**Dejar sin modificar**. Si se selecciona este elemento, Kaspersky Endpoint Security no modifica los archivos y carpetas y no los cifra ni descifra. **Según las reglas**. Si se selecciona este elemento, Kaspersky Endpoint Security cifra los archivos y las carpetas siguiendo las reglas de cifrado, descifra los archivos y las carpetas siguiendo las reglas de descifrado, y regula el acceso de las aplicaciones a los archivos cifrados siguiendo las reglas creadas para las aplicaciones. **Descifrar todo**. Si se selecciona este elemento, Kaspersky Endpoint Security descifra todos los archivos y carpetas cifrados.

Parámetro	Descripción
Cifrado	Esta ficha muestra las reglas de cifrado para los archivos almacenados en discos locales. Las opciones para agregar archivos son las siguientes: • **Carpetas predefinidas**. Kaspersky Endpoint Security permite agregar las siguientes áreas: **Documentos**. Archivos que se encuentren en la carpeta *Documentos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas. **Favoritos**. Archivos que se encuentren en la carpeta *Favoritos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas. **Escritorio**. Archivos que se encuentren en la carpeta *Escritorio* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas. **Archivos temporales**. Archivos temporales vinculados al funcionamiento de las aplicaciones instaladas en el equipo. Aquí se incluyen, por ejemplo, las copias de seguridad temporales que se crean al trabajar con documentos en las aplicaciones de Microsoft Office. **Archivos de Outlook**. Archivos vinculados al funcionamiento del cliente de correo electrónico Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de las libretas de direcciones sin conexión (OAB) y archivos de las libretas de direcciones personales (PAB). • **Carpeta personalizada**. Puede escribir la ruta de acceso a una carpeta. Cuando agregue una ruta de carpeta, siga estas reglas: Utilice una variable de entorno (por ejemplo, `%FOLDER%\UserFolder\`). Puede usar una sola variable de entorno por ruta, y únicamente al comienzo de la ruta. No utilice rutas relativas. No utilice los caracteres `*` y `?`. No utilice rutas UNC. Utilice los caracteres `;` o `,` como separadores. • **Archivos por extensión**. La lista contiene algunos grupos de extensiones que puede seleccionar (por ejemplo, el grupo *Archivos de almacenamiento*). También puede agregar extensiones de archivo manualmente.
Descifrado	Esta ficha muestra reglas de descifrado para los archivos almacenados en discos locales.
Reglas para aplicaciones	La ficha muestra una tabla que contiene reglas de acceso a archivos cifrados para aplicaciones y reglas de cifrado para archivos que se crean o modifican por aplicaciones particulares.
Paquetes cifrados	Requisitos de seguridad con los que deberá cumplir la contraseña que se defina al momento de crear un paquete cifrado.

Cifrado de unidades extraíbles

El cifrado de unidades extraíbles no es compatible con equipos basados en Arm.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha 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 se conecta una unidad extraíble con un sistema de archivos no compatible 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 la información almacenada en una unidad extraíble, puede usar los siguientes tipos de cifrado:

- Full Disk Encryption (FDE).

  Cifrado de la unidad extraíble completa, incluido su sistema de archivos.

  Tenga en cuenta que no se podrá acceder a la información cifrada fuera de la red corporativa. Aun dentro de la red corporativa, tampoco será posible acceder a esta información si el equipo no está conectado a Kaspersky Security Center (es decir, si se utiliza un equipo invitado).

- File Level Encryption (FLE).

  Cifrado únicamente de los archivos almacenados en la unidad extraíble. El sistema de archivos no se modifica.

> Si cifra los archivos de una unidad extraíble, podrá utilizar un modo especial —llamado *modo portátil*— para acceder a la información fuera de la red corporativa.

Kaspersky Endpoint Security crea una clave maestra como parte del proceso de cifrado. La clave maestra se guarda en los siguientes repositorios:

- Kaspersky Security Center
- El equipo del usuario

  La clave maestra se cifra con la clave secreta del usuario.
- Unidad extraíble

  La clave maestra se cifra con la clave pública de Kaspersky Security Center.

Una vez que haya cifrado una unidad extraíble, mientras se encuentre dentro de la red corporativa, podrá acceder a sus datos como si estuviera utilizando una unidad convencional sin cifrado.

Acceso a datos cifrados

Cuando se conecta una unidad extraíble con información cifrada, Kaspersky Endpoint Security hace lo siguiente:

1. Busca una clave maestra en el repositorio local del equipo del usuario.

   Si encuentra la clave maestra pertinente, el usuario puede acceder a la información de la unidad extraíble.

   Si no encuentra la clave maestra, Kaspersky Endpoint Security hace lo siguiente:

   a. Envía una solicitud a Kaspersky Security Center.

      Tras recibir la solicitud, Kaspersky Security Center envía una respuesta con la clave maestra.

   b. Kaspersky Endpoint Security guarda la clave maestra en el repositorio local del equipo para poder operar con la unidad extraíble cifrada.
2. Descifra la información.

Consideraciones especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles está sujeto a las siguientes consideraciones especiales:

- La directiva con los ajustes preestablecidos para el cifrado de unidades extraíbles se crea para un grupo específico de equipos administrados. Por lo tanto, el resultado de la aplicación de la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al cual está conectada la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra los archivos de solo lectura que puedan encontrarse en las unidades extraíbles.

- Los siguientes tipos de dispositivo se admiten como unidad extraíble:
  - Medios de datos conectados por medio de un bus USB
  - Discos duros conectados por medio de buses USB y FireWire
  - Unidades SSD conectadas por medio de buses USB y FireWire

Parámetros del componente Cifrado de unidades extraíbles

Parámetro	Descripción
Modo de cifrado	**Cifrar la unidad extraíble completa**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará las unidades extraíbles sector por sector, incluyendo sus sistemas de archivos. **Cifrar todos los archivos**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará todos los archivos almacenados en las unidades extraíbles. Kaspersky Endpoint Security no volverá a cifrar los archivos que ya estén cifrados. Tampoco cifrará el contenido del sistema de archivos de las unidades extraíbles, por lo que los nombres de los archivos cifrados, la estructura de carpetas, etc., seguirán siendo visibles. **Solo cifrar archivos nuevos**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security únicamente cifrará los archivos que se hayan creado o modificado en las unidades extraíbles desde la última aplicación de la directiva de Kaspersky Security Center. Este modo de cifrado es conveniente cuando se usa un disco extraíble para fines personales y laborales. Este modo de cifrado le permite dejar todos los archivos intactos y cifrar solo los archivos que el usuario crea en un equipo de trabajo que tiene instalado Kaspersky Endpoint Security y habilitada la función de cifrado. De este modo, siempre se puede acceder a archivos personales, independientemente de si Kaspersky Endpoint Security se instala en el equipo con la función de cifrado habilitada. **Descifrar la unidad extraíble completa**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security descifrará todos los archivos de las unidades extraíbles y, si estuvieran cifrados, también sus sistemas de archivos. **Dejar sin modificar**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación no modificará el estado de las unidades. Si la unidad se cifra, permanece cifrada. Si la unidad se descifra, permanece descifrada. Este elemento está seleccionado por defecto.
Modo portátil	La casilla habilita o deshabilita una opción que permite preparar una unidad extraíble de manera tal que sus archivos puedan manipularse en equipos que no estén conectados a la red corporativa. Si activa esta casilla, cuando se aplique la directiva, Kaspersky Endpoint Security le pedirá al usuario que especifique una contraseña antes de cifrar los archivos de la unidad extraíble. La contraseña dará acceso a los archivos cifrados de la unidad cuando se la conecte a un equipo que no se encuentre en la red corporativa. Puede configurar los requisitos de seguridad con los que deberá cumplir esta contraseña. El modo portátil estará disponible únicamente si ha seleccionado los modos **Cifrar todos los archivos** o **Solo cifrar archivos nuevos**.
Solo cifrar el espacio de disco usado	Esta casilla de verificación habilita / deshabilita el modo de cifrado en el cual se cifran solo los sectores de disco ocupados. Este modo se recomienda para unidades nuevas cuyos datos no se han modificado o eliminado. Si se selecciona la casilla de verificación, solo se cifran partes de la unidad que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se agregan. Si se desactiva la casilla de verificación, se cifra la unidad completa, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente. La posibilidad de cifrar solo el espacio de disco usado está disponible únicamente para el modo **Cifrar la unidad extraíble completa**. Activar o desactivar la casilla **Solo cifrar el espacio de disco usado** una vez que se ha iniciado el proceso de cifrado no tiene ningún efecto. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado.

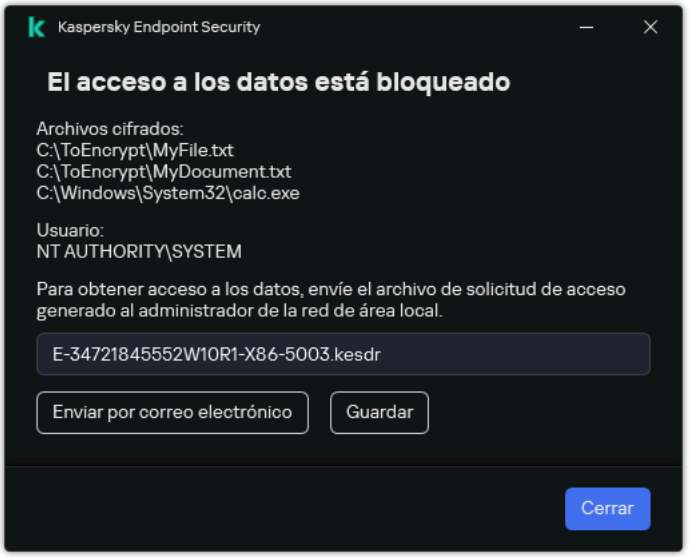
Parámetro	Descripción

Reglas personalizadas	Esta tabla contiene dispositivos para los cuales se definen reglas de cifrado personalizadas. Si desea crear una regla de cifrado para una unidad extraíble específica, tiene las siguientes opciones:
	• Agregar una unidad extraíble que exista en la lista de dispositivos de confianza de Control de dispositivos.
	• Agregar una unidad extraíble en forma manual:
	  • Por ID de dispositivo (Hardware ID, o HWID)
	  • Por modelo de dispositivo: Vendor ID (VID) y Product ID (PID)

Permitir cifrado de unidades extraíbles en el modo sin conexión	Si se selecciona esta casilla, Kaspersky Endpoint Security cifra unidades extraíbles incluso cuando no hay conexión con Kaspersky Security Center. En este caso, los datos requeridos para descifrar las unidades extraíbles se almacenan en el disco duro del equipo al cual la unidad extraíble se conecta y no se transmite a Kaspersky Security Center. Si se desmarca esta casilla, Kaspersky Endpoint Security no cifra unidades extraíbles sin una conexión con Kaspersky Security Center.
Configuración de contraseña de cifrado/Administrador de archivos portátil	Requisitos de seguridad para la contraseña del Administrador de archivos portátil.

Plantillas (cifrado de datos)

Kaspersky Endpoint Security puede restringir el acceso a los datos que se hayan cifrado en el pasado debido a, por ejemplo, un cambio en la infraestructura de la organización y un cambio en el Servidor de administración de Kaspersky Security Center. Si un usuario descubre que no puede acceder a los datos cifrados que necesita, puede pedirle acceso al administrador. Para ello, debe enviarle al administrador un archivo de solicitud de acceso. El administrador, por su parte, le enviará al usuario un archivo de respuesta, que este deberá cargar en Kaspersky Endpoint Security. La solicitud de acceso para el administrador puede enviarse por correo electrónico (vea la siguiente imagen).



Solicitar acceso a información cifrada

El mensaje con el que se da aviso de la falta de acceso está basado en una plantilla. Si lo desea, puede completar los siguientes campos para que no tenga que hacerlo el usuario:

- **Para**. Escriba la dirección de correo de un grupo de administradores que tenga permitido usar las funciones de cifrado de datos.
- **Asunto**. Escriba el asunto del mensaje que se enviará para solicitar acceso a los archivos cifrados. Puede agregar etiquetas que ayuden a filtrar los mensajes.
- **Mensaje del usuario**. De ser necesario, modifique el contenido del mensaje. Puede utilizar variables para introducir ciertos datos (por ejemplo, la variable `%USER_NAME%`).

Exclusiones

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza independientemente, teniendo en cuenta las características de los objetos manejados y las aplicaciones instaladas en el equipo. Puede ser necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a un objeto o una aplicación determinados, si está seguro de que dicho objeto o aplicación no suponen peligro alguno. 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 agregar telemetría EDR a la zona de confianza. Esto permite optimizar los datos que la aplicación envía al servidor de recopilación de 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 aplicaciones de confianza se agregan a la zona de confianza. Las exclusiones de análisis y aplicaciones de confianza predefinidas 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 el modo de Light Agent para proteger entornos virtuales. Con las exclusiones de análisis y las aplicaciones de confianza predefinidas, puede configurar rápidamente Kaspersky Endpoint Security en los entornos virtuales de Citrix y VMware.

Exclusiones de análisis

Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas. A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre el software legal que los intrusos pueden utilizar para dañar su equipo o datos personales están disponibles en el sitio web de la Enciclopedia TI de Kaspersky.

Kaspersky Endpoint Security puede bloquear estas aplicaciones. Para prevenir que se bloqueen, puede configurar la exclusión del análisis para las aplicaciones en uso. Busque para ello el nombre (o la máscara de nombre) pertinente en la Enciclopedia de Kaspersky y agréguelo a la zona de confianza. Por ejemplo, a menudo utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security considera esta actividad como sospechosa y puede bloquearla. Para evitar que la aplicación se bloquee, cree una exclusión de análisis con el nombre o la máscara de nombre que se indiquen en la Enciclopedia de Kaspersky.

Si una aplicación que recopila información y la envía para su proceso se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis si configura Kaspersky Endpoint Security tal como se describe en este documento.

Las exclusiones de análisis pueden ser utilizadas por los siguientes componentes de las aplicaciones y tareas que configuró el administrador del sistema:

- Detección de comportamiento
- Prevención de exploits
- Prevención de intrusiones en el host
- Protección contra amenazas de archivo
- Protección contra amenazas web
- Protección contra amenazas de correo
- Tarea de *Análisis de malware*

Lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de archivos y de red (incluida la actividad maliciosa) y el acceso al registro del sistema no son supervisados por Kaspersky Endpoint Security. De manera predeterminada, Kaspersky Endpoint Security supervisa las acciones y el tráfico de red de todas las aplicaciones y analiza los objetos que abren, ejecutan o guardan los procesos asociados a las mismas. 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 agrega a las exclusiones, Kaspersky Endpoint Security omitirá este archivo.

Por ejemplo, si considera que los objetos utilizados por la aplicación estándar Bloc de notas de Microsoft Windows son seguros, es decir, que confía en esta aplicación, puede agregar el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza para no supervisar los objetos utilizados por esta aplicación. Esto aumentará el rendimiento del equipo, lo cual es especialmente importante cuando se usan aplicaciones de servidor.

Además, ciertas acciones clasificadas por Kaspersky Endpoint Security como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de una cantidad de aplicaciones. Por ejemplo, la intercepción del texto escrito con el teclado es un proceso de rutina para los conmutadores de disposición del teclado automática (como Punto Switcher). Para tener en cuenta las características de estas aplicaciones y no supervisarlas, se recomienda agregarlas 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 otra aplicación antivirus).

Al mismo tiempo, el archivo ejecutable y los procesos de la aplicación de confianza seguirán siendo analizados en busca de virus y otras clases de malware. Una aplicación se puede excluir completamente del análisis de Kaspersky Endpoint Security mediante Exclusiones de análisis.

Parámetro	Descripción

Tipos de objetos detectados	Independientemente de la configuración de la aplicación ajustada, Kaspersky Endpoint Security siempre detecta y bloquea virus, gusanos y troyanos. Estos pueden ocasionar daños importantes al equipo.

- **Virus y gusanos**

  Subcategoría: Virus y gusanos (Viruses_and_Worms)

  Nivel de peligrosidad: Alto

  Los virus y gusanos tradicionales realizan acciones no autorizadas por el usuario. Pueden crear copias de sí mismos capaces de replicarse.

  Virus habitual

  Cuando un virus tradicional ingresa a un equipo, lo que hace es infectar un archivo, activarse, realizar acciones malintencionadas y agregar copias de sí mismo a otros archivos.

  Los virus tradicionales solo se multiplican en los recursos locales del equipo; no pueden penetrar otros equipos por sí mismos. Solo pueden pasar a otro equipo si agregan una copia de sí mismos a un archivo almacenado en una carpeta compartida o en un CD dentro del equipo, o si el usuario reenvía un mensaje de correo con un archivo adjunto infectado.

  El código de los virus tradicionales puede penetrar diversas áreas 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 scripts* y *virus de macros*.

  Los virus pueden infectar archivos mediante una variedad de técnicas. Los virus de tipo *Overwriting* escriben su código sobre el código del archivo infectado y borran el contenido de este último. El archivo infectado deja de funcionar y no se puede restaurar. Los virus de tipo *Parasitic* modifican archivos y los dejan total o parcialmente funcionales. Los virus de tipo *Companion* no modifican archivos, sino que crean duplicados. Cuando se abre un archivo infectado, se inicia un duplicado de este (que, en realidad, es un virus). También es posible encontrarse con los siguientes tipos de virus: Virus de tipo *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. Los gusanos reciben este nombre debido a su capacidad para "arrastrarse" de un equipo a otro y propagar copias de sí mismos sin el permiso del usuario mediante numerosos canales de datos.

  La principal función que permite diferenciar los distintos tipos de gusanos es la forma de propagarse. La siguiente tabla proporciona un resumen de distintos tipos de gusanos, clasificados según la forma en que se propagan.

  Formas de propagación

Tipo	Name	Descripción
Email-Worm	Email-Worm	Se propagan mediante el correo electrónico. Un mensaje de correo infectado contiene un documento adjunto con una copia de un gusano o un vínculo a un archivo cargado en un sitio web que puede haber sufrido un ataque o haber sido creado exclusivamente con ese fin. Cuando se abre el documento adjunto, se activa el gusano. Cuando se hace clic en el vínculo, se descarga y se abre el archivo, y el gusano empieza a realizar acciones malintencionadas. Después de esto, empieza a distribuir copias de sí mismo. Para ello, busca otras direcciones de correo y les envía mensajes infectados.
IM-Worm	Gusanos de cliente de MI	Se propagan a través de clientes de MI. Por lo general, estos gusanos envían mensajes que incluyen un vínculo a un archivo con una copia del gusano ubicado en un sitio web y utilizan las listas de contactos del usuario. Cuando el usuario descarga el archivo y lo abre, se activa el gusano.
IRC-Worm	Gusanos de chat de Internet	Se propagan mediante Internet Relay Chats, sistemas de servicio que permiten comunicarse con otras personas a través de Internet en tiempo real. Estos gusanos publican un archivo con una copia de sí mismos o un vínculo al archivo en un chat de Internet. Cuando el usuario descarga el archivo y lo abre, se activa el gusano.
Net-Worm	Gusanos de red	Estos gusanos se propagan a través de redes de equipos. A diferencia de otros tipos de gusanos, un gusano de red típico se propaga sin la participación del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red (punto vulnerable) especialmente formado que contiene el código del gusano o una parte de él. Si en la red hay algún equipo "vulnerable", recibe este paquete de red. El gusano se activa una vez que penetra completamente en el equipo.
P2P-Worm	Gusanos de redes de uso compartido de archivos	Se propagan mediante redes punto a punto de uso compartido de archivos. Para infiltrar una red P2P, el gusano se copia en una carpeta de uso compartido de archivos que, por lo general, está situada en el equipo del usuario. La red P2P muestra información sobre este archivo, de modo que el usuario pueda "encontrar" el archivo infectado en la red como a cualquier otro archivo, descargarlo y abrirlo. Gusanos más sofisticados emulan el protocolo de red de una red P2P específica: devuelven respuestas positivas a solicitudes de búsqueda y ofrecen copias de sí mismo para su descarga.
Gusano	Otros tipos de gusanos	Otros tipos de gusanos incluyen los siguientes: • Gusanos que distribuyen copias de sí mismos por los recursos de red. Al utilizar las funciones del sistema operativo, buscan carpetas disponibles de red, se conectan a equipos conectados a Internet e intentan obtener acceso total a sus unidades de disco. A diferencia de los tipos de gusanos descritos anteriormente, otras clases 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 celular a otro).

- **Troyanos y ransomware**

  Subcategoría: Troyanos

  Nivel de peligrosidad: Alto

A diferencia de los gusanos y los virus, los troyanos no se autorreplican. Por ejemplo, penetran un equipo a través del correo o un navegador cuando el usuario visita una página web infectada. Los troyanos requieren la participación del usuario para iniciarse. Comienzan a realizar acciones malintencionadas inmediatamente después de iniciarse.

Los distintos troyanos se comportan de manera diferente en los equipos infectados. Las principales funciones de los troyanos consisten en bloquear, modificar o destruir información y en deshabilitar equipos o redes. Los troyanos también reciben o envían archivos, los ejecutan, muestran mensajes en pantalla, solicitan páginas web, descargan e instalan programas y reinician equipos.

Con frecuencia, los piratas usan "conjuntos" de varios troyanos.

Los tipos de comportamiento de los caballos de troya se describen en la siguiente tabla.

