

**kaspersky**

# **Kaspersky Endpoint Security para Windows 11.8.0**

© 2023 AO Kaspersky Lab

# Contenido

[Preguntas frecuentes](#)

[Novedades](#)

[Kaspersky Endpoint Security para Windows](#)

[Kit de distribución](#)

[Requisitos de hardware y software](#)

[Comparación de funciones disponibles en la aplicación según el tipo de sistema operativo](#)

[Comparación: disponibilidad de características por herramienta de administración](#)

[Compatibilidad con otras aplicaciones](#)

[Instalación y eliminación de la aplicación](#)

[Despliegue a través de Kaspersky Security Center](#)

[Instalación estándar de la aplicación](#)

[Creación de un paquete de instalación](#)

[Actualización de bases de datos en el paquete de instalación](#)

[Creación de una tarea de instalación remota](#)

[Instalación de la aplicación de manera local mediante el Asistente de instalación](#)

[Instalando remotamente la aplicación usando System Center Configuration Manager](#)

[Descripción de la configuración de instalación del archivo setup.ini](#)

[Cambiar componentes de la aplicación](#)

[Actualización de una versión anterior de la aplicación](#)

[Eliminar la aplicación](#)

[Desinstalación a través de Kaspersky Security Center](#)

[Desinstalación de la aplicación mediante el Asistente de instalación](#)

[Licencias de la aplicación](#)

[Acerca del Contrato de licencia de usuario final](#)

[Acerca de la licencia](#)

[Acerca del certificado de la licencia](#)

[Acerca de la suscripción](#)

[Sobre una clave de licencia](#)

[Acerca del código de activación](#)

[Acerca del archivo clave](#)

[Comparación de la funcionalidad de la aplicación según el tipo de licencia para las estaciones de trabajo](#)

[Comparación de la funcionalidad de la aplicación según el tipo de licencia para servidores](#)

[Activación de la aplicación](#)

[Activación de la aplicación a través de Kaspersky Security Center](#)

[Uso del asistente de activación para activar la aplicación](#)

[Visualización de información de la licencia](#)

[Compra de una licencia](#)

[Renovación de suscripciones](#)

[Provisión de datos](#)

[Provisión de datos según el Contrato de licencia de usuario final](#)

[Provisión de datos al usar Kaspersky Security Network](#)

[Provisión de datos al usar soluciones de Detection and Response](#)

[Kaspersky Endpoint Detection and Response](#)

[Kaspersky Sandbox](#)

[Cumplimiento de la legislación de la Unión Europea \(GDPR\)](#)

[Primeros pasos](#)

[Acerca del Complemento de administración de Kaspersky Endpoint Security para Windows](#)

[Consideraciones especiales cuando se trabaja con distintas versiones de complementos de administración](#)

[Consideraciones especiales al utilizar protocolos cifrados para interactuar con servicios externos](#)

[Interfaz de la aplicación](#)

[Icono de la aplicación en el área de notificaciones de la barra de tareas](#)

[Interfaz simplificada de la aplicación](#)

[Configuración de la visualización de la interfaz de la aplicación](#)

[Primeros pasos](#)

[Gestión de directivas](#)

[Gestión de tareas](#)

[Configuración de los ajustes locales de la aplicación](#)

[Inicio y detención de Kaspersky Endpoint Security](#)

[Suspensión y reanudación de Protección y control del equipo](#)

[Crear y utilizar un archivo de configuración](#)

[Restaurar la configuración predeterminada de la aplicación](#)

[Análisis antivirus del equipo](#)

[Análisis del equipo](#)

[Análisis de unidades extraíbles cuando se conectan al equipo](#)

[Análisis en segundo plano](#)

[Analizar desde el menú contextual](#)

[Control de integridad de la aplicación](#)

[Edición de la cobertura del análisis](#)

[Análisis programado en ejecución](#)

[Ejecutar un análisis como un usuario diferente](#)

[Optimización del análisis](#)

[Actualización de las bases de datos y módulos de la aplicación](#)

[Escenarios de actualización de las bases de datos y los módulos de la aplicación](#)

[Actualización con un repositorio de servidor](#)

[Actualización con una carpeta compartida](#)

[Actualización con Kaspersky Update Utility](#)