Tipos de comportamiento de caballos de troya en equipos infectados

Tipo	Name	Descripción
Trojan-ArcBomb	Troyanos: "bombas en archivos de almacenamiento"	Cuando se descomprimen, estos archivos de almacenamiento aumentan de tamaño en una medida tal que afecta el funcionamiento del equipo. Cuando el usuario intenta descomprimir un archivo de almacenamiento de esta clase, es posible que el equipo se ralentice o se bloquee, y el disco duro puede llenarse de datos "vacíos". Las "bombas en archivo de almacenamiento" son especialmente peligrosas para los servidores de correo y de archivos. Si el servidor utiliza un sistema automático para procesar la información entrante, una "bomba en archivo de almacenamiento" puede detener el servidor.
Puerta trasera	Troyanos de administración remota	Se considera que son los troyanos más peligrosos. Funcionan de manera bastante similar a las aplicaciones de administración remota instaladas en los equipos. Estos programas se instalan en el equipo sin que el usuario los detecte, lo que permite al intruso administrarlo de forma remota.
Troyano	Troyanos	En esta categoría se incluyen las siguientes aplicaciones maliciosas: • **Troyanos tradicionales**. Estos programas solo realizan las funciones principales de los troyanos: bloquear, modificar o destruir información y deshabilitar equipos o redes. A diferencia de los otros tipos de troyano descritos en la tabla, estos no tienen funciones avanzadas. • **Troyanos versátiles**. Estos programas tienen funciones avanzadas típicas de diversos tipos de troyanos.
Trojan-Ransom	Ransom troyanos	Toman la información del usuario como "rehén", modificándola o bloqueándola, o afectan el funcionamiento del equipo, de modo que el usuario pierde la capacidad de utilizar la información. El intruso le exige al usuario un rescate a cambio de una aplicación que permita restaurar la información y la operatividad del equipo.
Trojan-Clicker	Trojan-Clicker	Acceden a páginas web desde el equipo del usuario, ya sea mediante el envío de comandos a un navegador por su cuenta o por medio de la modificación de las direcciones web especificadas en los archivos del sistema operativo. Al utilizar estos programas, los intrusos realizan ataques de red e incrementan las visitas a sitios web, lo que aumenta la cantidad de anuncios publicitarios que se muestran.
Trojan-Downloader	Descargadores troyanos	Acceden a la página web del intruso para descargar de allí otra aplicación malintencionada e instalarla en el equipo del usuario. El nombre del archivo que se debe descargar puede venir establecido de antemano dentro del troyano o puede determinarse al acceder a la página del atacante.
Trojan-Dropper	Caballos de troya instaladores de software malintencionado	Contienen otros troyanos que descargan en el disco duro y luego instalan. Los intrusos pueden utilizar programas de este tipo para cumplir los siguientes objetivos: • Instalar una aplicación malintencionada sin que el usuario lo advierta: Los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (por ejemplo, pueden advertir sobre la existencia de un archivo dañado o sobre incompatibilidades en el sistema operativo). • Impedir la detección de una aplicación malintencionada conocida. No todos los antivirus son capaces de detectar aplicaciones malintencionadas cuando vienen ocultas en troyanos de este tipo.
Trojan-Notifier	Caballos de troya notificadores	Le informan al atacante que puede introducirse en el sistema infectado y le envían información sobre el equipo: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso por medio del correo electrónico, FTP, ingreso a la página web del intruso o de otra manera. Los troyanos notificadores suelen utilizarse en conjuntos conformados por varios troyanos. Informan al intruso que se han instalado correctamente otros troyanos en el equipo del usuario.
Trojan-Proxy	Caballos de troya proxy	Permiten al intruso acceder de forma anónima a páginas web mediante el equipo del usuario. Con frecuencia, se utilizan para enviar correo no deseado.
Trojan-PSW	Programas que roban contraseñas	Los programas que roban contraseñas son una clase de caballo de troya que roba cuentas de usuarios, tales como datos de registro de software. Estos troyanos encuentran datos confidenciales en archivos del sistema y en el registro y se los envían al "atacante" mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo. Algunos de estos troyanos se categorizan en los distintos tipos descritos en esta 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 por Internet (Trojan-GameThief).
Trojan-Spy	Caballos de troya espías	Espían al usuario y reúnen información acerca de las acciones que este realiza cuando trabaja en el equipo. Pueden interceptar los datos introducidos por el usuario mediante el teclado, realizar capturas de pantalla o compilar listas de aplicaciones activas. Después de recibir la información, se la transfieren al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.
Trojan-DDoS	Caballos de troya atacantes de red	Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). Los piratas suelen infectar muchos equipos con estos programas de manera de utilizar los equipos para atacar a un único servidor simultáneamente. Los programas DoS llevan a cabo un ataque desde un único equipo con el conocimiento del usuario. Los programas DDoS (DoS distribuida) llevan a cabo ataques distribuidos desde distintos equipos sin que lo advierta el usuario del equipo infectado.
Trojan-IM	Troyanos que roban información de usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de quienes usan clientes de mensajería instantánea. Transfieren los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.
Rootkit	RootKits	Enmascaran la existencia y las acciones de otras aplicaciones malintencionadas para ayudarlas a perdurar en el sistema operativo. También pueden ocultar archivos, claves del registro que se utilicen para ejecutar aplicaciones malintencionadas o procesos que se encuentren cargados en la memoria del equipo infectado. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones en el equipo del usuario y en otros equipos de la red.

Trojan-SMS	Troyanos en la forma de mensajes SMS	Infectan teléfonos móviles y envían mensajes SMS a números de teléfono con tarifas elevadas.
Trojan-GameThief	Troyanos que roban información de usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, tras lo cual envían los datos al intruso mediante correo, 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 luego envían la información al hacker por correo electrónico, por FTP, a través de una página creada por el atacante o usando otros medios.
Trojan-Mailfinder	Troyanos que reúnen direcciones de correo	Recopilan direcciones de correo almacenadas en un equipo y se las envían al intruso mediante correo, FTP, acceso a la página web del intruso o de 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 malware, las herramientas maliciosas no realizan acciones inmediatamente después de iniciarse. Pueden almacenarse de manera segura e iniciarse en el equipo del usuario. A menudo, los intrusos utilizan las funciones de estos programas para crear virus, gusanos y troyanos, perpetrar ataques de red en servidores remotos, atacar equipos o llevar a cabo otras acciones malintencionadas.

  Varias funciones de las herramientas maliciosas se agrupan en los tipos descritos en la siguiente tabla.

  Funciones de herramientas maliciosas

Tipo	Name	Descripción
Constructor	Constructores	Permiten crear nuevos virus, gusanos y troyanos. Algunos constructores ofrecen una interfaz estándar, con ventanas para elegir el tipo de aplicación malintencionada que se va a crear, los métodos que se usarán para contrarrestar los depuradores y otras características.
DoS	Ataque de red	Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS).
Exploit	Exploits	Los *puntos vulnerables* son conjuntos de datos o códigos de programas que se sirven de las vulnerabilidades de la aplicación en la que se procesa para realizar una acción maliciosa en un equipo. Por ejemplo, un punto vulnerable puede escribir o leer archivos o solicitar páginas web "infectadas". Distintos puntos vulnerables se sirven de las vulnerabilidades de diversos servicios de red o aplicaciones. Disfrazados como paquete de red, los puntos vulnerables se transfieren a través de la red a numerosos equipos y buscan equipos con servicios de red vulnerables. Un punto vulnerable en un archivo DOC se sirve de las vulnerabilidades de un editor de texto. Puede comenzar a realizar las acciones preprogramadas por el pirata cuando el usuario abre el archivo infectado. Un punto vulnerable incrustado en un mensaje de correo busca vulnerabilidades en cualquier cliente de correo. Puede empezar a realizar una acción malintencionada apenas el usuario abre el mensaje infectado en dicho cliente. Los gusanos de red se propagan por las redes mediante los puntos vulnerables. Los puntos vulnerables Nuker son paquetes de red que deshabilitan equipos.
FileCryptor	Cifradores	Se utilizan para cifrar otras aplicaciones malintencionadas y evitar, con ello, que las aplicaciones antivirus las detecten.
Flooder	Programas para "contaminar" redes	Envían numerosos mensajes a través de canales de red. Este tipo de herramienta incluye, por ejemplo, programas que contaminan Internet Relay Chats. Las herramientas de tipo "flooder" no incluyen programas que "contaminan" los canales usados por el correo, los clientes de mensajería instantánea y los sistemas de comunicaciones móviles. Estos programas se describen de manera individual en la tabla (flooder de correo, IM-Flooder y flooder de SMS).
HackTool	Herramientas de piratería	Permiten los ataques a los equipos en los que están instalados o atacan otro equipo (por ejemplo, mediante la adición de nuevas cuentas de sistema sin el permiso del usuario o la eliminación de registros del sistema para ocultar rastros de su presencia en el sistema operativo). Este tipo de herramienta incluye algunos analizadores de protocolos que ofrecen funciones malintencionadas, como la interceptación de contraseñas. Los analizadores de protocolos son programas que permiten ver el tráfico de red.
Hoax	Hoax	Alarman al usuario con mensajes similares a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario de que se dio formato a un disco, cuando esto no sucedió en realidad.
Spoofer	Herramientas de falsificación	Envían mensajes y solicitudes de red con una dirección falsa del remitente. Los intrusos utilizan herramientas de falsificación para hacerse pasar por los verdaderos remitentes de los mensajes, por ejemplo.
VirTool	Herramientas que pueden ingresar modificaciones en las aplicaciones malintencionadas	Permiten la modificación de otros programas de software malware y los ocultan de las aplicaciones antivirus.
Email-Flooder	Programas que "contaminan" las direcciones de correo	Envían numerosos mensajes a varias direcciones de correo electrónico y, de este modo, las contaminan. Un gran volumen de mensajes entrantes impide que los usuarios vean mensajes deseados en sus buzones.
IM-Flooder	Programas que "contaminan" el tráfico de los clientes de MI	"Inundan" a los usuarios de clientes de MI con mensajes. Un gran volumen de mensajes impide a los usuarios visualizar mensajes entrantes deseados.
SMS-Flooder	Programas que "contaminan" el tráfico con mensajes SMS	Envían numerosos mensajes de SMS a teléfonos móviles.

- **Adware**

  Subcategoría: software de publicidad (Adware)

  Nivel de peligrosidad: medio

El adware muestra información publicitaria al usuario. Los programas de adware muestran anuncios publicitarios en las interfaces de otros programas y redireccionan las solicitudes de búsqueda a páginas web publicitarias. Algunos reúnen información de marketing acerca del usuario y la envían a su desarrollador. Esta información puede incluir los nombres de los sitios web visitados por el usuario o el contenido de sus solicitudes de búsqueda. A diferencia de los caballos de troya espías, el adware envía esta información al desarrollador con el permiso del usuario.

- **Marcadores automáticos**

  Subcategoría: Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales.

  Nivel de peligrosidad: medio

  La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP y Telnet.

  Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

  Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

Tipo	Name	Descripción
Cliente IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware.
Downloader	Programas para realizar descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas para supervisar	Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito.
RemoteAdmin	Programas de administración remota	Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo.
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores Telnet. Los intrusos los implantan 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 los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos.
NetTool	Herramientas de red	Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos.
Client-P2P	Clientes de red P2P	Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware.
Cliente SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
WebToolbar	Barras de herramientas web	Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Pseudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada.

- **Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales**

  Subcategoría: Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales.

  Nivel de peligrosidad: medio

  La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP y Telnet.

  Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

  Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

Tipo	Name	Descripción
Cliente IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware.

Downloader	Programas para realizar descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas para supervisar	Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito.
RemoteAdmin	Programas de administración remota	Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo.
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores Telnet. Los intrusos los implantan 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 los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos.
NetTool	Herramientas de red	Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos.
Client-P2P	Clientes de red P2P	Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware.
Cliente SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
WebToolbar	Barras de herramientas web	Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Pseudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada.

- **Objetos comprimidos cuya compresión pueda usarse para proteger un 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 descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen con compresores especiales. Los expertos de Kaspersky identificaron los compresores más utilizados por los piratas informáticos.

- **Objetos comprimidos con más de un empaquetador**

  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 descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen con compresores especiales. Los expertos de Kaspersky identificaron los compresores más utilizados por los piratas informáticos.

Exclusiones

Esta tabla contiene información acerca de las exclusiones de 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 archivo. Por ejemplo, `*\Program Files (x86)\Folder\Subfolder`.

Para excluir objetos de los análisis, puede usar los siguientes métodos:

- Especifique la ruta al archivo o a la carpeta.
- Especifique el hash del objeto.

- Usar máscaras:
  - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco 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 ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
  - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las 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 usar máscaras en cualquier parte de la ruta de acceso a una carpeta o un archivo. Por ejemplo, si desea que el alcance del análisis incluya la carpeta Descargas para todas las cuentas de usuario del equipo, escriba 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 en la consola de Kaspersky Security Center. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

- Escriba el nombre que se le da al tipo de objeto en la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`). Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza 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 de análisis locales en la interfaz de usuario de la aplicación si el administrador bloquea la configuración de las exclusiones de análisis en la consola (símbolo de "candado cerrado") y las exclusiones de análisis locales están prohibidas (la casilla **Permitir el uso de exclusiones locales** está desactivada).

Aplicaciones de confianza

En esta tabla, se enumeran las aplicaciones de confianza cuya actividad no supervisa Kaspersky Endpoint Security durante su funcionamiento.

Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar 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 aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

El componente Control de aplicaciones regula el inicio de cada una de las aplicaciones sin tener en cuenta si la aplicación se incluye 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 **Permitir el uso de aplicaciones de confianza locales** está desactivada).

Combinar 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 está seleccionada, los elementos de la lista de la directiva principal de Kaspersky Security Center se mostrarán en las directivas secundarias. Así 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. Si lo necesita, podrá agregar, editar y eliminar elementos de la lista en directivas de menor jerarquía. 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 esta casilla no está seleccionada, los elementos de las listas no se fusionarán cuando una directiva de Kaspersky Security Center herede la configuración de otra. Esta funcionalidad también permite fusionar listas en perfiles de directivas. Para fusionar listas, en el perfil de mayor prioridad, habilite la herencia de la configuración de un perfil de menor prioridad. Para obtener más detalles sobre las prioridades del perfil de directivas, consulte la Ayuda de Kaspersky Security Center .
Permitir el uso de exclusiones locales/Permitir el uso de aplicaciones de confianza locales *(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 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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo. Si la casilla no está seleccionada, 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 acerca de las exclusiones de telemetría EDR.
Telemetría KUMA *(disponible solo en la Consola de Kaspersky Security Center)*	Lista de eventos que se enviarán a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security funciona en los siguientes modos: • **Enviar todos los eventos**. En este modo, la aplicación envía todos los eventos del registro de Windows, excepto los agregados a las reglas de exclusión. • **Enviar solo los eventos seleccionados**. En este modo, la aplicación solo envía los eventos agregados a las reglas de inclusión.
Almacén de confianza de certificados del sistema	Si se selecciona uno de los almacenes de certificados de sistema 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 confianza**. Si se selecciona **No usar**, Kaspersky Endpoint Security analiza las aplicaciones independientemente de si tienen o no una firma digital. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

Configuración de la aplicación

Puede configurar la siguiente configuración general de la aplicación:

- Modo de funcionamiento
- Autoprotección
- Rendimiento
- Información para depuración
- Estado del equipo cuando se aplique la configuración

Parámetro	Descripción
Iniciar la aplicación al arrancar el equipo (recomendado)	Si esta opción está seleccionada, Kaspersky Endpoint Security se inicia después de cargado el sistema operativo y protege al equipo durante toda la sesión. Cuando se desactiva esta casilla, Kaspersky Endpoint Security no se inicia después de cargado el sistema operativo, sino cuando el usuario lo inicia manualmente. La protección del equipo está desactivada y los datos del usuario pueden estar expuestos a amenazas.
Usar la tecnología de desinfección avanzada (consume una cantidad considerable de recursos de la PC)	Por lo general, Kaspersky Endpoint Security finaliza la ejecución del malware detectado antes de que infecte el equipo. Con Tecnología de desinfección avanzada, el equipo está protegido ante malware ya activo (infección activa), lo que minimiza el riesgo de perder datos y que se propague la amenaza. Si esta tecnología está habilitada, al detectar actividad maliciosa, Kaspersky Endpoint Security muestra una notificación emergente. En la notificación, Kaspersky Endpoint Security ofrece al usuario realizar una desinfección avanzada del equipo. Cuando el usuario aprueba este procedimiento, Kaspersky Endpoint Security neutraliza la amenaza y reinicia el equipo. La tecnología de desinfección avanzada utiliza una cantidad considerable de recursos del equipo, lo que puede ralentizar otras aplicaciones. Cuando la aplicación está en proceso de detectar una infección activa, algunas funciones del sistema operativo pueden no estar disponibles. La disponibilidad del sistema operativo se restaura cuando finaliza la desinfección avanzada y se reinicia el equipo. Si Kaspersky Endpoint Security está instalado en un equipo con Windows for Servers, Kaspersky Endpoint Security no mostrará la notificación. Por lo tanto, el usuario no podrá seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación y habilitar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis de malware*. A continuación, debe iniciar la tarea *Análisis de malware*.
Usar Kaspersky Security Center como servidor proxy para la activación *(disponible solo en la Consola de Kaspersky Security Center)*	Si esta casilla está seleccionada, la aplicación usa el Servidor de administración de Kaspersky Security Center como servidor proxy para conectarse a los servidores de activación. Esto es necesario cuando está usando un código de activación para activar la aplicación en un segmento de red aislado sin acceso a Internet. Para activar la aplicación con un archivo de clave, no se requiere acceso a Internet.
Habilitar la Autoprotección	Si esta característica está seleccionada, Kaspersky Endpoint Security impide la modificación y la eliminación de archivos de aplicaciones en el disco duro, procesos de memoria y entradas en el registro del sistema.
Bloquear administración externa de los servicios de la aplicación	Si esta característica está seleccionada, Kaspersky Endpoint Security no permite administrar los servicios de la aplicación mediante aplicaciones de terceros (como CMD). Cuando se intenta administrar los servicios de la aplicación mediante aplicaciones de terceros, aparece una notificación en la barra de tareas de Microsoft Windows, por encima del ícono de la aplicación (a menos que el usuario haya desactivado el servicio de notificaciones). Puede permitir la administración externa de servicios de aplicaciones solo en equipos que no sean compatibles con la tecnología AM-PPL o en equipos que tengan la tecnología deshabilitada.
Posponer las tareas programadas cuando el equipo funciona con carga de batería	Si se selecciona esta casilla, el modo de ahorro de energía se habilita cuando el equipo funciona con alimentación de la batería. Kaspersky Endpoint Security pospone las tareas programadas. Las tareas de análisis y actualización podrán iniciarse manualmente cuando sea necesario. Cuando el modo de ahorro de energía está activado y el equipo está funcionando con alimentación de la batería, las siguientes tareas no se ejecutan, incluso si estuvieran programadas: • *Análisis completo* • *Análisis de áreas críticas* • *Análisis personalizado* • *Comprobación de integridad de la aplicación* • *Análisis de IOC* • *Actualización de bases de datos y módulos de la aplicación* (solo parches) La aplicación omite las actualizaciones programadas de la base de datos únicamente cuando el equipo portátil funciona con batería y el nivel de carga es inferior al 30 %. En todos los demás casos, Kaspersky Endpoint Security actualiza las bases de datos según lo programado, independientemente de si el equipo portátil está conectado a la corriente o funciona con batería, o de si la aplicación se encuentra en modo de ahorro de energía.

Parámetro	Descripción
Conceder recursos a otras aplicaciones	Es posible que el consumo de recursos del equipo por parte de Kaspersky Endpoint Security al analizar el equipo aumente la carga de la CPU y de los subsistemas del disco duro. Esto puede ralentizar otras aplicaciones. Para optimizar el rendimiento, Kaspersky Endpoint Security proporciona un *modo para transferir recursos a otras aplicaciones*. En este modo, el sistema operativo puede dar menos prioridad a los subprocesos de la tarea de análisis de Kaspersky Endpoint Security cuando la carga de la CPU sea alta. Esto permite redistribuir los recursos del sistema operativo a otras aplicaciones. De este modo, las tareas de análisis recibirán menos tiempo de CPU. Por consiguiente, Kaspersky Endpoint Security tardará más tiempo en analizar el equipo. Por defecto, la aplicación está configurada para dispensar recursos para otras aplicaciones.
Restringir el uso de CPU para las tareas del análisis	Para optimizar el rendimiento de Kaspersky Endpoint Security, puede limitar el uso de la CPU por parte de la tarea *Análisis de malware*. Si se selecciona la casilla, la carga promedio en todos los núcleos de la CPU de la tarea *Análisis de malware* alcanza el valor especificado. De manera predeterminada, la casilla está desactivada.
Habilitar escritura en archivos de volcado	Si se selecciona la casilla, Kaspersky Endpoint Security escribe en los archivos de volcado cuando se cierra inesperadamente. Si se desactiva la casilla, Kaspersky Endpoint Security no escribe en los archivos de volcado. La aplicación también elimina los archivos de volcado actuales del disco duro del equipo.
Habilitar la protección de los archivos de volcado y de seguimiento	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 los administradores del sistema y locales pueden acceder a archivos de seguimiento. Si la casilla se desactiva, todos los usuarios podrán acceder a los archivos de volcado y de seguimiento.
Estado del equipo cuando se aplique la configuración *(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 permite garantizar el funcionamiento ininterrumpido de los servidores. Puede actualizar la aplicación sin reiniciar el equipo 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 del parámetro varía según el tipo de sistema operativo. Si la aplicación está instalada en una estación de trabajo, se deshabilita la opción de actualizar la aplicación sin reiniciar. Si la aplicación está instalada en un servidor, se habilita la opción de actualizar la aplicación sin reiniciar.
Compatible con 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 habilitar el modo de compatibilidad. Los problemas pueden estar relacionados con la incompatibilidad de las RAT con la funcionalidad Secure Desktop. El propósito de esta funcionalidad es confirmar las acciones que potencialmente 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 derechos de alto nivel para proteger la solicitud. De esta forma, solo el usuario puede confirmar la acción y no el malware. Si se selecciona esta opción, se habilita el modo de compatibilidad con la RAT. La aplicación muestra un cuadro de diálogo de confirmación sin esta funcionalidad. Esto puede reducir el nivel de seguridad del equipo. No recomendamos habilitar el modo de compatibilidad si Kaspersky Endpoint Security no está causando problemas con la RAT. Si cancela la selección de esta opción, se deshabilita el modo de compatibilidad con la RAT. De manera predeterminada, la casilla está desactivada. Ejemplo: Cuando se utiliza el navegador en modo RemoteApp, es posible que Kaspersky Endpoint Security no muestre una ventana de confirmación cuando se visita un sitio web con un certificado no confiable, ya que 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 habilitar el modo de compatibilidad. También puede intentar habilitar el modo de compatibilidad si tiene problemas con la funcionalidad de Escritorio Seguro al utilizar otro software de terceros.

Informes y repositorios

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.14.1\Report`.

Copias de seguridad

El depósito *Copia de seguridad* contiene copias de respaldo de los archivos que se modifican o eliminan cuando se realiza una desinfección. Una *copia de seguridad* es una copia del archivo creada antes de desinfectar o eliminar el archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. Se conceden accesos limitados a esta carpeta al usuario cuya cuenta se utilizó para instalar Kaspersky Endpoint Security.

> Kaspersky Endpoint Security no brinda la capacidad de configurar permisos de acceso de usuario a copias de seguridad de 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 Cuarentena solo cuando se integra con la solución 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 a través de Web Console. También puede usar Web Console para administrar objetos en cuarentena (restaurar, eliminar, agregar, etc.). Puede restaurar objetos localmente en el equipo mediante el uso de la línea de comandos.

> Kaspersky Endpoint Security usa la cuenta del sistema (SYSTEM) para mover los archivos a cuarentena.

Parámetro	Descripción
Eliminar informes después de (días)	Si la casilla está seleccionada, los informes se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de informes es de 30 días. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.
Limitar el tamaño del archivo de informe a (MB)	Si la casilla está seleccionada, el tamaño máximo del archivo de informes se limitará al valor definido. Por defecto, el tamaño máximo del archivo es de 1024 MB. Para evitar que se exceda el tamaño máximo del archivo del informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas de este archivo cuando alcanza el tamaño máximo.
Eliminar objetos después de (días)	Si la casilla está seleccionada, los archivos se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de archivos es de 30 días. Al caducar el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos de Copia de seguridad.
Limitar el tamaño de Copia de seguridad a (MB)	Si la casilla está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo 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 la Cuarentena	Si la casilla está seleccionada, el espacio de Cuarentena se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo es de 1024 MB. Una vez que la Cuarentena alcanza el tamaño máximo, Kaspersky Endpoint Security envía el evento *No hay suficiente espacio en el almacenamiento en la cuarentena* a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación deja de mover nuevos objetos a cuarentena. Debe vaciar manualmente la Cuarentena.
Avisarme cuando el almacenamiento de la Cuarentena alcance el (%)	Valor umbral de la Cuarentena. Por ejemplo, puede establecer el umbral de la Cuarentena en 50 %. Una vez que la Cuarentena alcance 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 moviendo nuevos objetos a cuarentena.
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 deshabilitar la transferencia de algunos datos para optimizar el uso del 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 Cuarentena solo cuando se integra con la solución Kaspersky Detection and Response. • **Acerca de los archivos almacenados en Copias de seguridad**. Puede ver la lista de archivos en 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 no procesados en la consola de Kaspersky Security Center, en la carpeta **Avanzado** → **Repositorios** → **Amenazas activas**. • **Acerca de los dispositivos instalados**. Puede ver la lista de dispositivos conectados en la consola de Kaspersky Security Center en la carpeta **Avanzado** → **Repositorios** → **Hardware**. También podrá acceder a la lista de dispositivos en las propiedades del equipo y en la directiva de Kaspersky Endpoint Security para Windows (sección **Control de dispositivos**). • **Acerca de las aplicaciones iniciadas**. Puede ver la lista de archivos ejecutables en la consola de Kaspersky Security Center, en la carpeta **Avanzado** → **Administración de aplicaciones** → **Archivos ejecutables**. También podrá acceder a la lista de archivos ejecutables 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**. También podrá acceder a la lista de errores en las propiedades del equipo. • **Informe sobre el estado de las reglas del 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**. También podrá acceder al informe en las propiedades de la directiva de Kaspersky Endpoint Security para Windows (sección **Control de anomalías adaptativo**). • **Informe sobre las reglas activadas del 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**. También podrá acceder al informe en las propiedades de la directiva de Kaspersky Endpoint Security para Windows (sección **Control de anomalías adaptativo**). • **Acerca de la cadena de desarrollo de la amenaza**. Puede ver los detalles de la detección en Kaspersky Security Center Web Console en la sección **Supervisión** → **Alertas**. La solución Kaspersky Endpoint Detection and Response utiliza información sobre la cadena de desarrollo de la amenaza.

Configuración de red

Puede configurar el servidor proxy que se utiliza para conectarse a Internet y actualizar las bases de datos antivirus, seleccionar el modo de vigilancia para los puertos de red y configurar el análisis de conexiones cifradas.

Parámetro	Descripción
Limitar el tráfico de las conexiones de uso medido	Si esta casilla está seleccionada, la aplicación limita su propio tráfico de red cuando la conexión a Internet está limitada. Kaspersky Endpoint Security identifica las conexiones de Internet móviles de alta velocidad como limitadas, y las conexiones Wi-Fi como ilimitadas. Redes basadas en costos funciona en equipos con Windows 8 o posterior.
Inyectar un script en el tráfico web para interactuar con las páginas web	Si la casilla de verificación está seleccionada, Kaspersky Endpoint Security inyecta un script de interacción de la página web en el tráfico web. Esta secuencia de comandos garantiza que el componente Control web pueda funcionar correctamente. El script permite registrar eventos de Control web. Sin este script, no puede habilitar 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	La configuración del servidor proxy utilizado para el acceso a Internet de los usuarios de los equipos cliente. Kaspersky Endpoint Security utiliza estas opciones de configuración para ciertos componentes de protección, inclusive para la actualización de bases de datos y módulos de aplicación. Para la configuración automática de un servidor proxy, Kaspersky Endpoint Security usa el protocolo WPAD (protocolo de detección automática de proxy web). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, la aplicación usa la dirección especificada en la configuración del navegador Microsoft Internet Explorer.
No usar el servidor proxy para las direcciones locales	Si la casilla está seleccionada, Kaspersky Endpoint Security no utiliza un servidor proxy cuando realiza 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 ingresar 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 ingrese las credenciales. **No usar autenticación**. **Autenticación NTLM**. Autenticación NTLM con la cuenta de usuario actual (predeterminado). **Autenticación NTLM con nombre de usuario y contraseña**. Autenticación NTLM con credenciales especificadas manualmente. **Nombre de usuario y contraseña**. Autenticación con credenciales especificadas manualmente. **Autenticación automática**. **Autenticación Kerberos**. Autenticación 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) para cada registro CNAME. **Autenticación Kerberos con nombre de usuario y contraseña**. Autenticación Kerberos con credenciales especificadas manualmente. Si se selecciona la autenticación Kerberos, Kaspersky Endpoint Security puede, según la configuración del servidor proxy, realizar la autenticación mediante el protocolo Kerberos o NTLM.
Puertos vigilados	**Vigilar todos los puertos de red**. En este modo de supervisión de puertos de red, los componentes de protección (Protección contra archivos peligrosos, Protección contra amenazas web y Protección contra amenazas de correo) controlan los flujos de datos que se transmiten a través de cualquier puerto de red abierto del equipo. **Vigilar solo los puertos de red seleccionados**. Cuando se selecciona este modo, los componentes de protección vigilan los puertos de red seleccionados 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**. En este modo, se utiliza una lista predefinida con las aplicaciones a las que están asociados los puertos que Kaspersky Endpoint Security vigilará. La lista incluye aplicaciones como Google Chrome, Adobe Reader y Java. **Vigilar todos los puertos de las aplicaciones especificadas**. En este modo, se utiliza una lista de aplicaciones asociadas a los puertos que Kaspersky Endpoint Security deberá vigilar.

Parámetro	Descripción
Análisis de conexiones cifradas	Kaspersky Endpoint Security analiza el tráfico de red cifrado que se transmite a través de los protocolos siguientes: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security es compatible con los siguientes modos de análisis de conexiones cifradas: • **No analizar las conexiones cifradas**. Kaspersky Endpoint Security no tendrá acceso al contenido de los sitios web cuyas direcciones comienzan con `https://`. • **Analizar las conexiones cifradas si lo solicitan los componentes de protección**. Kaspersky Endpoint Security analizará solo el tráfico cifrado cuando lo soliciten los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control Web. • **Analizar siempre las conexiones cifradas**. Kaspersky Endpoint Security analizará el tráfico de red cifrado, aunque los componentes de protección estén deshabilitados. 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 únicamente en la interfaz de Kaspersky Endpoint Security. No puede verla 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 agregar 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 agregar un certificado al almacén de certificados del sistema, debe utilizar directivas de grupo de Active Directory.
Visita de 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 contendrá un vínculo para obtener acceso al recurso web solicitado. Si una aplicación o un servicio de terceros establece una conexión con un dominio con un certificado no confiable, Kaspersky Endpoint Security crea su propio certificado para analizar el tráfico. El nuevo certificado tiene el estado *No confiables*. Esto es necesario para advertir a la aplicación de terceros sobre la conexión no confiable, ya que en este caso puede no mostrarse la página HTML y la conexión se puede establecer en segundo plano. • **Bloquear**. Cuando se elige esta opción y se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security bloquea 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.
Visita de un dominio con un error de análisis de conexiones cifradas	• **Bloquear**. Si se produce un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red. • **Permitir y agregar el dominio a exclusiones**. Si se produce un error al analizar una conexión cifrada, Kaspersky Endpoint Security agrega el dominio que provocó el error a la lista de dominios con errores de análisis y no supervisa el tráfico de red cifrado cuando se visita este dominio. La lista de dominios con errores de análisis 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 las conexiones SSL 2.0	Si la casilla está seleccionada, la aplicación supervisa y bloquea las conexiones de red que se establecen con el protocolo SSL 2.0. Si la casilla está desactivada, 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 las conexiones SSL 3.0	Si la casilla está seleccionada, la aplicación bloquea las conexiones de red que se establecen con el protocolo SSL 3.0. Si la casilla está desactivada, 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 las conexiones TLS 1.0	Si la casilla está seleccionada, la aplicación bloquea las conexiones de red que se establecen con el protocolo TLS 1.0. Si la casilla está desactivada, 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 una conexión cifrada con el sitio web con certificado de EV	Los certificados de EV (Extended Validation Certificate) confirman la autenticidad de los sitios web y mejoran la seguridad de la conexión. Los navegadores utilizan un icono de candado en su barra de direcciones para indicar que un sitio web tiene un certificado de validación extendida. Además, es posible que en los navegadores se vea toda la barra de direcciones en color verde o una parte de ella. Si la casilla está seleccionada, la aplicación descifra y controla las conexiones cifradas que se establecen con sitios web que utilizan certificados de EV. Cuando esta casilla no está activada, la aplicación no tiene acceso al contenido del tráfico HTTPS. Esto significa que la aplicación únicamente puede controlar el tráfico HTTPS basándose en la dirección del sitio web (por ejemplo, `https://bing.com`). Si abre un sitio web con un certificado de validación extendida por primera vez, la conexión cifrada se descifrará sin importar si se seleccionó la casilla.
Configurar direcciones de confianza	Para esta función, se utiliza una lista de direcciones web que Kaspersky Endpoint Security excluye del análisis de conexiones. En este caso, Kaspersky Endpoint Security no analiza el tráfico HTTPS de las direcciones web de confianza cuando los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control web están haciendo su trabajo. Puede ingresar un nombre de dominio o una dirección IP. Kaspersky Endpoint Security admite el carácter `*` para ingresar una máscara en el nombre de dominio. Kaspersky Endpoint Security no admite el símbolo `*` para direcciones IP. Puede seleccionar un intervalo de direcciones IP con 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 no incluye 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 no incluye el dominio `domain.com`. • `*.domain.com`: el registro incluye las siguientes direcciones: `https://movies.domain.com`, `https://images.domain.com/page123`. El registro no incluye el 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 ingresar una máscara.
Para analizar conexiones cifradas en aplicaciones con su almacén de certificados propios, use *(disponible solo en la interfaz de Kaspersky Endpoint Security)*	Si esta casilla está seleccionada, 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 habilitar el Análisis de conexiones cifradas. Si el Análisis de conexiones cifradas está deshabilitado, la aplicación no analiza el tráfico del navegador Mozilla Firefox ni el cliente de correo Thunderbird. La aplicación utiliza el certificado raíz de Kaspersky para descifrar y analizar el tráfico cifrado. Puede seleccionar el almacén de certificados que contendrá el certificado raíz de Kaspersky. • **Almacén de certificados de Windows (recomendado)**. El certificado raíz de Kaspersky se agrega a esta tienda durante la instalación de Kaspersky Endpoint Security. • **Almacén de certificados propios**. Mozilla Firefox y Thunderbird utilizan sus propios almacenes de certificados. Si se selecciona el almacén de certificados de Mozilla, debe agregar manualmente el certificado raíz de Kaspersky a este almacén 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 ícono 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, encima del ícono de la aplicación, únicamente las notificaciones que requieren la intervención del usuario. **Mostrar interfaz del usuario**. La ventana principal de Kaspersky Endpoint Security y el ícono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. 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 Monitor de actividades de aplicaciones**. En el equipo cliente, en la ventana principal de Kaspersky Endpoint Security, el botón **Monitor de actividades de aplicaciones** no está disponible. El *Monitor de actividades de aplicaciones* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de las aplicaciones en el equipo de un usuario. **No mostrar interfaz del usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El ícono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.
Configurar las notificaciones	Tabla con la configuración de notificaciones de eventos de diferentes niveles de importancia que pueden producirse durante el funcionamiento de un componente o tarea, o de la aplicación completa. Kaspersky Endpoint Security muestra notificaciones sobre estos eventos en la pantalla, los envía por correo electrónico o los registra.
Configurar las notificaciones de correo electrónico	Parámetros del servidor SMTP con el que se enviarán las notificaciones de los eventos registrados mientras la aplicación esté en funcionamiento. De manera predeterminada, Kaspersky Endpoint Security usa la configuración de notificaciones por correo electrónico de Kaspersky Security Center. Para obtener más información sobre la configuración de notificaciones por correo electrónico, consulte la Ayuda de Kaspersky Security Center. Si necesita configurar notificaciones de correo electrónico individuales, puede editar las siguientes configuraciones: • **Dirección del remitente**. Dirección de correo electrónico del remitente. No se recomienda usar una dirección inexistente. • **Servidor SMTP**. Una o más direcciones de servidores de correo electrónico de su organización (por ejemplo, `mail.company.com`). Puede ingresar 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 por correo electrónico, puede enviar un mensaje de prueba. • **Dirección**. Direcciones de correo electrónico de los destinatarios a los que la aplicación enviará notificaciones. • **Modo de envío**. Modo de envío de notificaciones por correo electrónico. Kaspersky Endpoint Security puede enviar mensajes inmediatamente cuando ocurre un evento; alternativamente, puede seguir una programación preconfigurada.
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 sobre el estado de las bases de datos antimalware locales	Configuración de notificaciones sobre bases de datos antivirus obsoletas utilizadas por la aplicación.
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. El alcance 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 para el usuario/Vínculos a recursos web *(disponible solo en la Consola de Kaspersky Security Center)*	Lista de vínculos a recursos web que contienen información sobre asistencia técnica para Kaspersky Endpoint Security. Los vínculos agregados se mostrarán en la ventana **Soporte** de la interfaz local de Kaspersky Endpoint Security en lugar de los vínculos estándar.
Soporte para el 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 otro equipo. 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 local de Kaspersky Endpoint Security.

Parámetros de administración de la configuración de la aplicación

Configuración	Descripción
Importar	Extraiga la configuración de la aplicación de un archivo en formato CFG y aplíquela.
Exportar	Guarde la configuración actual de la aplicación en un archivo en formato CFG.
Restaurar	Puede restaurar la configuración de la aplicación recomendada por Kaspersky en cualquier momento. Después de restaurar la configuración, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección.

Actualización de bases de datos y módulos de software de la aplicación

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Endpoint Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antivirus y de la base de código) dejar de estar disponible en el software en el territorio de EE. UU.

Las actualizaciones regulares requieren una licencia en vigencia. Si no hay una licencia actual, se podrá realizar una única actualización.

Su equipo debe estar conectado a Internet para descargar correctamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. Por defecto, la configuración de la conexión a Internet se determina automáticamente. Si utiliza un servidor proxy, debe definir su configuración.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTP.

Al realizar una actualización, se descargan e instalan en el equipo los siguientes objetos:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se brinda con bases de datos que contienen firmas de virus y otras amenazas e información sobre maneras de neutralizarlas. Los componentes de protección utilizan esta información al realizar búsquedas de archivos infectados en el equipo y neutralizarlos. Las bases de datos se actualizan constantemente con registros de amenazas nuevas y métodos para contrarrestarlas. Por lo tanto, le recomendamos actualizar las bases de datos con regularidad.

  Además de las bases de datos de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de la aplicación interceptar el tráfico de la red.

- Módulos de la aplicación. Además de las bases de datos de Kaspersky Endpoint Security, también se pueden actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación repara vulnerabilidades en Kaspersky Endpoint Security y agrega funciones nuevas o mejora funciones existentes.

Durante la actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con la versión actualizada en el origen de actualizaciones. Si las bases de datos y los módulos de la aplicación actuales difieren de las respectivas versiones actualizadas, la parte faltante de las actualizaciones se instala en el equipo.

Si las bases de datos están obsoletas, es posible que el tamaño del paquete de actualización sea considerable, lo que puede ocasionar un mayor tráfico web (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 ícono de la aplicación en el área de notificaciones.

La información sobre los resultados de la actualización y sobre todos los eventos que ocurren durante la ejecución de la tarea de actualización se registra en el informe de Kaspersky Endpoint Security.

Si la aplicación funciona en el modo de Light Agent, se aplican consideraciones especiales en la actualización de las bases de datos y los módulos de la aplicación.

Configuración de actualización de las bases de datos y los módulos de la aplicación

Parámetro	Descripción
Programa de actualización de bases de datos	**Automáticamente**. En este modo, la aplicación comprueba el origen de las actualizaciones en busca de nuevos paquetes de actualizaciones con una cierta frecuencia. La frecuencia de las comprobaciones para detectar paquetes de actualizaciones aumenta durante las epidemias de virus y disminuye cuando no hay epidemias. Después de detectar un paquete de actualizaciones nuevo, Kaspersky Endpoint Security lo descarga e instala las actualizaciones en el equipo. **Manualmente**. Este modo de ejecución de la tarea de actualización permite iniciar manualmente la tarea de actualización. **Mediante programación**. En este modo de ejecución de la tarea de actualización, Kaspersky Endpoint Security ejecuta la tarea de actualización de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de actualización, también se puede iniciar manualmente la tarea de actualización de Kaspersky Endpoint Security.
Ejecutar tareas no realizadas	Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea omitida tan pronto como sea posible. La tarea puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea. Cuando la aplicación tiene la oportunidad de ejecutar tareas no realizadas, las ejecuta aleatoriamente dentro de un cierto intervalo de tiempo para distribuir la carga en el equipo. Si la casilla está desactivada, Kaspersky Endpoint Security no ejecuta las tareas omitidas. En lugar de eso, ejecuta la siguiente tarea según la programación actual.