[Actualización en modo móvil](#)

[Inicio y parada de una tarea de actualización](#)

[Inicio de una tarea de actualización con los permisos de una cuenta de usuario distinta](#)

[Selección del modo de ejecución de la tarea de actualización](#)

[Adición de un origen de actualizaciones](#)

[Configuración de actualización desde una carpeta compartida](#)

[Actualización de los módulos de la aplicación](#)

[Actualización mediante un servidor proxy](#)

[Reversión de la última actualización](#)

[Trabajar con amenazas activas](#)

[Desinfección de amenazas activas en estaciones de trabajo](#)

[Desinfección de amenazas activas en servidores](#)

[Activación o desactivación de la tecnología de desinfección avanzada](#)

[Procesamiento de amenazas activas](#)

[Protección del equipo](#)

[Protección frente a amenazas en archivos](#)

[Activación y desactivación de Protección frente a amenazas en archivos](#)

[Suspensión automática de Protección frente a amenazas en archivos](#)

[Modificación de las acciones tomadas en archivos infectados por parte del componente Protección frente a amenazas en archivos](#)

[Formación la cobertura de protección del componente Protección frente a amenazas en archivos](#)

[Uso de métodos de análisis](#)

[Utilización de las tecnologías de análisis en el funcionamiento del componente Protección frente a amenazas en archivos](#)

[Optimización del análisis de archivos](#)

[Análisis de archivos compuestos](#)

[Modificación del modo de análisis](#)

[Protección frente a amenazas web](#)

[Activación y desactivación de Protección frente a amenazas web](#)

[Modificación de las acciones que se van a realizar en objetos maliciosos del tráfico web](#)

[Análisis de URL contra bases de datos de phishing y direcciones web maliciosas](#)

[Utilización del análisis heurístico en el funcionamiento del componente Protección frente a amenazas web](#)

[Creación de la lista de direcciones web de confianza](#)

[Exportación e importación de la lista de direcciones web de confianza](#)

[Protección frente a amenazas en el correo](#)

[Activación y desactivación de Protección frente a amenazas en el correo](#)

[Modificación de las acciones que se van a realizar en mensajes de correo electrónico infectados](#)

[Formación la cobertura de protección del componente de Protección frente a amenazas en el correo](#)

[Analizar archivos compuestos adjuntos a mensajes de correo electrónico](#)

[Filtro de archivos adjuntos de mensajes de correo electrónico](#)

[Exportación e importación de extensiones para filtrado de adjuntos](#)

[Análisis de correos electrónicos en Microsoft Office Outlook](#)

[Protección frente a amenazas en la red](#)

[Activación y desactivación de Protección frente a amenazas en la red](#)

[Bloquear un equipo atacante](#)

[Configurar direcciones de exclusiones de bloqueo](#)

[Exportación e importación de la lista de exclusiones de bloqueo](#)

[Configurar la protección contra ataques a la red por tipo](#)

[Firewall](#)

[Activación y desactivación de Firewall](#)

[Modificación del estado de la conexión de red](#)

[Gestión de las reglas de paquetes de red](#)

[Crear una regla de paquetes de red](#)

[Activación o desactivación de una regla de paquetes de red](#)

[Modificación de la acción de Firewall para una regla de paquetes de red](#)

[Modificación de la prioridad de una regla de paquetes de red](#)

[Exportación e importación de reglas de paquetes de red](#)

[Gestionar reglas de red de la aplicación](#)

[Crear una regla de red de aplicaciones](#)

[Activar y desactivar una regla de red de la aplicación](#)

[Modificación de la acción de Firewall para una regla de red de la aplicación](#)

[Modificación de la prioridad de una regla de red de la aplicación](#)

[Monitor de red](#)

[Prevención de ataques de BadUSB](#)

[Activación y desactivación de Prevención de ataques de BadUSB](#)

[Usar el teclado en pantalla para la autorización de dispositivos USB](#)

[Protección AMSI](#)

[Activación y desactivación de la protección AMSI](#)

[Uso de la protección AMSI para analizar archivos compuestos](#)

#### [Prevención de exploits](#)

[Activación y desactivación de Prevención de vulnerabilidades](#)