Parámetro	Descripción
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. Como origen de actualizaciones, puede utilizar el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky o una carpeta local o de red dispuesta para tal fin. Si los servidores de actualizaciones de Kaspersky no están disponibles, Kaspersky Endpoint Security puede usar dominios alternativos para actualizar sus bases de datos y módulos de software de la aplicación. Para obtener más información, consulte la Base de conocimientos del Servicio de soporte técnico. La lista por defecto de orígenes de actualizaciones incluye a los servidores de actualización de Kaspersky Security Center y de Kaspersky. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las actualizaciones. Kaspersky Endpoint Security no admite actualizaciones que provengan de servidores HTTPS, a menos que sean servidores de actualización de Kaspersky. Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno tras otro, comenzando por el principio de la lista, y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible. De manera predeterminada, Kaspersky Endpoint Security usa el servidor de Kaspersky Security Center como el primer origen de actualizaciones. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una directiva a la computadora, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de *Actualización de bases de datos y módulos de la aplicación* de la tarea local, ya que es posible que la aplicación no tenga acceso al servidor de Kaspersky Security Center. Si la aplicación se ejecuta en el modo de Light Agent, se selecciona una carpeta en la SVM como origen de actualizaciones.
Ejecutar las actualizaciones de bases de datos como	Por defecto, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta ha usado para iniciar sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security puede actualizarse desde un origen de actualizaciones al cual el usuario que inició sesión no puede acceder debido a la falta de permisos exigidos (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o una fuente de actualización para la cual no se ha configurado la autenticación del servidor proxy. En la configuración de la aplicación, puede especificar un usuario que tenga dichos derechos y comenzar la tarea de actualización de Kaspersky Endpoint Security de la cuenta de este usuario.
Descargar actualizaciones de módulos de la aplicación	Descarga de actualizaciones del módulo de la aplicación con actualizaciones de la base de datos de la aplicación. Si está seleccionada la casilla, Kaspersky Endpoint Security notifica al usuario sobre actualizaciones de módulos de aplicación disponibles e incluye las actualizaciones de los módulos de aplicación en el paquete de actualización mientras se ejecuta la tarea de actualización. La forma en la que se aplican las actualizaciones de los módulos de la aplicación está determinada por la siguiente configuración: • **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. • **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada. Si está desmarcada la casilla, Kaspersky Endpoint Security no notifica al usuario sobre actualizaciones de módulos de aplicación disponibles y no incluye las actualizaciones de los módulos de aplicación en el paquete de actualización mientras se ejecuta la tarea de actualización. Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final. Esta casilla está seleccionada de forma predeterminada.
Copiar las actualizaciones a la siguiente carpeta	Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security copia el paquete de actualizaciones a la carpeta compartida especificada bajo la casilla de verificación. A continuación, otros equipos en la LAN pueden recibir el paquete de actualización desde esta carpeta compartida. Esto reduce el tráfico de Internet debido a que el paquete de actualización sólo puede descargarse una vez. La carpeta especificada por defecto es `C:\ProgramData\Kaspersky Lab\KES.14.1\Update distribution\`.

Parámetro	Descripción
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 equipos cliente para actualizar los módulos de la aplicación y las bases de datos. Para la configuración automática de un servidor proxy, Kaspersky Endpoint Security usa 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 del servidor proxy especificada en la configuración del navegador Microsoft Internet Explorer.
No usar el servidor proxy para direcciones locales *(disponible solo en la interfaz de Kaspersky Endpoint Security)*	Si la casilla está seleccionada, Kaspersky Endpoint Security no utiliza un servidor proxy cuando realiza una actualización desde una carpeta compartida.

Apéndice 2. Grupos de confianza de aplicaciones

Kaspersky Endpoint Security categoriza todas las aplicaciones que se inician en el equipo en grupos de confianza. Se categorizan según el nivel de peligrosidad que las aplicaciones suponen para el sistema operativo.

Los grupos de confianza se organizan del siguiente modo:

- **De confianza**. Este grupo incluye las aplicaciones para las que se cumplen una o más de las siguientes condiciones:
  - las aplicaciones tienen la firma digital de un proveedor de confianza;
  - las aplicaciones están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - El usuario colocó la aplicación en el grupo *De confianza*.

  No hay ninguna operación prohibida para estas aplicaciones.
- **Restricción mínima**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - las aplicaciones no tienen la firma digital de un proveedor de confianza;
  - las aplicaciones no están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - El usuario colocó la aplicación en el grupo *Restricción mínima*.

  Estas aplicaciones están sujetas a restricciones mínimas para el acceso a los recursos del sistema operativo.
- **Restricción máxima**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - las aplicaciones no tienen la firma digital de un proveedor de confianza;
  - las aplicaciones no están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - El usuario colocó la aplicación en el grupo *Restricción máxima*.

  Estas aplicaciones están sujetas a restricciones máximas para el acceso a los recursos del sistema operativo.

- **No confiables**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - las aplicaciones no tienen la firma digital de un proveedor de confianza;
  - las aplicaciones no están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - El usuario colocó la aplicación en el grupo *No confiables*.

  Estas aplicaciones no tienen permitido realizar ninguna operación.

Apéndice 3. Extensiones de archivo para el análisis rápido de unidades extraíbles

com: archivo ejecutable de una aplicación que no supera los 64 KB

exe: archivo ejecutable o archivo autoextraíble

sys: archivo de sistema de Microsoft Windows

prg – texto de programas para dBase™, Clipper o Microsoft FoxPro Visual®, o un programa WAVmaker

bin: archivo binario

bat: archivo de lote

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para el DOS), OS/2

dpl: biblioteca Borland Delphi comprimida

dll: biblioteca de vínculos dinámicos

scr: pantalla inicial de Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto de Microsoft OLE (Object Linking and Embedding)

tsp: programa que se ejecuta en modo de tiempo dividido

drv: controlador de dispositivos

vxd: controlador de dispositivos virtuales de Microsoft Windows

pif: archivo de información del programa

lnk: archivo de vínculos de Microsoft Windows

reg: archivo de claves del registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de la configuración para Microsoft Windows, Windows NT y algunas aplicaciones

cla: clase de Java

vbs – script de Visual Basic®

vbe: extensión de video del BIOS

js, jse: texto fuente de JavaScript

htm: documento del hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta – programa de hipertexto para Microsoft Internet Explorer®

asp: script de Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script que se integra en archivos HTML

wsh: archivo de Microsoft Windows Script Host

wsf: script de Microsoft Windows

the: archivo del tapiz de escritorio de Microsoft Windows 95

hlp: archivo de ayuda de Windows

msg: mensaje de correo electrónico de Microsoft Mail

plg: mensaje de correo electrónico

mbx: mensaje de correo electrónico guardado de Microsoft Office Outlook

doc*: documentos de Microsoft Office Word, por ejemplo: doc para documentos de Microsoft Office Word, docx para documentos de Microsoft Office Word 2007 compatibles con XML, y docm para documentos de Microsoft Office Word 2007 compatibles con macros

dot*: plantillas de documentos de Microsoft Office Word, por ejemplo: dot para plantillas de documentos de Microsoft Office Word, dotx para plantillas documentos de Microsoft Office Word 2007 y dotm para plantillas de documentos de Microsoft Office Word 2007 compatibles con macros

fpm: programa de base de datos, archivo de inicio de Microsoft Visual FoxPro

rtf: documento con formato de texto enriquecido

shs: fragmento del manipulador de objetos de desecho de la Shell de Windows

dwg – base de datos de planos de AutoCAD®

msi: paquete de Microsoft Windows Installer

otm: proyecto de VBA para Microsoft Office Outlook

pdf: documento de Adobe Acrobat

swf – objeto del paquete de Shockwave® Flash

jpg, jpeg: formato de gráfico de imagen comprimida

emf: archivo con formato de metarchivo mejorado

ico: archivo de icono de objeto

ov? - archivos ejecutables de Microsoft Office Word

xl*: documentos y archivos de Microsoft Office Excel, por ejemplo: xls, la extensión correspondiente a Microsoft Office Excel, xlc para diagramas, xlt para plantillas de documentos, xlsx para libros de Microsoft Office Excel 2007, xltm para libros de Microsoft Office Excel 2007 compatibles con macros, xlsb para libros 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 compatibles con macros y xlam para complementos de Microsoft Office Excel 2007 compatibles con macros

pp* – documentos y archivos de Microsoft Office PowerPoint®, por ejemplo: 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 compatibles con macros, potx para plantillas de presentaciones de Microsoft Office PowerPoint 2007, potm para plantillas de presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007, ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 compatibles con macros y ppam para complementos de Microsoft Office PowerPoint 2007 compatibles con macros

md* – documentos y archivos de Microsoft Office Access®, por ejemplo: mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: una diapositiva de Microsoft PowerPoint 2007

sldm: una diapositiva de Microsoft PowerPoint 2007 compatible con macros

thmx: un tema de Microsoft Office 2007

Apéndice 4. Tipos de archivo para el filtro de adjuntos de Protección contra amenazas de correo

Tenga en cuenta que el formato real de un archivo puede no coincidir con la extensión de su nombre de archivo.

Si habilita el filtrado de objetos adjuntos a mensajes de correo electrónico, el componente Protección contra amenazas de correo puede renombrar o eliminar archivos con las extensiones siguientes:

com: archivo ejecutable de una aplicación que no supera los 64 KB

exe: archivo ejecutable o archivo autoextraíble

sys: archivo de sistema de Microsoft Windows

prg – texto de programas para dBase™, Clipper o Microsoft FoxPro Visual®, o un programa WAVmaker

bin: archivo binario

bat: archivo de lote

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para el DOS), OS/2

dpl: biblioteca Borland Delphi comprimida

dll: biblioteca de vínculos dinámicos

scr: pantalla inicial de Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto de Microsoft OLE (Object Linking and Embedding)

tsp: programa que se ejecuta en modo de tiempo dividido

drv: controlador de dispositivos

vxd: controlador de dispositivos virtuales de Microsoft Windows

pif: archivo de información del programa

lnk: archivo de vínculos de Microsoft Windows

reg: archivo de claves del registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de la configuración para Microsoft Windows, Windows NT y algunas aplicaciones

cla: clase de Java

vbs – script de Visual Basic®

vbe: extensión de video del BIOS

js, jse: texto fuente de JavaScript

htm: documento del hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta – programa de hipertexto para Microsoft Internet Explorer®

asp: script de Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script que se integra en archivos HTML

wsh: archivo de Microsoft Windows Script Host

wsf: script de Microsoft Windows

the: archivo del tapiz de escritorio de Microsoft Windows 95

hlp: archivo de ayuda de Windows

msg: mensaje de correo electrónico de Microsoft Mail

plg: mensaje de correo electrónico

mbx: mensaje de correo electrónico guardado de Microsoft Office Outlook

doc*: documentos de Microsoft Office Word, por ejemplo: doc para documentos de Microsoft Office Word, docx para documentos de Microsoft Office Word 2007 compatibles con XML, y docm para documentos de Microsoft Office Word 2007 compatibles con macros

dot*: plantillas de documentos de Microsoft Office Word, por ejemplo: dot para plantillas de documentos de Microsoft Office Word, dotx para plantillas documentos de Microsoft Office Word 2007 y dotm para plantillas de documentos de Microsoft Office Word 2007 compatibles con macros

fpm: programa de base de datos, archivo de inicio de Microsoft Visual FoxPro

rtf: documento con formato de texto enriquecido

shs: fragmento del manipulador de objetos de desecho de la Shell de Windows

dwg – base de datos de planos de AutoCAD®

msi: paquete de Microsoft Windows Installer

otm: proyecto de VBA para Microsoft Office Outlook

pdf: documento de Adobe Acrobat

swf – objeto del paquete de Shockwave® Flash

jpg, jpeg: formato de gráfico de imagen comprimida

emf: archivo con formato de metarchivo mejorado

ico: archivo de icono de objeto

ov? - archivos ejecutables de Microsoft Office Word

xl*: documentos y archivos de Microsoft Office Excel, por ejemplo: xls, la extensión correspondiente a Microsoft Office Excel, xlc para diagramas, xlt para plantillas de documentos, xlsx para libros de Microsoft Office Excel 2007, xltm para libros de Microsoft Office Excel 2007 compatibles con macros, xlsb para libros 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 compatibles con macros y xlam para complementos de Microsoft Office Excel 2007 compatibles con macros

pp* – documentos y archivos de Microsoft Office PowerPoint®, por ejemplo: 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 compatibles con macros, potx para plantillas de presentaciones de Microsoft Office PowerPoint 2007, potm para plantillas de presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007, ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 compatibles con macros y ppam para complementos de Microsoft Office PowerPoint 2007 compatibles con macros

md* – documentos y archivos de Microsoft Office Access®, por ejemplo: mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: una diapositiva de Microsoft PowerPoint 2007

sldm: una diapositiva de Microsoft PowerPoint 2007 compatible con macros

thmx: un tema de 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 (Seguridad de la capa de transporte) 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`	Activación de 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`
	Actualización de bases de datos y módulos de software de la aplicación.

`downloads.upd.kaspersky.com` Protocolo: `HTTPS` Puerto: `443`	• Actualización de bases de datos y módulos de software de la aplicación. • Verificación del acceso a los servidores de Kaspersky. Si el acceso a los servidores mediante el DNS del sistema no es posible, la aplicación utiliza el DNS público. Esto es necesario para asegurarse de que las bases de datos antivirus estén actualizadas y se mantenga el nivel de seguridad del 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 la dirección IP pública 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 cuando se utiliza HTTPS. Si Kaspersky Endpoint Security utiliza un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio correspondiente. Si desea evitar que Kaspersky Endpoint Security utilice un servidor DNS público, comuníquese con el Servicio de soporte técnico para obtener 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 se está ejecutando Protección contra amenazas web.

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`
	Actualización de bases de datos y módulos de software 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`
	Al usar 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`
	Al usar Kaspersky Security Network.

`click.kaspersky.com`
`redirect.kaspersky.com`
Protocolo: `HTTPS`
Puerto: `443`
	Haga clic en los vínculos de la interfaz.

Configuración, usada para el cifrado

Dirección	Descripción

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocolo: `HTTP`
Puerto: `80`
	Infraestructura de clave pública (PKI).

Apéndice 6. Eventos de la aplicación

La información sobre la operación de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la finalización de cada tarea de análisis de malware, la tarea de actualización, la tarea de comprobación de integridad y la operación general de la aplicación se inscribe en el registro de eventos de Kaspersky Security Center y 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 un 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`: *Error funcional*, `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 se pueden crear con Kaspersky Endpoint Security para Windows así como con otras aplicaciones de Kaspersky (por ejemplo, Kaspersky Security for Windows Server). Los eventos generales tienen un id. más complejo, 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 caducó

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	`201`
Id. de eventos de Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Licencia a punto de caducar

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	`203`

Id. de eventos de Kaspersky Security Center	000000cb
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Faltan las bases de datos o están dañadas

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	206
Id. de eventos de Kaspersky Security Center	000000ce
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Las bases de datos están obsoletas

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	207
Id. de eventos de Kaspersky Security Center	000000cf
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La ejecución automática de la aplicación está deshabilitada

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	209
Id. de eventos de Kaspersky Security Center	000000d1
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de activación

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	229
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó una amenaza activa; ejecute la Desinfección avanzada

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	231
Id. de eventos de Kaspersky Security Center	000000e7

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Servidores de KSN no disponibles

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	2023
Id. de eventos de Kaspersky Security Center	000007e7
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No hay suficiente espacio en el almacenamiento en la cuarentena

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	343
Id. de eventos de Kaspersky Security Center	00000157
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto no restaurado de la Cuarentena

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	346
Id. de eventos de Kaspersky Security Center	0000015a
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se eliminó el objeto de la cuarentena

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	348
Id. de eventos de Kaspersky Security Center	0000015c
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La aplicación estableció una conexión con un sitio web que tiene un certificado que no es de confianza

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	57
Id. de eventos de Kaspersky Security Center	00000039

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al verificar una conexión cifrada. El dominio se agregó a la lista de exclusiones

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	`60`
Id. de eventos de Kaspersky Security Center	`0000003c`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto malicioso detectado (bases de datos locales)

Categoría	!
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Prevención de intrusiones en el host Detección de comportamiento Anticifrador Prevención de exploits Análisis de malware
Id. del evento de Windows	`302`
Id. de eventos 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. Cuando se detecta un cifrado externo de las carpetas compartidas, la aplicación muestra la ruta hacia 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 la 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.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto malicioso detectado (KSN)

Categoría	!
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Prevención de intrusiones en el host Detección de comportamiento Anticifrador Prevención de exploits Análisis de malware
Id. del evento de Windows	`302`
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede desinfectar

Categoría	!
Componente	Protección contra amenazas de archivo Protección contra amenazas de correo Prevención de intrusiones en el host Detección de comportamiento Anticifrador Análisis de malware
Id. del evento de Windows	`312`
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede eliminar

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Prevención de intrusiones en el host Detección de comportamiento Anticifrador Análisis de malware
Id. del evento de Windows	`313`
Id. de eventos de Kaspersky Security Center	`00000139`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de procesamiento

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Prevención de intrusiones en el host Protección vía AMSI Análisis de malware
Id. del evento de Windows	`317`
Id. de eventos de Kaspersky Security Center	`0000013d`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Proceso finalizado

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Prevención de intrusiones en el host Detección de comportamiento Análisis de malware
Id. del evento de Windows	`452`
Id. de eventos de Kaspersky Security Center	`000001c4`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede finalizar el proceso

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Prevención de intrusiones en el host Detección de comportamiento Análisis de malware
Id. del evento de Windows	`453`
Id. de eventos de Kaspersky Security Center	`000001c5`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Vínculo peligroso bloqueado

Categoría	!
Componente	Protección contra amenazas web
Id. del evento de Windows	362
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Vínculo peligroso abierto

Categoría	!
Componente	Protección contra amenazas web
Id. del evento de Windows	363
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó un vínculo peligroso que ya se había abierto

Categoría	!
Componente	Protección contra amenazas web
Id. del evento de Windows	1201
Id. de eventos 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 la 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.

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acción del proceso bloqueada

Categoría	!
Componente	Control de anomalías adaptativo
Id. del evento de Windows	`2200`
Id. de eventos 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 la 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).
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Teclado no autorizado

Categoría	!
Componente	Prevención de ataques BadUSB
Id. del evento de Windows	`2051`
Id. de eventos de Kaspersky Security Center	`00000803`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La solicitud de AMSI se bloqueó

Categoría	!
Componente	Protección vía AMSI
Id. del evento de Windows	`2200`
Id. de eventos de Kaspersky Security Center	`00000898`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Actividad de red bloqueada

Categoría	!
Componente	Firewall
Id. del evento de Windows	`602`
Id. de eventos de Kaspersky Security Center	`00000329`

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Ataque de red detectado

Categoría	!
Componente	Protección contra amenazas de red
Id. del evento de Windows	`651`
Id. de eventos 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 a la 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 se dirigió el ataque de red. La dirección IP se indica en el orden de bytes del host. Por ejemplo, `2886729929` para `172.16.0.201`.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Inicio de aplicación prohibido

Categoría	!
Componente	Control de aplicaciones
Id. del evento de Windows	`702`
Id. de eventos 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 la categoría creada 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 del 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 tratando de ejecutar.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se inició un proceso prohibido antes del inicio de Kaspersky Endpoint Security

Categoría	!
Componente	Control de aplicaciones
Id. del evento de Windows	`710`
Id. de eventos de Kaspersky Security Center	`000002c6`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso denegado (bases de datos locales)

Categoría	ⓘ
Componente	Control web
Id. del evento de Windows	752
Id. de eventos de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parámetros de eventos	• GNRL_EA_PARAM_1 es la dirección 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso denegado (KSN)

Categoría	ⓘ
Componente	Control web
Id. del evento de Windows	752
Id. de eventos de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parámetros de eventos	• GNRL_EA_PARAM_1 es la dirección 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Operación con el dispositivo prohibida

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	802
Id. de eventos de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el Id. de hardware (HWID). • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión de red bloqueada

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	809
Id. de eventos de Kaspersky Security Center	00000329
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al actualizar el componente

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1011
Id. de eventos de Kaspersky Security Center	000003f3
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al distribuir las actualizaciones de componentes

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1012
Id. de eventos de Kaspersky Security Center	000003f4
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error de actualización local

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1014
Id. de eventos de Kaspersky Security Center	000003f6
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error de actualización por red

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1015
Id. de eventos de Kaspersky Security Center	000003f7
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

No se pueden iniciar dos tareas al mismo tiempo

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1017
Id. de eventos de Kaspersky Security Center	000003f9
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al comprobar las bases de datos y los módulos de la aplicación

Categoría	⊙
Componente	Actualización
Id. del evento de Windows	1018
Id. de eventos de Kaspersky Security Center	000003fa
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de interacción con Kaspersky Security Center

Categoría	⊙
Componente	Actualización
Id. del evento de Windows	1019
Id. de eventos de Kaspersky Security Center	000003fb
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se actualizaron todos los componentes

Categoría	⊙
Componente	Actualización
Id. del evento de Windows	1021
Id. de eventos de Kaspersky Security Center	000003fd
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La actualización se completó correctamente. Error en la distribución de actualizaciones

Categoría	⊙
Componente	Actualización
Id. del evento de Windows	1023
Id. de eventos de Kaspersky Security Center	000003ff
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error interno de tarea

Categoría	⊙
Componente	Auditoría del sistema
Id. del evento de Windows	101
Id. de eventos de Kaspersky Security Center	00000065
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

No se pudo instalar el parche

Categoría	!
Componente	Actualización
Id. del evento de Windows	`2153`
Id. de eventos de Kaspersky Security Center	`00000869`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo revertir el parche

Categoría	!
Componente	Actualización
Id. del evento de Windows	`2156`
Id. de eventos de Kaspersky Security Center	`0000086c`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al implementar las reglas de cifrado o descifrado de archivos

Categoría	!
Componente	Cifrado de datos
Id. del evento de Windows	`904`
Id. de eventos de Kaspersky Security Center	`00000388`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de cifrado o descifrado de archivos

Categoría	!
Componente	Cifrado de datos
Id. del evento de Windows	`912`
Id. de eventos 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 la causa del error. • `GNRL_EA_PARAM_3` es el tipo del dispositivo.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso al archivo bloqueado