[Selección de la acción que se realizará al detectar una vulnerabilidad](#)

[Protección de la memoria de los procesos del sistema](#)

#### [Detección de comportamiento](#)

[Activar y desactivar Detección de comportamiento](#)

[Selección de la acción que se debe tomar al detectar actividad de malware](#)

[Protección de carpetas compartidas frente a cifrado externo](#)

[Activación y desactivación de la protección de carpetas compartidas frente al cifrado externo](#)

[Selección de la acción que se debe tomar al detectar el cifrado externo de carpetas compartidas](#)

[Creación de una exclusión para la protección de carpetas compartidas frente a cifrado externo](#)

[Configuración de exclusión de direcciones en Protección de carpetas compartidas frente a cifrado externo.](#)

[Exportar e importar una lista de exclusiones a la protección de carpetas compartidas frente a cifrado externo](#)

#### [Prevención de intrusiones en el host](#)

[Activación y desactivación de Prevención de intrusiones en el host](#)

[Gestionar grupos de confianza de aplicaciones](#)

[Cambiar el grupo de confianza de una aplicación](#)

[Configuración de derechos del grupo de confianza](#)

[Seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security.](#)

[Selección de un grupo de confianza para aplicaciones desconocidas](#)

[Seleccionar un grupo de confianza para aplicaciones firmadas digitalmente](#)

[Administración de los derechos de las aplicaciones](#)

[Protección de recursos del sistema operativo y de datos personales](#)

[Eliminación de información sobre aplicaciones sin uso](#)

[Control de prevención de intrusiones en el host](#)

[Protección del acceso a audio y vídeo](#)

#### [Motor de reparación](#)

##### [Kaspersky Security Network](#)

[Activación y desactivación del uso de Kaspersky Security Network](#)

[Limitaciones de KSN privado](#)

[Activar y desactivar el modo Cloud para los componentes de protección](#)

[Configuración del proxy de KSN](#)

[Comprobar la reputación de un archivo en Kaspersky Security Network](#)

##### [Análisis de conexiones cifradas](#)

[Configuración los parámetros del análisis de conexiones cifradas.](#)

[Analizar conexiones cifradas en Firefox y Thunderbird](#)

[Exclusión de conexiones cifradas del análisis](#)

##### [Eliminación de datos](#)

#### [Control del equipo](#)

##### [Control Web](#)

[Activación y desactivación de Control Web](#)

[Acciones con reglas de acceso a recursos web](#)

[Adición de una regla de acceso a recursos web](#)

[Asignación de prioridades a reglas de acceso a recursos web](#)

[Activación y desactivación de una regla de acceso a recursos web](#)

[Exportación e importación de la lista de direcciones web de confianza](#)

[Comprobación de las reglas de acceso a recursos web](#)

[Exportación e importación de la lista de direcciones de recursos web](#)

[Supervisión de las actividades de los usuarios en Internet](#)

[Edición de plantillas de mensajes de Control Web](#)

[Edición de máscaras para direcciones de recursos web](#)

[Migración de reglas de acceso a recursos web de las versiones previas de la aplicación](#)

#### [Control de dispositivos](#)

[Activación y desactivación del Control de dispositivos](#)

[Sobre las reglas de acceso](#)

[Edición de una regla de acceso a dispositivos](#)

[Edición de una regla de acceso a bus de conexión](#)

[Añadir una red wifi a la lista de confianza](#)

[Seguimiento del uso de unidades extraíbles](#)

[Cambiar la duración del almacenamiento en caché](#)

[Acciones con dispositivos de confianza](#)

[Adición de un dispositivo a la lista de confianza en la interfaz de la aplicación](#)

[Adición de un dispositivo a la lista de confianza desde Kaspersky Security Center](#)

[Exportación e importación de la lista de dispositivos de confianza](#)

[Obtención de acceso a un dispositivo bloqueado](#)

[Modo con conexión para otorgar acceso](#)

[Modo sin conexión para otorgar acceso](#)

[Edición de plantillas de mensajes de Control de dispositivos](#)

[Anti-Bridging](#)

[Activar el componente Anti-Bridging](#)

[Cambio del estado de una regla de conexión](#)

[Cambio de la prioridad de una regla de conexión](#)