Categoría	!
Componente	Cifrado de datos
Id. del evento de Windows	`940`

Id. de eventos 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` es el nombre del archivo ejecutable de la aplicación (por ejemplo, chrome.exe) que intenta acceder al archivo.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error al habilitar el modo portátil

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	`951`
Id. de eventos de Kaspersky Security Center	`000003b7`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al deshabilitar el modo portátil

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	`953`
Id. de eventos de Kaspersky Security Center	`000003b9`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al crear el paquete cifrado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	`931`
Id. de eventos de Kaspersky Security Center	`000003a3`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de cifrado o descifrado del dispositivo

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	`1305`
Id. de eventos de Kaspersky Security Center	`00000519`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo cargar el módulo de cifrado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1311
Id. de eventos de Kaspersky Security Center	0000051f
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La tarea de administración de cuentas del Agente de autenticación finalizó con un error

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1340
Id. de eventos de Kaspersky Security Center	0000053c
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede aplicar la directiva

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	1312
Id. de eventos de Kaspersky Security Center	00000520
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo realizar la actualización de FDE

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1342
Id. de eventos de Kaspersky Security Center	0000053e
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo revertir la actualización de FDE (para más información, consulte la ayuda en línea de Kaspersky Endpoint Security para Windows)

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1344
Id. de eventos de Kaspersky Security Center	00000540
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Servidor de Kaspersky Anti Targeted Attack Platform no disponible

Categoría	!
Componente	Endpoint Sensor
Id. del evento de Windows	2100
Id. de eventos de Kaspersky Security Center	00000834
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo eliminar el objeto

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2252
Id. de eventos de Kaspersky Security Center	000008cc
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto no está en cuarentena (Sandbox)

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2603
Id. de eventos de Kaspersky Security Center	00000a2b
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Ocurrió un error interno

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2607
Id. de eventos de Kaspersky Security Center	00000a2f
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado del servidor de Sandbox no válido

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2613
Id. de eventos de Kaspersky Security Center	00000a35
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El nodo Sandbox no está disponible

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2614
Id. de eventos de Kaspersky Security Center	00000a36
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al procesar el objeto en Sandbox

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2617
Id. de eventos de Kaspersky Security Center	00000a39
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se superó la carga máxima de Sandbox

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2618
Id. de eventos de Kaspersky Security Center	00000a3a
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

IOC encontrado

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2651
Id. de eventos de Kaspersky Security Center	00000a5b
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se produjo un error en la verificación de la licencia de Sandbox

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2620
Id. de eventos de Kaspersky Security Center	00000a3c
Registros 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

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2623
Id. de eventos de Kaspersky Security Center	00000a3e
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al crear la tarea de Sandbox

Categoría	!
Componente	Sandbox
Id. del evento de Windows	2621
Id. de eventos de Kaspersky Security Center	00000a3d
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó el inicio del objeto

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2553
Id. de eventos de Kaspersky Security Center	000009f9
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó el inicio del proceso

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2551
Id. de eventos de Kaspersky Security Center	000009f7
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó la ejecución del script

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2559
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto no está en cuarentena (Endpoint Detection and Response)

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2556
Id. de eventos de Kaspersky Security Center	000009fc
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El inicio del proceso no está bloqueado

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2561
Id. de eventos de Kaspersky Security Center	00000a01
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto no está bloqueado

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2562
Id. de eventos de Kaspersky Security Center	00000a02
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La ejecución de script no está bloqueada

Categoría	!
Componente	Endpoint Detection and Response
Id. del evento de Windows	2563
Id. de eventos de Kaspersky Security Center	00000a03
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al cambiar los componentes de la aplicación

Categoría	!
Componente	Auditoría del sistema
Id. del evento de Windows	1401
Id. de eventos de Kaspersky Security Center	00000579
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Hay patrones de posibles ataques de fuerza bruta en el sistema

Categoría	ⓘ
Componente	Inspección de registros
Id. del evento de Windows	`2800`
Id. de eventos de Kaspersky Security Center	`00000af0`
Registros 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

Categoría	ⓘ
Componente	Inspección de registros
Id. del evento de Windows	`2801`
Id. de eventos de Kaspersky Security Center	`00000af1`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectaron acciones atípicas de parte de un nuevo servicio instalado

Categoría	ⓘ
Componente	Inspección de registros
Id. del evento de Windows	`2802`
Id. de eventos de Kaspersky Security Center	`00000af2`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó un inicio de sesión atípico que usa credenciales explícitas

Categoría	ⓘ
Componente	Inspección de registros
Id. del evento de Windows	`2803`
Id. de eventos de Kaspersky Security Center	`00000af3`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema

Categoría	ⓘ
Componente	Inspección de registros
Id. del evento de Windows	`2804`
Id. de eventos de Kaspersky Security Center	`00000af4`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios

Categoría	!
Componente	Inspección de registros
Id. del evento de Windows	2805
Id. de eventos de Kaspersky Security Center	00000af5
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó una actividad inusual durante un inicio de sesión en la red

Categoría	!
Componente	Inspección de registros
Id. del evento de Windows	2806
Id. de eventos de Kaspersky Security Center	00000af6
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se activó una regla de Inspección de registros

Categoría	!
Componente	Inspección de registros
Id. del evento de Windows	2807
Id. de eventos de Kaspersky Security Center	00000af7
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Un evento atípico se produce con demasiada frecuencia. Se inició el agregado de eventos

Categoría	!
Componente	Inspección de registros
Id. del evento de Windows	2808
Id. de eventos de Kaspersky Security Center	00000af8
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe sobre un evento atípico en el periodo de agregado

Categoría	!
Componente	Inspección de registros
Id. del evento de Windows	2809
Id. de eventos de Kaspersky Security Center	00000af9
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectarse al servidor de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
Id. del evento de Windows	2850
Id. de eventos de Kaspersky Security Center	00000b22
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
Id. del evento de Windows	2851
Id. de eventos de Kaspersky Security Center	00000b23
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
Id. del evento de Windows	2852
Id. de eventos de Kaspersky Security Center	00000b24
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectarse al servidor de respuesta de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	2858
Id. de eventos de Kaspersky Security Center	00000b22
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de repuesta de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	2859
Id. de eventos de Kaspersky Security Center	00000b23
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de repuesta de EDR Expert

Categoría	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	2860
Id. de eventos de Kaspersky Security Center	00000b24
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectarse con el servidor de recolección de telemetría de EDR Expert

Categoría	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	2854
Id. de eventos de Kaspersky Security Center	00000b22
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de recolección de telemetría de EDR Expert

Categoría	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	2855
Id. de eventos de Kaspersky Security Center	00000b23
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de recolección de telemetría de EDR Expert

Categoría	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	2856
Id. de eventos de Kaspersky Security Center	00000b24
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al conectarse con el servidor de NDR

Categoría	!
Componente	Network Detection and Response (KATA)
Id. del evento de Windows	3080
Id. de eventos de Kaspersky Security Center	00000c08

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de NDR

Categoría	⊗
Componente	Network Detection and Response (KATA)
Id. del evento de Windows	3081
Id. de eventos de Kaspersky Security Center	00000c09
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de NDR

Categoría	⊗
Componente	Network Detection and Response (KATA)
Id. del evento de Windows	3082
Id. de eventos de Kaspersky Security Center	00000c0a
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Su dispositivo está conectado a un Servidor de administración no confiable. Comuníquese con el administrador

Categoría	⊗
Componente	Protección de la conexión del Servidor de administración
Id. del evento de Windows	3301
Id. de eventos de Kaspersky Security Center	00000ce5
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó el cambio de un archivo o una carpeta

Categoría	ⓘ / ⚠ / ⊗
Componente	Control de integridad del sistema
Id. del evento de Windows	2950
Id. de eventos de Kaspersky Security Center	00000b86
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El objeto cambia con demasiada frecuencia. Comenzó la incorporación de eventos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2955
Id. de eventos de Kaspersky Security Center	00000b8b
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe sobre la modificación de objetos para el periodo de incorporación

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2956
Id. de eventos de Kaspersky Security Center	00000b8c
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El alcance del monitoreo incluye objetos incorrectos

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2953
Id. de eventos de Kaspersky Security Center	00000b89
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó el cambio del registro

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2951
Id. de eventos de Kaspersky Security Center	00000b87
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se detectó una conexión/desconexión de dispositivos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema

Id. del evento de Windows	2952
Id. de eventos de Kaspersky Security Center	00000b88
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El alcance del monitoreo incluye objetos incorrectos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2903
Id. de eventos de Kaspersky Security Center	00000b89
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Los intentos de realizar las operaciones restringidas con el objeto son demasiados. Se inició la incorporación de eventos

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2963
Id. de eventos de Kaspersky Security Center	00000b93
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó una operación con los archivos del alcance de supervisión

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2959
Id. de eventos de Kaspersky Security Center	00000b8f
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se bloqueó la modificación del registro

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2960
Id. de eventos de Kaspersky Security Center	00000b90
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Error de procesamiento

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2954
Id. de eventos de Kaspersky Security Center	00000b8a
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de integridad del sistema: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2964
Id. de eventos de Kaspersky Security Center	00000b94
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de aplicaciones: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente

Categoría	ⓘ
Componente	Control de aplicaciones
Id. del evento de Windows	711
Id. de eventos de Kaspersky Security Center	000002c7
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de dispositivos: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	810

Id. de eventos de Kaspersky Security Center	0000032a
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control web: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente

Categoría	!
Componente	Control web
Id. del evento de Windows	757
Id. de eventos de Kaspersky Security Center	000002f5
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Control de anomalías adaptativo: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente

Categoría	!
Componente	Control de anomalías adaptativo
Id. del evento de Windows	504
Id. de eventos de Kaspersky Security Center	000001f8
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Inspección de registros: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente

Categoría	!
Componente	Inspección de registros
Id. del evento de Windows	2810
Id. de eventos de Kaspersky Security Center	00000afa
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo conectar con el Servidor de integración durante más de 6 horas. Compruebe el estado del Servidor de Integración y la configuración de red

Categoría	!
Componente	Light Agent
Id. del evento de Windows	3103
Id. de eventos de Kaspersky Security Center	00000c1f
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La SVM no está disponible

Categoría	!
Componente	Light Agent
Id. del evento de Windows	3151
Id. de eventos de Kaspersky Security Center	00000c4f
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó un objeto malicioso. Desinfección avanzada debe iniciarse en una plantilla de máquina virtual

Categoría	!
Componente	Light Agent
Id. del evento de Windows	3182
Id. de eventos de Kaspersky Security Center	00000c6e
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó la conexión de red establecida mediante el protocolo obsoleto

Categoría	!
Componente	Protección
Id. del evento de Windows	75
Id. de eventos de Kaspersky Security Center	0000004b
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de conexión del servidor de KUMA

Categoría	!
Componente	Integración con KUMA
Id. del evento de Windows	2854
Id. de eventos de Kaspersky Security Center	00000b26
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del servidor de KUMA

Categoría	!
Componente	Integración con KUMA
Id. del evento de Windows	2855
Id. de eventos de Kaspersky Security Center	00000b27
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Certificado no válido del agente en el servidor de KUMA

Categoría	ⓘ
Componente	Integración con KUMA
Id. del evento de Windows	2856
Id. de eventos de Kaspersky Security Center	00000b28
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error funcional

No se puede realizar la tarea

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	212
Id. de eventos de Kaspersky Security Center	000000d4
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La configuración de la tarea no es válida y no se aplicó

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	707
Id. de eventos de Kaspersky Security Center	000002c3
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Advertencia

La aplicación se cerró en forma forzosa durante una sesión anterior

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	237
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La licencia caducará pronto

Categoría	⚠
Componente	Auditoría del sistema

Id. del evento de Windows	204
Id. de eventos de Kaspersky Security Center	000000cc
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Las bases de datos están desactualizadas

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	208
Id. de eventos de Kaspersky Security Center	000000d0
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Actualizaciones automáticas deshabilitadas

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	210
Id. de eventos de Kaspersky Security Center	000000d2
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Autoprotección deshabilitada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	211
Id. de eventos de Kaspersky Security Center	000000d3
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Componentes de protección deshabilitados

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	214
Id. de eventos de Kaspersky Security Center	000000d6
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El equipo está funcionando en modo seguro

Categoría	⚠
Componente	Auditoría del sistema

Id. del evento de Windows	215
Id. de eventos de Kaspersky Security Center	000000d7
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Hay archivos sin procesar

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	216
Id. de eventos de Kaspersky Security Center	000000d8
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Directiva de grupo aplicada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	219
Id. de eventos de Kaspersky Security Center	000000db
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Tarea detenida

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	222
Id. de eventos de Kaspersky Security Center	000000de
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para completar la actualización, salga de la aplicación y ábrala nuevamente

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	224
Id. de eventos de Kaspersky Security Center	0000057b
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Es necesario reiniciar el equipo

Categoría	⚠
Componente	Auditoría del sistema

Id. del evento de Windows	225
Id. de eventos de Kaspersky Security Center	000000e1
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La licencia permite usar componentes que no se han instalado

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	226
Id. de eventos de Kaspersky Security Center	000000e2
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Desinfección avanzada iniciada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	232
Id. de eventos de Kaspersky Security Center	000000e8
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Desinfección avanzada completada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	233
Id. de eventos de Kaspersky Security Center	000000e9
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Clave de reserva incorrecta

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	230
Id. de eventos de Kaspersky Security Center	000000e6
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La suscripción está por caducar

Categoría	⚠
Componente	Auditoría del sistema

Id. del evento de Windows	240
Id. de eventos de Kaspersky Security Center	000000f0
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Bloqueado

Categoría	⚠
Componente	Detección de comportamiento Anticifrador Prevención de exploits Protección contra amenazas web
Id. del evento de Windows	331
Id. de eventos 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. Cuando se detecta un cifrado externo de las carpetas compartidas, la aplicación muestra la ruta hacia 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 la 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.
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La configuración del sistema operativo no permite controlar el acceso a las redes Wi-Fi

Categoría	⚠
Componente	Control de dispositivos
Id. del evento de Windows	249
Id. de eventos de Kaspersky Security Center	000000f9
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto no restaurado de Copia de seguridad

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	336
Id. de eventos de Kaspersky Security Center	00000150

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Actividad de red sospechosa detectada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`2001`
Id. de eventos de Kaspersky Security Center	`000007d1`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión cifrada terminada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`250`
Id. de eventos de Kaspersky Security Center	`000007d3`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La participación en KSN está deshabilitada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`2021`
Id. de eventos de Kaspersky Security Center	`000007e5`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El procesamiento de algunas funciones del SO está deshabilitado

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`245`
Id. de eventos de Kaspersky Security Center	`000000f5`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El almacenamiento de cuarentena tiene espacio insuficiente

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`344`
Id. de eventos de Kaspersky Security Center	`00000158`

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión de red bloqueada

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`809`
Id. de eventos de Kaspersky Security Center	`00000abe`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se puede crear una copia de seguridad

Categoría	⚠
Componente	Protección contra amenazas de archivo Protección contra amenazas de correo Prevención de intrusiones en el host Protección vía AMSI Análisis de malware
Id. del evento de Windows	`314`
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Categoría	⚠
Componente	Protección contra amenazas de archivo Detección de comportamiento Anticifrador Prevención de intrusiones en el host Análisis de malware
Id. del evento de Windows	`310`
Id. de eventos de Kaspersky Security Center	`00000136`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto cifrado

Categoría	⚠
Componente	Prevención de intrusiones en el host
Id. del evento de Windows	`320`
Id. de eventos de Kaspersky Security Center	`00000140`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto dañado

Categoría	⚠
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Prevención de intrusiones en el host Análisis de malware
Id. del evento de Windows	`321`
Id. de eventos de Kaspersky Security Center	`00000141`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se detectó software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales (bases locales)

Categoría	⚠
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Prevención de intrusiones en el host Protección vía AMSI Detección de comportamiento Anticifrador Anticifrador Análisis de malware
Id. del evento de Windows	`303`
Id. de eventos 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`).
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales (KSN)

Categoría	⚠
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Prevención de intrusiones en el host Protección vía AMSI Detección de comportamiento Anticifrador Anticifrador Análisis de malware
Id. del evento de Windows	`303`
Id. de eventos 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`).
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado

Categoría	⚠
Componente	Protección contra amenazas de archivo Protección contra amenazas de correo Prevención de intrusiones en el host Prevención de exploits Detección de comportamiento Anticifrador Análisis de malware
Id. del evento de Windows	`307`
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto desinfectado

Categoría	⚠
Componente	Protección contra amenazas de archivo Protección contra amenazas de correo Prevención de intrusiones en el host Análisis de malware
Id. del evento de Windows	`306`
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto se desinfectará al reiniciar

Categoría	⚠
Componente	Prevención de intrusiones en el host Protección contra amenazas de archivo Análisis de malware
Id. del evento de Windows	`324`
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El objeto se eliminará al reiniciar

Categoría	⚠
Componente	Detección de comportamiento Anticifrador Prevención de exploits Prevención de intrusiones en el host Protección contra amenazas de archivo Análisis de malware
Id. del evento de Windows	`323`
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto eliminado en respuesta a la configuración

Categoría	⚠
Componente	Protección contra amenazas de correo
Id. del evento de Windows	342
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Reversión completada

Categoría	⚠
Componente	Protección contra amenazas de archivo Detección de comportamiento Anticifrador Prevención de exploits Análisis de malware
Id. del evento de Windows	455
Id. de eventos de Kaspersky Security Center	000001c7
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó la descarga del objeto

Categoría	⚠
Componente	Protección contra amenazas web
Id. del evento de Windows	341
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error de autorización de teclado

Categoría	⚠
Componente	Prevención de ataques BadUSB
Id. del evento de Windows	2052
Id. de eventos de Kaspersky Security Center	00000804

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El resultado del análisis del objeto se envió a una aplicación de otro desarrollador

Categoría	⚠
Componente	Protección vía AMSI
Id. del evento de Windows	`1512`
Id. de eventos 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 la 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Configuración de tarea aplicada correctamente

Categoría	⚠
Componente	Control de aplicaciones
Id. del evento de Windows	`708`
Id. de eventos de Kaspersky Security Center	`000002c4`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Advertencia acerca de contenido indeseado (bases de datos locales)

Categoría	⚠
Componente	Control web
Id. del evento de Windows	`708`
Id. de eventos de Kaspersky Security Center	`GNRL_EV_WEB_URL_WARNING`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es la dirección 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Advertencia acerca de contenido indeseado (KSN)

Categoría	⚠
Componente	Control web

Id. del evento de Windows	708
Id. de eventos de Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parámetros de eventos	• GNRL_EA_PARAM_1 es la dirección 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.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se accedió a contenido indeseado tras una advertencia

Categoría	⚠
Componente	Control web
Id. del evento de Windows	754
Id. de eventos de Kaspersky Security Center	000002f2
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Acceso temporal al dispositivo activado

Categoría	⚠
Componente	Control de dispositivos
Id. del evento de Windows	803
Id. de eventos de Kaspersky Security Center	000002f2
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Operación cancelada por el usuario

Categoría	⚠
Componente	Actualización
Id. del evento de Windows	1016
Id. de eventos de Kaspersky Security Center	000003f8
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El usuario optó por no implementar la directiva de cifrado

Categoría	⚠
Componente	Cifrado de datos
Id. del evento de Windows	1306
Id. de eventos de Kaspersky Security Center	0000051a
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se interrumpió la implementación de las reglas de cifrado o descifrado de archivos

Categoría	⚠
Componente	Cifrado de datos
Id. del evento de Windows	903
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado de archivos interrumpido

Categoría	⚠
Componente	Cifrado de datos
Id. del evento de Windows	914
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado del dispositivo interrumpido

Categoría	⚠
Componente	Cifrado de datos
Id. del evento de Windows	1303
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Error al instalar o actualizar los controladores de Cifrado de disco de Kaspersky en la imagen de WinRE

Categoría	⚠
Componente	Cifrado de datos
Id. del evento de Windows	1345
Id. de eventos de Kaspersky Security Center	00000541
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al comprobar la firma del módulo

Categoría	⚠
Componente	Comprobación de integridad del sistema
Id. del evento de Windows	2002
Id. de eventos de Kaspersky Security Center	000007d2
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó el inicio de la aplicación

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2105
Id. de eventos de Kaspersky Security Center	00000839
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó la apertura del documento

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2106
Id. de eventos de Kaspersky Security Center	0000083a
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador del servidor de Kaspersky Anti Targeted Attack Platform finalizó el proceso

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2112
Id. de eventos de Kaspersky Security Center	00000840
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador del servidor de Kaspersky Anti Targeted Attack Platform finalizó la aplicación

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2113
Id. de eventos de Kaspersky Security Center	00000841
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador del servidor de Kaspersky Anti Targeted Attack Platform eliminó el archivo o flujo

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2111
Id. de eventos de Kaspersky Security Center	0000083f
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador restauró el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2110
Id. de eventos de Kaspersky Security Center	0000083e
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El administrador colocó el archivo en la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2109
Id. de eventos de Kaspersky Security Center	0000083d
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se bloqueó la actividad de red de las aplicaciones de terceros

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2107
Id. de eventos de Kaspersky Security Center	0000083b
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se desbloqueó la actividad de red de las aplicaciones de terceros