#### [Control de anomalías adaptativo](#)

[Activación y desactivación del Control de anomalías adaptativo](#)

[Activación y desactivación de una regla del Control de anomalías adaptativo](#)

[Cambio de la acción que se realiza al activarse una regla del Control de anomalías adaptativo](#)

[Crear una exclusión de una regla del Control de anomalías adaptativo](#)

[Importar e importar exclusiones para las reglas del Control de anomalías adaptativo](#)

[Actualización de las reglas del Control de anomalías adaptativo](#)

[Modificación de las plantillas de mensajes del Control de anomalías adaptativo](#)

[Visualización de informes del Control de anomalías adaptable](#)

#### [Control de aplicaciones](#)

[Limitaciones de funcionalidad de Control de aplicaciones](#)

[Activación y desactivación de Control de aplicaciones](#)

[Seleccionar el modo de Control de aplicaciones](#)

[Trabajar con reglas de Control de aplicaciones en la interfaz de la aplicación](#)

[Adición de una regla de Control de aplicaciones](#)

[Adición de una condición de activación para una regla de Control de aplicaciones](#)

[Cambiar el estado de una regla de Control de aplicaciones](#)

[Administrar las reglas de Control de aplicaciones en Kaspersky Security Center](#)

[Recepción de información sobre las aplicaciones que se instalan en equipos de usuarios](#)

[Creación de categorías de aplicaciones](#)

[Añadir archivos ejecutables desde la carpeta Archivos ejecutables a la categoría de aplicación](#)

[Añadir archivos ejecutables relacionados con eventos a la categoría de aplicación](#)

[Añadir y modificar una regla de Control de aplicaciones con Kaspersky Security Center](#)  
[Cambiar el estado de una regla de Control de aplicaciones mediante Kaspersky Security Center](#)  
[Exportación e importación de reglas de Control de aplicaciones](#)  
[Comprobación de las reglas de Control de aplicaciones con Kaspersky Security Center](#)  
[Ver eventos resultantes de la comprobación del funcionamiento del componente Control de aplicaciones](#)  
[Ver un informe sobre las aplicaciones bloqueadas en el modo de prueba](#)  
[Ver eventos resultantes del funcionamiento del componente Control de aplicaciones](#)  
[Ver un informe sobre aplicaciones bloqueadas](#)

[Probar reglas de Control de aplicaciones](#)

[Supervisión de la actividad de aplicaciones](#)

[Reglas para crear máscaras de nombre para archivos o carpetas](#)

[Edición de plantillas de mensajes de Control de aplicaciones](#)

[Mejores prácticas para implementar una lista de aplicaciones permitidas](#)

[Configuración del modo de lista de admitidos para aplicaciones](#)

[Prueba del modo de lista de admitidos](#)

[Soporte para el modo de lista de admitidos](#)

[Supervisión de puertos de red](#)

[Activación de la vigilancia de todos los puertos de red](#)

[Creación de una lista de puertos de red supervisados](#)

[Creación de una lista de aplicaciones para las que se supervisan todos los puertos de red](#)

[Exportación e importación de listas de puertos vigilados](#)

[Protección con contraseña](#)

[Activar la protección con contraseña](#)

[Otorgarle permisos a usuarios o grupos individuales](#)

[Utilizar una contraseña temporal para otorgar permisos](#)

[Aspectos especiales de los permisos de la protección con contraseña](#)

[Zona de confianza](#)

[Creación de una exclusión del análisis](#)

[Activación y desactivación de una exclusión del análisis](#)

[Selección de los tipos de objetos detectables](#)

[Edición de la lista de aplicaciones de confianza](#)

[Activación y desactivación de reglas de la zona de confianza para una aplicación en la lista de aplicaciones de confianza](#)

[Uso del almacén de certificados de confianza del sistema](#)

[Gestión de Copia de seguridad](#)

[Configuración del período de almacenamiento máximo de archivos en Copia de seguridad](#)

[Configuración del tamaño máximo de Copia de seguridad](#)

[Restauración de archivos de Copia de seguridad](#)

[Eliminación de las copias de seguridad de los archivos de Copia de seguridad](#)

[Servicio de notificaciones](#)

[Configuración de los parámetros de registro de eventos](#)

[Configuración de la visualización y entrega de notificaciones](#)

[Configuración de la visualización de advertencias sobre el estado de la aplicación en el área de notificaciones](#)

[Mensajes entre los usuarios y el administrador](#)

[Gestión de informes](#)

[Ver informes](#)

[Configuración del período máximo de almacenamiento del informe](#)

[Configuración del tamaño máximo del archivo del informe](#)

[Almacenamiento de informes en archivos](#)

[Limpieza de informes](#)

[Autoprotección de Kaspersky Endpoint Security](#)

[Activación y desactivación de Autoprotección](#)

[Activación y desactivación de la compatibilidad con AM-PPL](#)

[Activación y desactivación de protección de gestión externa](#)

[Soporte de las aplicaciones de administración remota](#)

[Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones](#)

[Activación o desactivación del modo de ahorro de energía](#)

[Activación o desactivación de la concesión de recursos a otras aplicaciones](#)

[Prácticas recomendadas para optimizar el rendimiento de Kaspersky Endpoint Security](#)

[Cifrado de datos](#)

[Limitaciones de funcionalidad del cifrado](#)

[Cómo cambiar la longitud de la clave de cifrado \(AES56 o AES256\)](#)

[Cifrado de disco de Kaspersky](#)

[Características especiales del cifrado de unidades SSD](#)

[Cifrado de disco completo con la tecnología Cifrado de disco de Kaspersky](#)

[Creación de una lista de discos duros excluidos del cifrado](#)

[Exportar e importar una lista de discos duros excluidos del cifrado](#)

[Activación de la tecnología de inicio de sesión único \(SSO\)](#)

[Administración de cuentas del Agente de autenticación](#)

[Utilizar una tarjeta inteligente y un token con el Agente de autenticación](#)

[Descifrado de discos duros](#)

[Restauración del acceso a una unidad protegida por la tecnología Cifrado de disco de Kaspersky](#)

[Actualización del sistema operativo](#)

[Eliminación de errores al actualizar la función de cifrado](#)

[Seleccionar el nivel de rastreo del Agente de autenticación](#)

[Editar los textos de ayuda del Agente de autenticación](#)

[Eliminar los objetos y datos restantes después de probar el Agente de autenticación](#)

[Administración de BitLocker](#)

[Inicio del Cifrado de unidad BitLocker](#)

[Descifrado de un disco duro protegido por BitLocker](#)

[Restauración del acceso a una unidad protegida por BitLocker](#)

[Pausar la protección de BitLocker para actualizar el software](#)

[Cifrado de archivos en unidades locales del equipo](#)

[Cifrado de los archivos de las unidades del equipo local](#)

[Creación de reglas de acceso a archivos cifrados para aplicaciones](#)

[Cifrar archivos creados o modificados por aplicaciones específicas](#)

[Generación de una regla de descifrado](#)

[Descifrado de archivos de las unidades del equipo local](#)

[Creación de paquetes cifrados](#)

[Restauración del acceso a los archivos cifrados](#)

[Restauración del acceso a los datos cifrados después del error del sistema operativo](#)

[Modificación de plantillas de mensajes de acceso a archivos cifrados](#)

[Cifrado de unidades extraíbles](#)

[Iniciar el cifrado de unidades extraíbles](#)

[Añadir una regla de cifrado para unidades extraíbles](#)

[Exportación e importación de una lista de reglas de cifrado para unidades extraíbles](#)

[Modo portátil para acceder a archivos cifrados de unidades extraíbles](#)



[Descifrado de unidades extraíbles](#)

[Visualización de los detalles del cifrado de datos](#)

[Ver el estado de cifrado](#)

[Ver las estadísticas del cifrado en los paneles de Kaspersky Security Center](#)

[Ver errores de cifrado de archivos en unidades del equipo local](#)

[Visualización del informe del cifrado de datos](#)

[Trabajar con dispositivos cifrados cuando no hay acceso a estos](#)

[Recuperación de datos mediante la Utilidad de restauración FDERT](#)

[Creación de un disco de rescate del sistema operativo](#)

[Componentes de Detection and Response.](#)

[Kaspersky Endpoint Agent](#)

[Migración de directivas y tareas para Kaspersky Endpoint Agent](#)