Categoría	⚠
Componente	Endpoint Sensor
Id. del evento de Windows	2108
Id. de eventos de Kaspersky Security Center	0000083c
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto se eliminará al reiniciar (Sandbox)

Categoría	⚠
Componente	Sandbox
Id. del evento de Windows	2605
Id. de eventos de Kaspersky Security Center	00000a2d
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El tamaño total de las tareas de análisis superó el límite

Categoría	⚠
Componente	Sandbox
Id. del evento de Windows	2612
Id. de eventos de Kaspersky Security Center	00000a34
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se permitió el inicio del objeto, evento registrado

Categoría	⚠
Componente	Endpoint Detection and Response
Id. del evento de Windows	2553
Id. de eventos de Kaspersky Security Center	000009fa
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se permitió el inicio del proceso, evento registrado

Categoría	⚠
Componente	Endpoint Detection and Response
Id. del evento de Windows	2554
Id. de eventos de Kaspersky Security Center	000009f8
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto se eliminará al reiniciar (Endpoint Detection and Response)

Categoría	⚠
Componente	Endpoint Detection and Response
Id. del evento de Windows	2558
Id. de eventos de Kaspersky Security Center	000009fe
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Aislamiento de la red

Categoría	⚠
Componente	Endpoint Detection and Response
Id. del evento de Windows	2700
Id. de eventos de Kaspersky Security Center	00000a8c
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Finalización del aislamiento de la red

Categoría	⚠
Componente	Endpoint Detection and Response
Id. del evento de Windows	`2701`
Id. de eventos de Kaspersky Security Center	`00000a8d`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se debe reiniciar para completar la tarea

Categoría	⚠
Componente	Auditoría del sistema
Id. del evento de Windows	`225`
Id. de eventos de Kaspersky Security Center	`0000057b`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje de bloqueo del inicio de una aplicación para el administrador

Categoría	⚠
Componente	Control de aplicaciones
Id. del evento de Windows	`503`
Id. de eventos 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 del 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 tratando de ejecutar.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje de bloqueo del acceso a un dispositivo para el administrador

Categoría	⚠
Componente	Control de dispositivos
Id. del evento de Windows	`804`
Id. de eventos 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 el Id. de hardware (HWID). • `GNRL_EA_PARAM_2` es el nombre del usuario de la sesión.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje de bloqueo del acceso a una página web para el administrador

Categoría	⚠
Componente	Control web
Id. del evento de Windows	755
Id. de eventos 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 dirección URL. • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Conexión del dispositivo bloqueada

Categoría	⚠
Componente	Control de dispositivos
Id. del evento de Windows	807
Id. de eventos de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parámetros de eventos	• GNRL_EA_PARAM_1 es el Id. de hardware (HWID). • GNRL_EA_PARAM_2 es el nombre del usuario de la sesión.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje de bloqueo de actividad de aplicación enviado al administrador

Categoría	⚠
Componente	Monitor de integridad de archivos
Id. del evento de Windows	2901
Id. de eventos de Kaspersky Security Center	00000b55
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Categoría	⚠
Componente	Monitor de integridad de archivos
Id. del evento de Windows	2900
Id. de eventos de Kaspersky Security Center	00000b54
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Categoría	⚠
Componente	Control de anomalías adaptativo
Id. del evento de Windows	503

Id. de eventos 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 la 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).
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se permite iniciar la aplicación cliente del servicio en la nube

Categoría	⚠
Componente	Cloud Discovery
Id. del evento de Windows	`2212`
Id. de eventos de Kaspersky Security Center	`000008a4`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se permite acceder al servicio en la nube

Categoría	⚠
Componente	Cloud Discovery
Id. del evento de Windows	`2213`
Id. de eventos de Kaspersky Security Center	`000008a5`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó el cambio de un archivo o una carpeta

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	`2950`
Id. de eventos de Kaspersky Security Center	`00000b86`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El objeto cambia con demasiada frecuencia. Comenzó la incorporación de eventos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2955
Id. de eventos de Kaspersky Security Center	00000b8b
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe sobre la modificación de objetos para el periodo de incorporación

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2956
Id. de eventos de Kaspersky Security Center	00000b8c
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se detectó el cambio del registro

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2951
Id. de eventos de Kaspersky Security Center	00000b87
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se detectó una conexión/desconexión de dispositivos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2952
Id. de eventos de Kaspersky Security Center	00000b88
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El alcance del monitoreo incluye objetos incorrectos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2903
Id. de eventos de Kaspersky Security Center	00000b89
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se permitió la operación prohibida en modo de prueba

Categoría	⚠
Componente	Control de integridad del sistema
Id. del evento de Windows	2961
Id. de eventos de Kaspersky Security Center	00000b91
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo conectar con el Servidor de integración durante más de 30 minutos. Compruebe el estado del Servidor de integración y la configuración de red

Categoría	⚠
Componente	Light Agent
Id. del evento de Windows	3102
Id. de eventos de Kaspersky Security Center	00000c1e
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

No se pudo conectar con el Servidor de integración. Compruebe el estado del Servidor de integración y la configuración de red

Categoría	⚠
Componente	Light Agent
Id. del evento de Windows	3101
Id. de eventos de Kaspersky Security Center	00000c1d
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La plantilla de la máquina virtual debe actualizarse

Categoría	⚠
Componente	Light Agent
Id. del evento de Windows	3181
Id. de eventos de Kaspersky Security Center	00000c6d

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La licencia Standard caducó. La aplicación se ejecutará con la licencia Enterprise

Categoría	⚠
Componente	Light Agent
Id. del evento de Windows	3171
Id. de eventos de Kaspersky Security Center	00000c64
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Mensaje informativo

Aplicación iniciada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	235
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Aplicación detenida

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	236
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Autoprotección restringió el acceso al recurso protegido

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	213
Id. de eventos de Kaspersky Security Center	000000d5
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe borrado

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	217
Id. de eventos de Kaspersky Security Center	000000d9
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Directiva de grupo deshabilitada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	220
Id. de eventos de Kaspersky Security Center	000000dc
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Configuración de la aplicación cambiada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	218
Id. de eventos de Kaspersky Security Center	000000da
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Tarea iniciada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	221
Id. de eventos de Kaspersky Security Center	000000dd
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Tarea completada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	223
Id. de eventos de Kaspersky Security Center	000000df
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Todos los componentes de la aplicación definidos por la licencia se instalaron y se ejecutan en modo normal

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	227
Id. de eventos de Kaspersky Security Center	000000e3
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se modificó la configuración de la suscripción

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	238
Id. de eventos de Kaspersky Security Center	000000ee
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se ha renovado la suscripción

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	239
Id. de eventos de Kaspersky Security Center	000000ef
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto restaurado de Copia de seguridad

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	335
Id. de eventos de Kaspersky Security Center	0000014f
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Introducción de nombre de usuario y contraseña

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	2000
Id. de eventos de Kaspersky Security Center	000007d0
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La participación en KSN está habilitada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	2020
Id. de eventos de Kaspersky Security Center	000007e4
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Servidores de KSN disponibles

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	2022
Id. de eventos de Kaspersky Security Center	000007e6
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La aplicación funciona y procesa los datos conforme a las leyes pertinentes y utiliza la infraestructura adecuada

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	2024
Id. de eventos de Kaspersky Security Center	000007e8
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto restaurado de la cuarentena

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	345
Id. de eventos de Kaspersky Security Center	00000159
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado de la cuarentena

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	347
Id. de eventos de Kaspersky Security Center	0000015b
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se creó una copia de seguridad del objeto

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Protección contra amenazas de correo Detección de comportamiento Anticifrador Prevención de intrusiones en el host Sandbox Análisis de malware
Id. del evento de Windows	`308`
Id. de eventos de Kaspersky Security Center	`00000134`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Sobrescrito con una copia desinfectada anteriormente

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Prevención de intrusiones en el host Análisis de malware
Id. del evento de Windows	`327`
Id. de eventos de Kaspersky Security Center	`00000147`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Detección de archivo de almacenamiento protegido con contraseña

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Prevención de intrusiones en el host Análisis de malware
Id. del evento de Windows	`322`
Id. de eventos 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 la información adicional sobre el objeto detectado: Componente de la aplicación (`engine`). Tecnología de detección de amenazas (`method`). Amenaza detectada por KSN Privada (denylist): true o false.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Información sobre el objeto detectado

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Prevención de intrusiones en el host Análisis de malware

Id. del evento de Windows	332
Id. de eventos de Kaspersky Security Center	0000014c
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El objeto está en la lista de admitidos de Kaspersky Private Security Network

Categoría	ⓘ
Componente	Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Prevención de intrusiones en el host Análisis de malware
Id. del evento de Windows	340
Id. de eventos de Kaspersky Security Center	00000154
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto renombrado

Categoría	ⓘ
Componente	Protección contra amenazas de correo Prevención de exploits Detección de comportamiento Anticifrador Análisis de malware
Id. del evento de Windows	329
Id. de eventos de Kaspersky Security Center	00000149
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto procesado

Categoría	ⓘ
Componente	Prevención de intrusiones en el host Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Análisis de malware
Id. del evento de Windows	301
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Objeto omitido

Categoría	ⓘ
Componente	Prevención de intrusiones en el host Protección contra amenazas de archivo Protección vía AMSI Análisis de malware

Id. del evento de Windows	315
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo de almacenamiento detectado

Categoría	ⓘ
Componente	Prevención de intrusiones en el host Protección contra amenazas de archivo Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Análisis de malware
Id. del evento de Windows	318
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se detectó un objeto comprimido

Categoría	ⓘ
Componente	Prevención de intrusiones en el host Protección contra archivos peligrosos Protección contra amenazas web Protección contra amenazas de correo Protección vía AMSI Análisis de malware
Id. del evento de Windows	319
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Vínculo procesado

Categoría	ⓘ
Componente	Protección contra amenazas web
Id. del evento de Windows	361
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Inicio de aplicación autorizado

Categoría	ⓘ
Componente	Control de aplicaciones
Id. del evento de Windows	701
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Origen de actualizaciones seleccionado

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1001
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Servidor proxy seleccionado

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1002
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El vínculo está en la lista de admitidos de Kaspersky Private Security Network

Categoría	ⓘ
Componente	Protección contra amenazas web
Id. del evento de Windows	370
Id. de eventos de Kaspersky Security Center	00000172
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Aplicación ubicada en el grupo de confianza

Categoría	ⓘ
Componente	Prevención de intrusiones en el host
Id. del evento de Windows	401
Id. de eventos de Kaspersky Security Center	00000191
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Aplicación ubicada en un grupo restringido

Categoría	ⓘ
Componente	Prevención de intrusiones en el host
Id. del evento de Windows	402
Id. de eventos de Kaspersky Security Center	00000192

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Prevención de intrusiones en el host accionada

Categoría	ⓘ
Componente	Prevención de intrusiones en el host
Id. del evento de Windows	403
Id. de eventos de Kaspersky Security Center	00000193
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Archivo restaurado

Categoría	ⓘ
Componente	Detección de comportamiento Anticifrador Prevención de exploits Prevención de intrusiones en el host
Id. del evento de Windows	457
Id. de eventos de Kaspersky Security Center	000001c9
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Valor del Registro restaurado

Categoría	ⓘ
Componente	Detección de comportamiento Prevención de exploits
Id. del evento de Windows	458
Id. de eventos de Kaspersky Security Center	000001ca
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Valor del Registro eliminado

Categoría	ⓘ
Componente	Detección de comportamiento Prevención de exploits
Id. del evento de Windows	459
Id. de eventos de Kaspersky Security Center	000001cb
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Acción del proceso omitida

Categoría	ⓘ
Componente	Control de anomalías adaptativo

Id. del evento de Windows	2201
Id. de eventos 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 la 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).
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Teclado autorizado

Categoría	ⓘ
Componente	Prevención de ataques BadUSB
Id. del evento de Windows	2050
Id. de eventos de Kaspersky Security Center	00000802
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Actividad de red autorizada

Categoría	ⓘ
Componente	Firewall
Id. del evento de Windows	601
Id. de eventos de Kaspersky Security Center	00000259
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Inicio de aplicación prohibido en el modo de prueba

Categoría	ⓘ
Componente	Control de aplicaciones
Id. del evento de Windows	703
Id. de eventos 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 la categoría creada manualmente. • GNRL_EA_PARAM_4 es el identificador de seguridad (SID) de la cuenta. • 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 del 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 tratando de ejecutar.

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Inicio de aplicación autorizado en el modo de prueba

Categoría	ⓘ
Componente	Control de aplicaciones
Id. del evento de Windows	`704`
Id. de eventos 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 la categoría creada manualmente. • `GNRL_EA_PARAM_4` es el identificador de seguridad (SID) de la cuenta. • `GNRL_EA_PARAM_5` es información sobre la firma digital de la aplicación.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se abrió una página permitida

Categoría	ⓘ
Componente	Control web
Id. del evento de Windows	`751`
Id. de eventos de Kaspersky Security Center	`000002f4`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Operación con el dispositivo autorizada

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	`801`
Id. de eventos de Kaspersky Security Center	`00000321`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se realizó una operación en un archivo

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	`808`
Id. de eventos de Kaspersky Security Center	`GNRL_EV_USB_FILE_OPERATION`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es la operación que se realiza en un archivo (escribir o eliminar). • `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 el Id. de hardware (HWID).

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

No hay actualizaciones disponibles

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	`1020`
Id. de eventos de Kaspersky Security Center	`000003fc`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La distribución de actualizaciones se completó correctamente

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	`1022`
Id. de eventos de Kaspersky Security Center	`000003fe`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Descargando archivos

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	`1003`
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo descargado

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	`1004`
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo instalado

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	`1005`
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo actualizado

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1006
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Archivo revertido debido a error de actualización

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1007
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Actualizando archivos

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1008
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Distribuyendo actualizaciones

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1009
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Revirtiendo archivos

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1010
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Creando la lista de archivos para descargar

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	1013
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Descargando parches

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	2150
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Instalando el parche

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	2151
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Parche instalado

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	2152
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Revirtiendo el parche

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	2154
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Parche revertido

Categoría	ⓘ
Componente	Actualización
Id. del evento de Windows	2155
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se inició la implementación de las reglas de cifrado o descifrado de archivos

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	901
Id. de eventos de Kaspersky Security Center	00000385
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se completó la implementación de las reglas de cifrado o descifrado de archivos

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	902
Id. de eventos de Kaspersky Security Center	00000386
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se reanudó la implementación de las reglas de cifrado o descifrado de archivos

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	905
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado de archivos iniciado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	910
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado de archivos completado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	911
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El archivo no se cifró porque es una exclusión

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	913
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Modo portátil habilitado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	950
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Modo portátil deshabilitado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	952
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado del dispositivo iniciado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1301
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado del dispositivo completado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1302
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cifrado o descifrado del dispositivo reanudado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1304
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Dispositivo sin cifrar

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1307
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El proceso de cifrado o descifrado de dispositivos se cambió al modo activo

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1308
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El proceso de cifrado o descifrado de dispositivos se cambió al modo pasivo

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1309
Id. de eventos de Kaspersky Security Center	–

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se cargó el módulo de cifrado

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1310
Id. de eventos de Kaspersky Security Center	0000051e
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Nueva cuenta del Agente de autenticación creada

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1330
Id. de eventos de Kaspersky Security Center	00000532
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Cuenta del Agente de autenticación eliminada

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1331
Id. de eventos de Kaspersky Security Center	00000533
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Contraseña de la cuenta del Agente de autenticación cambiada

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1332
Id. de eventos de Kaspersky Security Center	00000534
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Inicio de sesión del Agente de autenticación correcto

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1333
Id. de eventos de Kaspersky Security Center	00000535

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Intento de inicio de sesión del Agente de autenticación fallido

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1334
Id. de eventos de Kaspersky Security Center	00000536
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se accedió al disco duro con el procedimiento de solicitud de acceso a dispositivos cifrados

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1335
Id. de eventos de Kaspersky Security Center	00000537
Registros 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

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1336
Id. de eventos de Kaspersky Security Center	00000538
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La cuenta no se agregó. Esta cuenta ya existe

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1337
Id. de eventos de Kaspersky Security Center	00000539
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La cuenta no se modificó. Esta cuenta no existe

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1338
Id. de eventos de Kaspersky Security Center	0000053a

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La cuenta no se eliminó. Esta cuenta no existe

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1339
Id. de eventos de Kaspersky Security Center	0000053b
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

La actualización de FDE se realizó correctamente

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1341
Id. de eventos de Kaspersky Security Center	0000053d
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La reversión de la actualización de FDE se realizó correctamente

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1343
Id. de eventos de Kaspersky Security Center	0000053f
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al eliminar los controladores de Cifrado de disco de Kaspersky de la imagen de WinRE

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1346
Id. de eventos de Kaspersky Security Center	00000542
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se cambió la clave de recuperación de BitLocker

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1370
Id. de eventos de Kaspersky Security Center	0000055a

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se cambió la contraseña o el PIN de BitLocker

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1371
Id. de eventos de Kaspersky Security Center	0000055b
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

La clave de recuperación BitLocker se guardó en una unidad extraíble

Categoría	ⓘ
Componente	Cifrado de datos
Id. del evento de Windows	1372
Id. de eventos de Kaspersky Security Center	0000055c
Registros 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

Categoría	ⓘ
Componente	Endpoint Sensor
Id. del evento de Windows	2103
Id. de eventos de Kaspersky Security Center	00000837
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El componente Endpoint Sensor se conectó al servidor

Categoría	ⓘ
Componente	Endpoint Sensor
Id. del evento de Windows	2101
Id. de eventos de Kaspersky Security Center	00000835
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se recuperó la conexión con el servidor de Kaspersky Anti Targeted Attack Platform

Categoría	ⓘ
Componente	Endpoint Sensor
Id. del evento de Windows	2102
Id. de eventos de Kaspersky Security Center	00000836

Registros 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

Categoría	ⓘ
Componente	Endpoint Sensor
Id. del evento de Windows	`2104`
Id. de eventos de Kaspersky Security Center	`00000838`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado

Categoría	ⓘ
Componente	Eliminación de datos
Id. del evento de Windows	`2251`
Id. de eventos de Kaspersky Security Center	`000008cb`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Estadísticas de la tarea de eliminación

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
Id. del evento de Windows	`2853`
Id. de eventos de Kaspersky Security Center	`00000b25`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Categoría	ⓘ
Componente	Eliminación de datos
Id. del evento de Windows	`2253`
Id. de eventos de Kaspersky Security Center	`000008cd`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto en cuarentena (Sandbox)

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	`2602`
Id. de eventos de Kaspersky Security Center	`00000a2a`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado (Sandbox)

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	2604
Id. de eventos de Kaspersky Security Center	00000a2c
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Se inició el análisis de IOC

Categoría	ⓘ
Componente	Endpoint Detection and Response
Id. del evento de Windows	2652
Id. de eventos de Kaspersky Security Center	00000a5c
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se completó el análisis de IOC

Categoría	ⓘ
Componente	Endpoint Detection and Response
Id. del evento de Windows	2653
Id. de eventos de Kaspersky Security Center	00000a5d
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto en cuarentena (Endpoint Detection and Response)

Categoría	ⓘ
Componente	Endpoint Detection and Response
Id. del evento de Windows	2555
Id. de eventos de Kaspersky Security Center	000009fb
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Objeto eliminado (Endpoint Detection and Response)

Categoría	ⓘ
Componente	Endpoint Detection and Response
Id. del evento de Windows	2557
Id. de eventos de Kaspersky Security Center	000009fd
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Los componentes de la aplicación se cambiaron correctamente

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	1402
Id. de eventos de Kaspersky Security Center	0000057a
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	2606
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	2609
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	2610
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	2616
Id. de eventos de Kaspersky Security Center	–
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	–

El Servidor de administración al que está conectado su dispositivo está configurado como de confianza

Categoría	ⓘ
Componente	Protección de la conexión del Servidor de administración
Id. del evento de Windows	3300
Id. de eventos de Kaspersky Security Center	00000ce4

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Su dispositivo está conectado a un nuevo Servidor de administración de confianza

Categoría	ⓘ
Componente	Protección de la conexión del Servidor de administración
Id. del evento de Windows	`3302`
Id. de eventos de Kaspersky Security Center	`00000ce6`
Registros 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 es de confianza

Categoría	ⓘ
Componente	Protección de la conexión del Servidor de administración
Id. del evento de Windows	`3303`
Id. de eventos de Kaspersky Security Center	`00000ce7`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Detección de Sandbox asíncrona

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	`2619`
Id. de eventos 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 el id. del incidente. • `GNRL_EA_PARAM_4` es el hash del objeto (SHA256).
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Un usuario envió correctamente la tarea de análisis a Sandbox

Categoría	ⓘ
Componente	Sandbox
Id. del evento de Windows	`2622`
Id. de eventos de Kaspersky Security Center	`00000a3e`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El dispositivo está conectado

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	`805`
Id. de eventos de Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUGGED`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el Id. de hardware (HWID). • `GNRL_EA_PARAM_2` es el nombre del usuario de la sesión.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El dispositivo está desconectado

Categoría	ⓘ
Componente	Control de dispositivos
Id. del evento de Windows	`806`
Id. de eventos de Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_UNPLUGGED`
Parámetros de eventos	• `GNRL_EA_PARAM_1` es el Id. de hardware (HWID). • `GNRL_EA_PARAM_2` es el nombre del usuario de la sesión.
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Error al eliminar la versión anterior de la aplicación

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	`246`
Id. de eventos de Kaspersky Security Center	`000000f6`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se estableció la conexión al servidor de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
Id. del evento de Windows	`2853`
Id. de eventos de Kaspersky Security Center	`00000b25`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se estableció la conexión al servidor de repuesta de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	`2853`
Id. de eventos de Kaspersky Security Center	`00000b25`

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se estableció la conexión al servidor de recolección de telemetría de EDR Expert

Categoría	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Id. del evento de Windows	`2857`
Id. de eventos de Kaspersky Security Center	`00000b26`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se estableció la conexión al servidor de NDR

Categoría	ⓘ
Componente	Network Detection and Response (KATA)
Id. del evento de Windows	`3083`
Id. de eventos de Kaspersky Security Center	`00000c0b`
Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se permite iniciar la aplicación cliente del servicio en la nube

Categoría	ⓘ
Componente	Cloud Discovery
Id. del evento de Windows	`2210`
Id. de eventos de Kaspersky Security Center	`000008a2`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se permite acceder al servicio en la nube

Categoría	ⓘ
Componente	Cloud Discovery
Id. del evento de Windows	`2211`
Id. de eventos de Kaspersky Security Center	`000008a3`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Acceso al área protegida

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	`2004`
Id. de eventos de Kaspersky Security Center	`000007d4`

Registros de eventos de Windows (predeterminado)	✓
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se detectó el cambio de un archivo o una carpeta

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	`2950`
Id. de eventos de Kaspersky Security Center	`00000b86`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El objeto cambia con demasiada frecuencia. Comenzó la incorporación de eventos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	`2955`
Id. de eventos de Kaspersky Security Center	`00000b8b`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Informe sobre la modificación de objetos para el periodo de incorporación

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	`2956`
Id. de eventos de Kaspersky Security Center	`00000b8c`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se detectó el cambio del registro

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	`2951`
Id. de eventos de Kaspersky Security Center	`00000b87`
Registros de eventos de Windows (predeterminado)	–

Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se detectó una conexión/desconexión de dispositivos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2952
Id. de eventos de Kaspersky Security Center	00000b88
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

El alcance del monitoreo incluye objetos incorrectos

Categoría	ⓘ / ⚠ / ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2903
Id. de eventos de Kaspersky Security Center	00000b89
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Línea de base creada

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2957
Id. de eventos de Kaspersky Security Center	00000b8d
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Línea de base actualizada

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	2958
Id. de eventos de Kaspersky Security Center	00000b8e

Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

El usuario de confianza realiza una operación

Categoría	ⓘ
Componente	Control de integridad del sistema
Id. del evento de Windows	`2962`
Id. de eventos de Kaspersky Security Center	`00000b92`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Para configurar el período de retención para este evento, vaya a la sección **Configuración de eventos** de la directiva y establezca el período de retención para el evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

Se conectó a la SVM

Categoría	ⓘ
Componente	Light Agent
Id. del evento de Windows	`3152`
Id. de eventos de Kaspersky Security Center	`00000c50`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se creó una nueva contraseña temporal

Categoría	ⓘ
Componente	Auditoría del sistema
Id. del evento de Windows	`265`
Id. de eventos de Kaspersky Security Center	`00000109`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se conectó al Servidor de integración

Categoría	ⓘ
Componente	Light Agent
Id. del evento de Windows	`3105`
Id. de eventos de Kaspersky Security Center	`00000c21`
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Restaurando la conexión con el servidor de integración

Categoría	ⓘ
Componente	Light Agent
Id. del evento de Windows	3104
Id. de eventos de Kaspersky Security Center	00000c20
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Se estableció la conexión al servidor de KUMA

Categoría	ⓘ
Componente	Integración con KUMA
Id. del evento de Windows	2857
Id. de eventos de Kaspersky Security Center	00000b29
Registros de eventos de Windows (predeterminado)	–
Registro de eventos de Kaspersky Security Center (predeterminado)	✓

Apéndice 7. Extensiones de archivo compatibles para la Prevención de ejecución

Kaspersky Endpoint Security es compatible con la prevención de la apertura de archivos con formato de Office en determinadas aplicaciones. La información sobre las extensiones de archivo y las aplicaciones admitidas se encuentra en la siguiente tabla.

Extensiones de archivo compatibles para la Prevención de ejecución

Nombre de la aplicación.	Archivos ejecutables	Extensión de archivos
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

Nombre de la aplicación.	Archivos ejecutables	Extensión de archivos
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Lector de PDF de Foxit STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Apéndice 8. Intérpretes de scripts compatibles para la prevención de ejecución

Prevención de ejecución admite los siguientes intérpretes de scripts:

- 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

Prevención de ejecución permite trabajar con aplicaciones Java en el entorno de tiempo de ejecución de Java (procesos de java.exe y javaw.exe).

Apéndice 9. Alcance del análisis de IOC en el registro (RegistryItem)

Cuando agrega el tipo de datos **Registro de Windows: RegistryItem** al alcance del Análisis de IOC, Kaspersky Endpoint Security analiza las siguientes claves del 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 archivos de IOC

Al crear tareas de Análisis de IOC, tenga en cuenta los siguientes requisitos y limitaciones de los archivos de IOC:

- La aplicación es compatible con archivos de IOC con extensiones IOC y XML en las versiones 1.0 y 1.1 del estándar abierto OpenIOC para describir indicadores de compromiso.
- Después de cargar los archivos de IOC, puede editarlos de forma manual en el editor incorporado 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 de IOC que son compatibles 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 de ellos no son compatibles, la aplicación utiliza solo los archivos de IOC compatibles cuando se ejecuta la tarea. Si al crear una tarea de *Análisis de IOC* en la línea de comandos, todos los archivos de IOC que carga resultan no 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 con Web Console ni 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 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 IOC y crear varias tareas de *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 haciendo clic en el siguiente vínculo, contiene una tabla con la lista completa de términos IOC del estándar 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.

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 Email/*, solo se admiten las condiciones `contains` e `is`. Para que el Análisis retrospectivo de IOC funcione correctamente, cuando se utiliza la condición `is`, las direcciones de correo electrónico de los archivos de IOC deben especificarse en el siguiente formato: `"name@example.org" <SMTP:name@example.org>`. Al ejecutar la tarea *Análisis de IOC* normalmente, basta con especificar la dirección de correo electrónico en el siguiente formato: `name@example.org`.

Atributos de la condición compatible	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operadores compatibles	`AND` `OR`
Tipos de datos compatibles	`"date"`: fecha (condiciones aplicables: `is`, `greater-than`, `less-than`) `"int"`: entero (condiciones aplicables: `is`, `greater-than`, `less-than`) `"string"`: cadena (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 el formato `ISO 8601, Zulu time zone, UTC`.

Apéndice 11. API para respuesta a amenazas de EDR

Kaspersky Endpoint Security 12.9 para Windows es compatible con las acciones de respuesta a amenazas de EDR (EDR responses) utilizando Kaspersky Security Center OpenAPI. Es decir, puede llamar a métodos de OpenAPI para automatizar la respuesta a amenazas de EDR con Python. Puede llamar a estos métodos al realizar la integración con las soluciones SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, la solución de Kaspersky SIEM, es compatible con OpenAPI de respuesta a amenazas de EDR a partir de la versión 3.4.1. Para ver ejemplos de scripts, consulte la documentación de KUMA.

Para realizar acciones de respuesta a amenazas de EDR, debe crear una solicitud y enviarla utilizando 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 a 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 una versión posterior y en Kaspersky Security Center Linux 15.2 o una versión posterior. Otras consolas, incluidas las consolas de las soluciones de Kaspersky Detection and Response, no son compatibles.

Para la respuesta a amenazas de EDR, debe especificar los parámetros básicos de la solicitud, por ejemplo, en formato JSON:

- `task` es el tipo de tarea (ver más abajo).
- `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 agrega al nombre de la tarea creada.

Para configurar la respuesta a 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 la `[Response][KUMA] <task type> - <Date> <Time> - <ID>` en la consola de Kaspersky Security Center.

Conexión a Kaspersky Security Center OpenAPI

Como parte de respuesta a amenazas de EDR, la aplicación crea tareas especiales en la consola de Kaspersky Security Center. Para crear estas tareas, es necesario 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 cambió. Kaspersky XDR usa tokens PAT en lugar de 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 la solicitud, 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 obligatorio.
`kscPort`	`int`	Puerto de la conexión del Servidor de administración Parámetro obligatorio.
`kscCert`	`string`	Ruta a un archivo de certificado para conectarse al Servidor de administración de Kaspersky Security Center. De manera predeterminada, el parámetro está establecido en `False`.
`kscUser`	`string`	Nombre de cuenta del usuario. Parámetro obligatorio.
`kscPassword`	`string`	Contraseña de la cuenta de usuario. Parámetro obligatorio.

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 lo tanto, debe especificar un usuario separado que se usará para realizar solo 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`	Busque el archivo que desea eliminar en las 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;
};
```

Poner archivo en cuarentena – quarantineFile

Configuración de la tarea Poner archivo en 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 de almacenamiento Zip con archivos de IOC que desea usar para analizar.
`isolateHost`	`boolean`	Aísle el equipo de la red cuando se detecte un indicador de compromiso 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 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 de acceso 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;
};
```

Finalizar proceso – terminateProcess

Configuración de la tarea Finalizar 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 entre 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 la red del equipo – isolateHost

Configuración de aislamiento de la red del equipo

Parámetro	Tipo	Descripción
`action`	`string`	Modo de funcionamiento del 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

Ajustes de prevención de ejecución

Parámetro	Tipo	Descripción
hash	string	Hash MD5 del archivo que desea evitar que se ejecute.
path	string	Ruta al archivo que desea evitar que se ejecute.
caseSensitive	boolean	Distinción entre 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 de malware – onDemandScan

Configuración de la tarea Análisis de malware

Parámetro	Tipo	Descripción
path	string	Lista delimitada por espacios de archivos y carpetas para análisis personalizado.
recursive	boolean	Modo de análisis recursivo.
type	number	Alcance 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 del componente de la aplicación

Para configurar algunos componentes de la aplicación, se deben agregar reglas especiales. Por ejemplo, para Control web, se debe agregar una regla con una lista de direcciones web que desea que la aplicación bloquee. En las reglas de componentes de la aplicación, también se puede configurar una programación para el componente o seleccionar usuarios a los que la aplicación debe aplicar la regla.

Se deben agregar reglas para configurar los siguientes componentes de la aplicación:

- Control de aplicaciones.
- Control web.
- Control de dispositivos.
- Inspección de registro.
- Control de anomalías adaptativo.
- Control de integridad del sistema.

A partir de Kaspersky Endpoint Security para Windows 12.5, puede seleccionar usuarios no solo de Active Directory, sino también de la lista de usuarios en Kaspersky Security Center. También puede ingresar los datos de la cuenta de usuario local manualmente. Esto significa que puede agregar usuarios de las siguientes maneras:

- Active Directory (recomendado)
- Lista de usuarios en Kaspersky Security Center
- Cuenta de usuario local

> Para emplear correctamente todos los métodos de selección de usuario, debe actualizar la aplicación y el complemento de administración de Kaspersky Endpoint Security a la versión 12.5 o superior.

Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar 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 completamente responsable de la seguridad de un equipo si se usan cuentas de usuario locales; esto incluye, en especial, la responsabilidad de controlar y restringir el acceso a la configuración de Kaspersky Endpoint Security.

La aplicación usa el SID (Identificador de seguridad) del usuario para identificar a los usuarios. Al usar 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 coloca una carga adicional en el equipo para identificar a un usuario. Si agregó más de 1000 cuentas de usuario locales a una regla de la aplicación, las aplicaciones se comunican 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, se recomienda usar cuentas de usuario de Active Directory o de la lista de usuarios de Kaspersky Security Center.

La aplicación utiliza nombres NetBIOS para identificar las cuentas de usuario agregadas manualmente que tienen los formatos `<username>` y `<hostname>\<username>`. Un nombre 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. Entonces, la aplicación deshabilita la regla y muestra un error, por ejemplo, *Control web: activación de reglas deshabilitada para cuentas de usuario sin un identificador de seguridad (SID) coincidente*. Para que la regla funcione, debe acortar el nombre del equipo de forma manual. Puede agregar cuentas de usuario desde Active Directory o Kaspersky Security Center. En este caso, la aplicación acorta el nombre del equipo de forma automática.

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 solo permite usar cuentas de usuario integradas agregadas desde Active Directory o la lista de usuarios en Kaspersky Security Center. Las reglas en las que se agrega una cuenta de usuario integrada localmente no funcionan.

Información legal

Suministro 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 operación.

La información recibida es protegida por Kaspersky de acuerdo con la ley y con los requisitos y las reglamentaciones aplicables de Kaspersky. La información se transmite a través de canales de comunicación cifrados.

Suministro de datos estipulado en 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;
- versión de las actualizaciones instaladas en Kaspersky Endpoint Security;
- id. del equipo e id. asignado a la copia de Kaspersky Endpoint Security instalada en el equipo;
- número de serie e identificador de la clave activa;
- tipo, versión y número de bits del sistema operativo, junto con el 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 diseminación y el uso del software Kaspersky.

Al utilizar un código de activación, acepta transmitir automáticamente los datos enumerados anteriormente. Si no está de acuerdo en compartir esta información con Kaspersky, debe utilizar un archivo de clave para activar Kaspersky Endpoint Security.

Al aceptar los términos 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. único de la ejecución de la tarea de actualización,
    - id. único de la instalación de Kaspersky Endpoint Security.
- Al utilizar vínculos 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 instalada en Kaspersky Endpoint Security,
    - hash del archivo en el que se haya detectado una amenaza, además del nombre con el que Kaspersky clasifica dicha amenaza,
    - categoría del error de activación de Kaspersky Endpoint Security,
    - código del error de activación de Kaspersky Endpoint Security,
    - días por delante hasta que caduque la clave,
    - días transcurridos desde que se agregó la clave,
    - días transcurridos desde que caducó la licencia,
    - cantidad de equipos en los que se aplicó la licencia actual,
    - clave activa,
    - plazo de licencia de Kaspersky Endpoint Security,
    - estado de la licencia,
    - tipo de licencia actual,
    - tipo de aplicación,
    - id. único de la ejecución de la tarea de actualización,

- id. único asignado a la instalación de Kaspersky Endpoint Security en el equipo,
- idioma de la interfaz de Kaspersky Endpoint Security.

La información recibida es protegida por Kaspersky de acuerdo con la ley y con los requisitos y las reglamentaciones aplicables de Kaspersky. La información se transmite 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_<identificador del idioma>.txt contienen el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network y están incluidos en el kit de distribución.

Provisión de datos al utilizar 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 analizarse: las sumas de comprobación del archivo analizado (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;
- ID 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 firmado del ticket del servicio de activación (identificador del centro de activación regional, suma de comprobación del código de activación, suma de comprobación del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket), estado de la licencia, fecha y hora de inicio/finalización 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 comprobación (MD5) del archivo de clave;
- Información sobre el software del titular de los derechos: 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:

Cuando la casilla **Kaspersky Security Network** está activada y la casilla **Habilitar el modo KSN extendido** está desactivada, la aplicación transmite 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 analizarse: las sumas de comprobación del archivo analizado (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;
- ID 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 firmado del ticket del servicio de activación (identificador del centro de activación regional, suma de comprobación del código de activación, suma de comprobación del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket), estado de la licencia, fecha y hora de inicio/finalización 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 comprobación (MD5) del archivo de clave;
- Información sobre el software del titular de los derechos: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

Cuando tanto la casilla **Habilitar el modo KSN extendido** como la casilla **Kaspersky Security Network** están activadas, la aplicación transmite la información que se indica más arriba y, además, lo siguiente:

- 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 URL y las direcciones IP de descarga y de las páginas de descarga, el identificador del protocolo de descarga y el número de puerto de conexión, el estado de las URL como malicioso o no, los atributos, el tamaño y las sumas de comprobación del archivo (MD5, SHA2-256, SHA1), información sobre el proceso que descargó el archivo (sumas de comprobación (MD5, SHA2-256, SHA1), fecha y hora de creación/compilación, estado de reproducción automática, atributos, nombres de los empacadores, información sobre firmas, marca de archivo ejecutable, el identificador de formato y la entropía), el nombre del archivo y su ruta en el equipo, la firma digital y la marca de tiempo de su generación, la dirección URL donde ocurrió la detección, el número del script en la página que parece ser sospechosa o dañina, información sobre solicitudes HTTP generadas y la respuesta a ellas;

- información sobre las aplicaciones en ejecución y sus módulos: datos sobre los procesos que se están ejecutando en el sistema (identificador del proceso [PID], nombre del proceso, información sobre la cuenta con la que se inició el proceso, aplicación y comando con que se inició el proceso, el signo de programa o proceso de confianza, ruta de acceso completa a los archivos del proceso y sus sumas de comprobación [MD5, SHA2-256, SHA1], línea de comandos de inicio, nivel de integridad del proceso y descripción del producto al cual pertenece el proceso [nombre del producto e información sobre el editor], así como los certificados digitales utilizados y la información necesaria para verificar su autenticidad o información sobre 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 y sumas de comprobación [MD5, SHA2-256, SHA1], además de las rutas de acceso a estos en el equipo), información del encabezado de archivo PE y nombres de los empaquetadores (para archivos empaquetados);

- 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; nombre, tamaño y ruta de los archivos infectados; código de la plantilla de la ruta; marca de archivo ejecutable; indicador que señala si el objeto es un contenedor; nombres del empaquetador (para archivos empaquetados); código del tipo de archivo; id. del formato de archivo; lista de acciones realizadas por el malware y decisión tomada por el software y por el usuario en respuesta a ellas: id. de las bases de datos antivirus y de los registros de las bases de datos antivirus que se hayan usado para tomar la decisión; indicador de un objeto potencialmente malicioso; nombre de la amenaza detectada según la clasificación del Titular de los derechos; nivel de peligro; estado de detección y método de detección; motivo de inclusión 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 de la cual se transmitieron el mensaje o el vínculo infectados; direcciones IP despersonalizadas (IPv4 e IPv6) del host del objeto bloqueado; entropía del archivo; indicador de ejecución automática del archivo; hora a la que se detectó por primera vez el archivo en el sistema; número de ocasiones en las que se ejecutó el archivo desde el envío de las últimas estadísticas; información sobre el nombre; sumas de comprobación (MD5, SHA2-256, SHA1) y tamaño del cliente de correo a través del cual se recibió el objeto malicioso; id. de la tarea del software que realizó el análisis; indicador que señala si la firma o la reputación del archivo se comprobaron; resultado del procesamiento del archivo; suma de comprobación (MD5) del patrón obtenido para el objeto; tamaño del patrón en bytes; y las 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 Control de anomalías adaptativo: el identificador 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, así como sobre el proceso sujeto a la actividad sospechosa (identificador 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 del 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, la suma de comprobación del código de activación, la 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 de 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. de la 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, además del 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 las unidades 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 (arranque seguro, KPTI, WHQL Enforce, BitLocker, distinción entre mayúsculas y minúsculas), 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 supervisión 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 luego de su actualización, tiempo de demora de procesamiento del evento para cada uno de los componentes de supervisión 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 seguimiento (nombre, estructura, parámetros de seguimiento, desglose de la cantidad de operaciones de pista por tipo), información sobre el SO (nombre, tipo, versión, edición, fecha de lanzamiento, hora de inicio);

- información de ETW, proveedores de eventos 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 finalización, tipo de token de acceso, SID, Id. de sesión, 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, localización, versión e identificador de la aplicación, versión del archivo e identificador);

- información de ETW; proveedores de eventos FileIo/DiskIo/Image/Windows Kernel Disk de Microsoft: información sobre el archivo y las operaciones del disco (tipo, capacidad, horario de inicio, horario de finalización, duración, estado de finalización, 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/finalización 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 finalización, hora, cantidad, PID), estructura de asignación de la memoria (tipo, capacidad, id. de sesión, 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 finalización, 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 supervisión 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 en la autodefensa del Software: el nombre y el tamaño del archivo de proceso, sus sumas de comprobación (MD5, SHA2-256, SHA1), la ruta completa al archivo de proceso y el código de plantilla de la ruta de archivo, las marcas de tiempo de creación/compilación, marca de archivo ejecutable, atributos del archivo de proceso, información sobre el certificado utilizado para firmar el archivo de proceso, código de la cuenta utilizada para iniciar el proceso, Id. de las operaciones realizadas para acceder al proceso, tipo de recurso con el que se realiza la operación (proceso, archivo, objeto de registro, función de búsqueda FindWindow), nombre del recurso con el que se realiza la operación, indicador que muestra que la operación se completó correctamente, el estado del archivo del proceso y su firma según la KSN;

- información sobre el software del titular de los derechos: versión completa, tipo, localización 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 que se instaló 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 de las actualizaciones instaladas, tamaño de palabra, edición y parámetros del modo de ejecución del SO, versión y sumas de comprobación (MD5, SHA2-256, SHA1) del archivo del núcleo del SO, fecha y hora de inicio del SO;
- archivos ejecutables y no ejecutables, total o parcialmente;
- secciones de la RAM del equipo;
- sectores involucrados en el proceso de arranque del SO;
- paquetes de datos tomados del tráfico de red;
- páginas web y mensajes de correo electrónico con objetos sospechosos o maliciosos;
- descripción de las clases e instancias de las clases del repositorio de WMI;
- informes de actividad de aplicaciones:
  - 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, las marcas de hora de creación y modificación 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 apropiados, 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 el 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 del software instalado, 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 utilizar las 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 en formato simple y no cifrado.