[Migrar la configuración \[KES + KEA\] a la configuración \[KES + agente incorporado\]](#)

[Managed Detection and Response](#)

[Integración con MDR](#)

[Migración desde Kaspersky Endpoint Agent](#)

[Endpoint Detection and Response](#)

[Integración con Kaspersky Endpoint Detection and Response](#)

[Migración desde Kaspersky Endpoint Agent](#)

[Analizar en busca de indicadores de compromiso \(tarea estándar\)](#)

[Mover archivo a la cuarentena](#)

[Obtener archivo](#)

[Eliminar el archivo](#)

[Inicio del proceso](#)

[Terminar proceso](#)

[Prevención de ejecución](#)

[Aislamiento de equipos de la red](#)

[Apéndice 1. Extensiones de archivos compatibles con la Prevención de ejecución](#)

[Apéndice 2. Intérpretes de scripts compatibles](#)

[Apéndice 3. Cobertura de análisis de IOC en el registro \(RegistryItem\)](#)

[Apéndice 4. Requisitos de los archivos de IOC](#)

[Kaspersky Sandbox](#)

[Integración con Kaspersky Sandbox](#)

[Migración desde Kaspersky Endpoint Agent](#)

[Añadir un certificado TLS](#)

[Añadir servidores de Kaspersky Sandbox](#)

[Analizar en busca de indicadores de compromiso \(tarea independiente\)](#)

[Administración de Cuarentena](#)

[Configuración del tamaño máximo de Cuarentena](#)

[Envío de datos sobre archivos en Cuarentena a Kaspersky Security Center](#)

[Kaspersky Security para Windows Server](#)

[Instalación de KES encima de KSWS](#)

[Activación de KES con una clave de KSWS](#)

[Administración de la aplicación desde la línea de comandos](#)

[Instalación de la aplicación](#)

[Activación de la aplicación](#)

[Eliminar la aplicación](#)

[Comandos AVP](#)

[SCAN. Análisis antivirus](#)  
[UPDATE. Actualización de las bases de datos y módulos de la aplicación](#)  
[ROLLBACK. Reversión de la última actualización](#)  
[TRACES. Rastreo](#)  
[START. Iniciar un perfil](#)  
[STOP. Detener un perfil](#)  
[STATUS. Estado del perfil](#)  
[STATISTICS. Estadísticas sobre el funcionamiento de los perfiles](#)  
[RESTORE. Restauración de archivos de Copia de seguridad](#)  
[EXPORT. Exportar ajustes de la aplicación](#)  
[IMPORT. Importar configuración de la aplicación](#)  
[ADDKEY. Aplicar un archivo clave.](#)  
[LICENSE. Administración de licencias](#)  
[RENEW. Compra de una licencia](#)  
[PBATESTRESET. Restablecer los resultados de la comprobación de disco antes de cifrar el disco](#)  
[EXIT. Salir de la aplicación](#)  
[EXITPOLICY. Desactivar una directiva](#)  
[STARTPOLICY. Activar una directiva](#)  
[DISABLE. Desactivar la protección](#)  
[SPYWARE. Detección de spyware](#)  
[KSN. Transición de KSN global/privada](#)

#### [Comandos KESCLI](#)

[Scan. Análisis antivirus](#)  
[GetScanState. Estado de finalización del análisis](#)  
[GetLastScanTime. Especificación del tiempo para completar el análisis](#)  
[GetThreats. Obtención de datos sobre amenazas detectadas](#)  
[UpdateDefinitions. Actualización de las bases de datos y módulos de la aplicación](#)  
[GetDefinitionState. Especificación del tiempo para completar la actualización](#)  
[EnableRTP. Activación de la protección](#)  
[GetRealTimeProtectionState. Estado de la Protección frente a amenazas en archivos](#)  
[Version. Identificación de la versión de la aplicación](#)

#### [Comandos de administración de Detection and Response](#)

[SANDBOX. Administrar Kaspersky Sandbox](#)  
[PREVENCIÓN. Administración de la prevención de ejecución](#)  
[AISLAMIENTO. Administrar el aislamiento de red](#)  
[RESTORE. Restauración de archivos de la cuarentena](#)  
[IOCSCAN. Analizar en busca de indicadores de compromiso \(IOC\)](#)  
[MDRLICENSE. Activación MDR](#)

#### [Códigos de error](#)

[Apéndice. Perfiles de la aplicación](#)

#### [Administrar la aplicación a través de la API REST](#)

[Instalar la aplicación con la API REST](#)

[Funcionamiento con la API](#)

#### [Fuentes de información de la aplicación](#)

#### [Cómo ponerse en contacto con el Soporte técnico](#)

[Contenido y almacenamiento de archivos de seguimiento](#)

[Rastreo del funcionamiento de aplicaciones](#)

[Rastreo del rendimiento de aplicaciones](#)

[Escritura de volcado](#)

[Protección de archivos de volcado y archivos de seguimiento](#)

[Limitaciones y advertencias](#)

[Glosario](#)

[Administrador de archivos portátil](#)

[Agente de autenticación](#)

[Agente de red](#)

[Archivador](#)

[Archivo de IOC](#)

[Archivo infectable](#)

[Archivo infectado](#)

[Base de datos de direcciones web maliciosas](#)

[Base de datos de direcciones web phishing](#)

[Bases de datos antivirus](#)

[Certificado de licencia](#)

[Clave activa](#)

[Clave adicional](#)

[Cobertura de protección](#)

[Cobertura del análisis](#)

[Desinfección](#)

[Emisor del certificado](#)

[Falsa alarma](#)

[Forma normalizada de la dirección de un recurso web](#)

[Grupo de administración](#)

[IOC](#)

[Máscara](#)

[Módulo de plataforma segura](#)

[Objeto OLE](#)

[OpenIOC](#)

[Tarea](#)

[Apéndices](#)

[Apéndice 1. Configuración de la aplicación](#)

[Protección frente a amenazas en archivos](#)

[Protección frente a amenazas web](#)

[Protección frente a amenazas en el correo](#)

[Protección frente a amenazas en la red](#)

[Firewall](#)

[Prevención de ataques de BadUSB](#)

[Protección AMSI](#)

[Prevención de exploits](#)

[Detección de comportamiento](#)

[Prevención de intrusiones en el host](#)

[Motor de reparación](#)

[Kaspersky Security Network](#)

[Control Web](#)

[Control de dispositivos](#)

[Control de aplicaciones](#)

[Control de anomalías adaptativo](#)

[Sensor de Endpoint](#)  
[Kaspersky Sandbox](#)  
[Endpoint Detection and Response](#)  
[Cifrado de disco completo](#)  
[Cifrado de archivos](#)  
[Cifrado de unidades extraíbles](#)  
[Plantillas \(cifrado de datos\)](#)  
[Exclusiones](#)  
[Configuración de la aplicación](#)  
[Informes y almacenamiento](#)  
[Configuración de red](#)  
[Interfaz](#)  
[Administrar configuración](#)  
[Actualización de las bases de datos y módulos de la aplicación](#)  
[Apéndice 2. Grupos de confianza de aplicaciones](#)  
[Apéndice 3. Extensiones de archivo para el análisis rápido de unidades extraíbles](#)  
[Apéndice 4. Tipos de archivo para el filtrado de adjuntos Protección frente a amenazas en el correo](#)  
[Apéndice 5. Configuración de red para la interacción con servicios externos](#)  
[Apéndice 6. Eventos de la aplicación en el Registro de eventos de Windows](#)  
[Apéndice 7. Eventos de la aplicación en el registro de eventos de Kaspersky Security Center](#)  
[Información sobre el código de terceros](#)  
[Información de marcas registradas](#)

# Preguntas frecuentes



## GENERAL

[¿En qué equipos puedo usar Kaspersky Endpoint Security?](#)

[¿Qué ha cambiado desde la última versión?](#)

[¿Con qué otras aplicaciones de Kaspersky puede funcionar Kaspersky Endpoint Security?](#)

[¿Cómo puedo reducir el impacto de Kaspersky Endpoint Security en los recursos del equipo?](#)



## INSTALACIÓN

[¿Cómo puedo instalar Kaspersky Endpoint Security en todos los equipos de mi organización?](#)

[¿Qué parámetros de instalación puedo configurar en la línea de comandos?](#)