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 de este cuando se desinstala Kaspersky Endpoint Security.

Datos recibidos como resultado de 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
- Nombre y tipo de registro DNS
- Dirección IP del equipo protegido
- Dirección física (dirección MAC) del equipo protegido
- Identificador en la entrada del registro de eventos
- Nombre de la fuente de datos en el registro
- Nombre del registro
- Hora del evento
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo (incluida la ruta)
- Tamaño del archivo
- Dirección IP remota y puerto con los 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 del 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 comenzó 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 cuenta del usuario
- Nombre del volumen
- Letra del volumen
- Tipo de volumen
- Valor de registro de Windows
- Valor de colmena de registro
- Ruta de la clave de registro (sin colmena ni nombre 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 solicitud HTTP

Datos para crear una cadena de desarrollo de la amenaza

Los datos para crear una cadena de desarrollo de la amenaza se almacenan durante siete días de manera predeterminada. 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
- Razón por la que falló el procesamiento de detección
- Tipo de objeto detectado
- Nombre del objeto detectado
- Estado de amenaza después de que se procesa 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 privilegiados
  - 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 procesado
- Identificadores únicos del archivo
- Nombre completo del archivo (nombre del archivo local o dirección web del archivo descargado)
- Ruta a la variable de registro de Windows procesada
- Nombre de la variable de registro de Windows procesada
- Valor de la variable de registro de Windows procesada
- Tipo de la variable de 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 vínculo 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 de este cuando se desinstala Kaspersky Endpoint Security.

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 incorporado de Kaspersky Endpoint Security:
  - Archivos en cuarentena
  - Clave pública del certificado utilizado para la integración con Kaspersky Sandbox
- Caché del agente incorporado de Kaspersky Endpoint Security:
  - Hora en que los resultados del análisis se registraron en la memoria caché
  - Hash MD5 de la tarea de análisis
  - Identificador de la 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 del objeto
  - Identificador del sistema (SID) del usuario del sistema operativo cuya cuenta se utilizó para crear la tarea
  - Hash MD5 de la tarea de análisis del objeto
- Información sobre las tareas para las que el agente incorporado de Kaspersky Endpoint Security espera los resultados del análisis de Kaspersky Sandbox:
  - Hora en que se recibió la tarea de análisis del objeto
  - Estado de procesamiento del objeto
  - Id. de la sesión de usuario en el sistema operativo donde se creó la tarea de análisis del objeto
  - Identificador de la tarea de análisis del objeto
  - Hash MD5 de la tarea de análisis del objeto
  - Identificador del sistema (SID) del usuario del sistema operativo cuya cuenta se utilizó para crear la tarea
  - Esquema XML del IOC creado automáticamente
  - Hash MD5 o SHA256 del objeto escaneado

- Errores de procesamiento
- Nombres de los objetos para los que se creó la tarea
- Resultado del análisis del objeto

Datos de solicitudes a Kaspersky Sandbox

Los siguientes datos de las solicitudes del agente incorporado de Kaspersky Endpoint Security a Kaspersky Sandbox se almacenan localmente en el equipo:

- Hash MD5 de la tarea de análisis
- Identificador de la tarea de análisis
- Objeto escaneado 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
- Nombre y tipo de registro DNS
- Dirección IP del equipo protegido
- Dirección física (dirección MAC) del equipo protegido
- Identificador en la entrada del registro de eventos
- Nombre de la fuente de datos en el registro
- Nombre del registro
- Hora del evento
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo (incluida la ruta)
- Tamaño del archivo
- Dirección IP remota y puerto con los 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 del 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 comenzó 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 cuenta del usuario
- Nombre del volumen
- Letra del volumen
- Tipo de volumen
- Valor de registro de Windows
- Valor de colmena de registro
- Ruta de la clave de registro (sin colmena ni nombre 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 solicitud HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Todos los datos que la aplicación almacena localmente en el equipo se eliminan de este cuando se desinstala Kaspersky Endpoint Security.

Datos de servicio

El agente incorporado 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 del nodo central de KATA
  - 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 el nodo central de KATA

    - 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 respuestas
- 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 del 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 la aplicación.
        - Versión de la aplicación
        - Proveedor de aplicaciones
        - Descripción del archivo
        - Versión de 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 enviado a AMSI
  - Contenido del objeto enviado a AMSI
  - Nombre del objeto
  - Hashes MD5 y SHA256 del objeto
- Datos sobre el bloqueo de aplicaciones:
  - Identificador único del proceso que inició el bloqueo de la aplicación
  - Identificador único del proceso principal
  - Identificador único del sistema del proceso
  - Comando utilizado para iniciar un proceso
  - Id. de sesión de inicio
  - 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 bloqueados:
  - 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 archivo
  - Identificadores únicos del archivo

    - Tipo de operación de modificación
    - Indicador que señala que el archivo se eliminará después de reiniciar el equipo
    - Identificador único del archivo modificado
    - Identificador único del archivo antes de la modificación
    - Conjunto de marcadores de bits que determinan cómo se abrió el archivo
    - Datos sobre operaciones en la lista de control de acceso
    - Datos sobre cambios en la propiedad o el grupo principal del archivo
- Datos sobre la sesión de inicio de sesión:
    - Id. de sesión de inicio
    - Nombre de usuario que inició sesión
    - Tipo de cuenta de usuario
    - Tipo de sesión
- Datos sobre conexiones de red:
    - Identificador único del proceso que inició la conexión
    - Dirección IP local utilizada para iniciar la conexión
    - Dirección IP remota del endpoint de conexión
    - Dirección de conexión
    - Protocolo de transferencia de datos
    - Método HTTP
    - Ruta sin el nombre de host
    - Nombre de host
    - Estado dinámico del proceso en el momento de la conexión
    - Indicador que señala que la conexión está abierta a nivel de socket de tipo raw
    - Versión de TLS utilizada en la sesión de conexión
    - Nombre del servidor TLS
    - Hashes 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 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 de la consola
    - Tipo de entrada de la consola
    - Texto ingresado por un usuario o un proceso
- Datos sobre la creación del proceso:
    - Identificador único del proceso
    - Identificador único del proceso principal
    - Identificador único del sistema del proceso
    - Comando utilizado para iniciar un proceso
    - Id. de sesión de inicio
    - 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 del módulo
    - Nombre completo del ensamblado .NET si el archivo cargado es un módulo .NET
    - Marcadores del ensamblado .NET definidos en su manifiesto

- Datos sobre la finalización del proceso:
  - Identificador único del proceso finalizado
- 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 del registro
  - Nombre del valor dentro de una clave del registro
  - Tipo de datos almacenados en el valor de clave del registro
  - Datos especificados en el valor de clave del registro
  - Nombre de la clave antes de renombrarla
  - Información relativa a un cambio de propiedad de la clave o del 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:
  - Marcador 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 en la que se guardó el registro de amenazas en la base de datos
  - Modo de procesamiento de amenazas
  - 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 de objeto
    - Contenido del objeto
- Datos sobre el acceso a los procesos:
    - Identificador único del proceso que intentó acceder
    - Identificador único del proceso de destino al que se accedió
    - Conjunto de derechos solicitados al proceso de destino
    - Tipo de operación
    - Conjunto de llamadas al 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 DNS
    - Dirección IP del servidor DNS
    - Marcadores que administran el comportamiento de una consulta DNS
    - Estado de finalización de la solicitud
    - Nombre de dominio completo especificado en la consulta DNS
    - Tipo de datos en la consulta DNS
    - Respuestas del servidor DNS
- Datos sobre la infiltración de código:
    - Identificador único del proceso que intentó infiltrar el código
    - Método de acceso utilizado
    - Conjunto de llamadas en el momento en que se detectó el código infiltrado
    - Identificador único del proceso de destino al que se le 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 con nombre
  - Tipo de operación (creación o conexión)
- Datos sobre consultas WMI:
  - Identificador único del proceso que inició la operación WMI
  - Tipo de operación 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 solicitud LDAP
  - Alcance de la búsqueda de las consultas LDAP
  - Filtro LDAP
  - Parámetro que especifica la partición de Active Directory a la que se dirigió la consulta
  - Atributos de búsqueda 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 señala que el dispositivo USB es una unidad del sistema
- Datos sobre la creación, eliminación y modificación de una tarea programada

- Datos sobre la 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 cómo iniciar/detener el 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 finalización del agente
  - Código de finalización del proceso del agente
- Configuración de filtrado de eventos:
  - Nombres de módulo
  - 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 completas 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 incorporado de Kaspersky Endpoint Security

- Configuración general de la tarea:
  - Tipo de tarea
  - Configuración de la programación de tarea
  - Nombres y contraseñas de las cuentas con las cuales se pueden ejecutar las tareas
  - Versiones de configuración

    - Identificadores de objetos en cuarentena
    - Ruta 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 de IOC
    - Nombre del servicio
    - Tipo de inicio de servicio
    - Carpetas para las que se deben recibir los resultados de la tarea *Obtener análisis forense*
    - Máscaras de los nombres de objetos y extensiones para la tarea *Obtener análisis forense*
- Configuración de aislamiento de la red:
    - Tipos de configuración
    - Versiones de configuración
    - Listas de exclusiones de aislamiento de red y configuración de exclusión: dirección del tráfico, direcciones IP, puertos, protocolos y rutas completas a archivos ejecutables
    - Indicadores de las acciones adicionales
    - Tiempo de deshabilitación del aislamiento automático
- Configuración de prevención de ejecución:
    - Tipos de configuración
    - 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 las solicitudes enviadas por Kaspersky Endpoint Security al componente EDR Expert

Al integrarse con la solución EDR Expert (on-premises), los siguientes datos se almacenan localmente en los equipos.

- En solicitudes de sincronización:
  - Id. única
  - 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 autodefensa 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 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 tareas

    - Hora de finalización de la tarea
    - 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, hash MD5 y SHA256, identificadores de objetos en cuarentena
    - Información sobre los procesos iniciados o detenidos en un equipo a pedido del servidor: PID y UniquePID, código de error, hashes MD5 y SHA256 de los objetos
    - Información sobre los servicios iniciados o detenidos en un equipo a petición 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
    - Nombre de la sesión de inicio
    - Fecha y hora en que comenzó el proceso
    - Hashes MD5 y SHA256 del objeto
- Datos en archivos:
    - Ruta de archivo
    - Nombre de archivo
    - Tamaño del archivo
    - Atributos del 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 de errores que ocurren al recuperar información sobre objetos:
  - Nombre completo del objeto que se procesó cuando ocurrió un error
  - Código de error
- Datos de los resultados de análisis de YARA:

  El agente incorporado 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 tareas 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 de archivo
  - Tamaño del archivo
  - Nombre del proceso
  - Argumentos del proceso
  - Ruta al archivo del 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 comenzó el proceso
- Datos de los resultados de análisis de IOC:
  - Dirección IP de la tabla ARP
  - Dirección física de la tabla ARP
  - Nombre del registro DNS
  - Tipo de registro DNS
  - Nombre de host
  - Dirección IP
  - Id. del evento en el registro
  - Nombre de la fuente de datos en el registro
  - Nombre del registro

- Nombre 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 con los 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 del 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 comenzó el proceso
- Ruta a la clave del registro
- Nombre de la clave del Registro
- Valor de texto de la clave del 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
- Nombre 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 de este cuando se desinstala Kaspersky Endpoint Security.

Datos de telemetría

- **Datos sobre archivos**
  - Identificadores únicos del archivo
  - Tipo de archivo
  - Ruta completa del archivo
  - Tamaño del archivo
  - Atributos del 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 la aplicación.
  - Versión de la aplicación
  - Proveedor de aplicaciones
  - Descripción del archivo
  - Versión de 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 utilizadas 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 huella digital del certificado
- Huella digital del certificado
- Período de validez del certificado

- **Datos sobre la sesión de inicio de sesión**
  - Id. de sesión de inicio
  - Nombre de cuenta del usuario que inició sesión
  - Tipo de cuenta de usuario
  - Tipo de sesión
  - Dirección IP de la máquina desde la que se intentó iniciar sesión
  - Dirección IP de la máquina local para la que se intentó iniciar sesión
  - Marcador que indica 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 utilizado para la sesión de terminal
  - Protocolo IPv4 utilizado para la sesión de terminal
- **Datos sobre la comunicación de la red**
  - Inicio y finalización del intervalo de tiempo durante el cual se recopilaron 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 de la puerta de enlace
- 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 en el 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 endpoint de conexión
  - Método HTTP
  - Ruta sin el nombre de host
  - Nombre de host
  - Estado dinámico del proceso en el momento de la conexión
  - Dirección de conexión
  - Estado de proceso dinámico
  - Campo EtherType de trama Ethernet
- **Datos capturados mientras escucha en un puerto de red**
  - Identificador único del proceso que inició la conexión
  - Protocolo de transferencia de datos
  - Dirección local
  - Estado dinámico del proceso en el momento de la conexión

- **Resultado de la verificación de la conexión**
  - Configuración de red de host
  - Descripción de la interfaz de red
  - Nombre de dominio DNS
  - Dirección MAC local del equipo
  - Número de métrica de conexión IP
  - Lista de direcciones IP
  - Dirección IP
  - Máscara de red
  - Dirección IP de la puerta de enlace
  - Dirección MAC de la puerta de enlace
  - Lista de parches instalados
  - Número de parche
  - Fecha de instalación de parche
  - Modelo del dispositivo
  - Proveedor del dispositivo
  - Id. del host en Kaspersky Security Center
  - Descripción del antivirus de Kaspersky instalado
  - Nombre del componente del antivirus de Kaspersky instalado
  - Versión del componente del antivirus de 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 de Kaspersky instalado
  - Lista de claves de licencia
  - Número de serie de clave
  - Tipo de clave

- Fecha de caducidad de la clave
- Estado de la clave

- **Datos sobre la creación del proceso en el host**
  - Identificador único del proceso
  - Identificador único del proceso principal
  - Identificador único del sistema del proceso
  - Comando utilizado para iniciar un proceso
  - Id. de sesión de inicio
  - Id. de sesión de terminal
  - Identificador único del archivo de proceso
  - Nivel de integridad del proceso
  - Lista de tokens de derechos de proceso
  - Derechos de atributo
  - Lista de identificadores únicos de archivos interpretados
  - Estado del proceso
  - Comando utilizado para iniciar un proceso
- **Datos sobre la finalización del proceso**
  - Identificador único del proceso
- **Datos sobre la amenaza detectada**
  - Información sobre amenazas
  - 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 de objeto
- Contexto de la amenaza detectada
- Contenido del objeto
- Marcador que indica que la detección de amenazas se ejecutó en segundo plano

- **Datos sobre el procesamiento de amenazas**
  - Información sobre amenazas
  - 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 amenaza

- Motivo por el cual la amenaza no se pudo remediar
- Dirección física local

- **Datos sobre los usuarios**
  - SID de usuario
  - Id. de usuario
  - Nombre de usuario
  - Nombre completo del usuario
  - Descripción del usuario
  - Si la cuenta está activa o bloqueada
  - Si la contraseña caducó
  - Si se requiere un cambio de contraseña
  - Si se permite el cambio de contraseña
  - Tipo de cuenta de usuario
  - Si el inicio de sesión automático está habilitado para esta cuenta
  - 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 de este cuando se desinstala Kaspersky Endpoint Security.

Al integrarse con Kaspersky Unified Monitoring and Analysis Platform (KUMA), se transfieren los datos de configuración de la conexión, así como todos los eventos guardados en los registros de Windows.

Los principales registros de eventos de Windows son el sistema, la seguridad, la aplicación, los eventos reenviados y los eventos de hardware. Los usuarios también pueden crear y trabajar con registros personalizados para cumplir sus requisitos específicos.

Cumplimiento de la legislación de la Unión Europea (RGPD)

Kaspersky Endpoint Security puede transmitir datos a Kaspersky en las siguientes situaciones:

- Al usar Kaspersky Security Network.
- Al activar la aplicación con un código de activación nuevo.

- Al actualizar módulos de aplicaciones y bases de datos antivirus.
- Al seguir vínculos en la interfaz de la aplicación.

Independientemente de la clasificación de datos y el territorio desde el que se reciben los datos, Kaspersky respeta altos estándares de seguridad de datos y emplea diversas medidas legales, organizativas y técnicas para proteger los datos de los usuarios, garantizar la seguridad y confidencialidad de los datos, y también garantizar el cumplimiento de los derechos de los usuarios garantizados por la legislación vigente. 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 las situaciones descritas pueden clasificarse como datos personales de acuerdo con su legislación o norma local, debe asegurarse de que dichos datos se procesen legalmente y de obtener el consentimiento de los usuarios finales para la recopilación y la 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_<identificador del idioma>.txt contienen el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network y están incluidos en el kit de distribución.

Si no desea transmitir datos a Kaspersky, puede deshabilitar el suministro de datos.

Uso de Kaspersky Security Network

Al utilizar Kaspersky Security Network, acepta proporcionar automáticamente los datos indicados en la Declaración de Kaspersky Security Network. Si no acepta proporcionar estos datos a Kaspersky, utilice Kaspersky Private Security Network (KPSN) o deshabilite el uso de KSN. Para obtener más información sobre KPSN, consulte la documentación de Kaspersky Private Security Network.

Activar la aplicación con un código de activación nuevo

Al utilizar un código de activación, acepta proporcionar automáticamente los datos enumerados en el Contrato de licencia de usuario final. Si no está de acuerdo en suministrar estos datos con Kaspersky, utilice un archivo de clave para activar Kaspersky Endpoint Security.

Actualizar módulos de aplicaciones y bases de datos antivirus

Al utilizar los servidores de Kaspersky, acepta proporcionar automáticamente los datos indicados 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.

Seguir vínculos en la interfaz de la aplicación

Al utilizar los vínculos en la interfaz de la aplicación, acepta proporcionar automáticamente los datos indicados en el Contrato de licencia de usuario final. La lista precisa de datos transmitidos en cada vínculo específico depende de dónde se encuentra el vínculo en la interfaz de la aplicación y del problema que pretende resolver. Si no acepta proporcionar estos datos a Kaspersky, utilice la interfaz de la aplicación simplificada u oculte la interfaz de la aplicación.

Creación de archivos de volcado

Si ha habilitado la escritura de volcado, Kaspersky Endpoint Security creará un archivo de volcado que incluirá todos los datos de la memoria de los procesos de la aplicación en el momento en que se creó este archivo de volcado.

Avisos de marca registrada

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Adobe, Acrobat, Flash, Reader y Shockwave son marcas comerciales registradas o marcas comerciales de Adobe en los Estados Unidos u otros países.

Amazon, Amazon Web Services y AWS son marcas comerciales de Amazon.com, Inc. o de 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 filiales) en EE. UU. o en otros países.

AutoCAD es una marca comercial o una marca registrada de Autodesk, Inc. y/o sus filiales y/o sus empresas vinculadas en los Estados Unidos y/o en otros países.

La palabra Bluetooth y la marca y los logotipos asociados son propiedad de Bluetooth SIG, Inc.

Borland es una marca comercial o una marca registrada de Borland Software Corporation.

Cisco, Cisco AnyConnect y IOS son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. o de sus empresas afiliadas en los Estados Unidos y en algunos 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 subsidiarias.

dBase es una marca comercial 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 o marcas registradas de Docker, Inc. en los Estados Unidos o en otros países. Docker, Inc. y otras partes también pueden tener derechos de marca registrada en otros términos usados en este documento.

ESET es una marca comercial o marca registrada de ESET spol. s.r.o. o entidad de ESET respectiva.

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 comercial o marca de servicio de ICQ LLC.

Intel es la marca comercial de Intel Corporation o sus subsidiarias.

IBM es una marca comercial de International Business Machines Corporation, registrada en muchas jurisdicciones del mundo.

Lenovo y Lenovo ThinkPad son marcas comerciales de Lenovo en los Estados Unidos o en otros sitios.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca registrada o una marca comercial de Logitech en los Estados Unidos y/o en otros países.

LogMeIn Pro y Remotely Anywhere son marcas registradas de LogMeIn, Inc.

Mail.ru es una marca comercial de Mail.ru LLC.

McAfee es la marca comercial o la marca comercial registrada de McAfee LLC o sus subsidiarias 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 la Fundación Mozilla en EE. UU. y otros países.

NetApp es una marca comercial o marca registrada de NetApp, Inc. en los Estados Unidos o en otros países.

OpenSSL es una marca comercial de OpenSSL Software Foundation.

OpenStack es una marca comercial registrada de OpenStack Foundation en los Estados Unidos y en otros países.

Oracle, Java y JavaScript son marcas registradas de Oracle Corporation y/o de sus empresas vinculadas.

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 y otros países.

Thawte es una marca comercial o marca comercial registrada de Symantec Corporation o de sus empresas vinculadas en los Estados Unidos y en otros países.

Trend Micro es una marca comercial o una marca registrada de Trend Micro Incorporated.

VERISIGN es una marca comercial 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 comerciales registradas o marcas comerciales de VMware, Inc. en los Estados Unidos y otros países.

Información acerca de código de terceros

La información acerca del código de terceros se incluye en el archivo legal_notices.txt, ubicado en la carpeta de instalación de la aplicación.