[¿Cómo puedo desinstalar Kaspersky Endpoint Security de forma remota?](#)



## ACTUALIZACIÓN

[¿Cuáles son los métodos para actualizar las bases de datos?](#)

[¿Qué debo hacer si surgen problemas después de una actualización?](#)

[¿Cómo actualizo las bases de datos fuera de la red corporativa?](#)

[¿Puedo usar un servidor proxy para realizar una actualización?](#)



## SEGURIDAD

[¿Cómo analiza Kaspersky Endpoint Security el correo electrónico?](#)

[¿Cómo evito que un archivo de confianza se analice?](#)

[¿Cómo protejo el equipo contra las unidades flash infectadas?](#)

[¿Cómo puedo realizar un análisis antivirus sin que el usuario lo sepa?](#)

[¿Cómo pongo en pausa la protección de Kaspersky Endpoint Security?](#)

[¿Cómo restauro un archivo que Kaspersky Endpoint Security ha eliminado por error?](#)

[¿Cómo puedo evitar que los usuarios desinstalen Kaspersky Endpoint Security?](#)



## INTERNET

[¿Es posible analizar conexiones cifradas \(HTTPS\) con Kaspersky Endpoint Security?](#)

[¿Qué debo hacer para que los usuarios solo puedan conectarse a redes wifi de confianza?](#)

[¿Cómo bloqueo las redes sociales?](#)



## APLICACIONES

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

[¿Cómo evito que se ejecuten videojuegos?](#)

[¿Cómo verifico si Control de aplicaciones se ha configurado correctamente?](#)

[¿Cómo añado una aplicación a la lista de aplicaciones de confianza?](#)



## DISPOSITIVOS

[¿Cómo puedo impedir el uso de unidades flash?](#)

[¿Cómo añado un dispositivo a la lista de dispositivos de confianza?](#)

[¿Es posible obtener acceso a un dispositivo bloqueado?](#)



## CIFRADO

[¿En qué casos no es posible usar las funciones de cifrado?](#)

[¿Cómo puedo restringir con contraseña el acceso a un archivo de almacenamiento?](#)

[¿Puedo usar una tarjeta inteligente o un token con las funciones de cifrado?](#)

[¿Puedo acceder a los archivos que cifre si no tengo conexión con Kaspersky Security Center?](#)

[¿Qué debo hacer ante un problema con el sistema operativo si mi información está cifrada?](#)



## SOPORTE

[¿Dónde se guardan los archivos de los informes?](#)

[¿Cómo creo un archivo de seguimiento?](#)

[¿Cómo activo la creación de archivos de volcado?](#)

# Novedades

## Actualización 11.8.0

Kaspersky Endpoint Security 11.8.0 para Windows ofrece las siguientes características y mejoras:

1. [Se añadió el agente integrado para respaldar el funcionamiento de la solución Kaspersky Endpoint Detection and Response Expert](#). *Kaspersky Endpoint Detection and Response Expert* es una solución para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre la solución, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).
2. La interfaz del [Monitor de red](#) ya está mejorada. El Monitor de red ahora muestra el protocolo UDP además de TCP.
3. Se optimizó la tarea de [Análisis antivirus](#). Si ha reiniciado el equipo durante el análisis, Kaspersky Endpoint Security ejecuta automáticamente la tarea, continuando desde el punto donde se interrumpió el análisis.
4. Ahora puede establecer un límite para el tiempo de ejecución de la tarea. Puede limitar el tiempo de ejecución para las tareas *Análisis antivirus* y *Análisis de IOC*. Tras el periodo de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. Para reducir el tiempo de ejecución de la tarea *Análisis antivirus*, puede [configurar el alcance del análisis](#) u [optimizar el análisis](#).
5. Las limitaciones de las plataformas de servidor se levantan para la aplicación instalada en Windows 10 Enterprise multisesión. Kaspersky Endpoint Security ahora considera a Windows 10 Enterprise multisesión como un sistema operativo de estación de trabajo, no como un sistema operativo de servidor. En consecuencia, [las limitaciones de la plataforma del servidor](#) ya no se aplican a la aplicación en la multisesión de Windows 10 Enterprise. La aplicación también utiliza una clave de licencia de estación de trabajo para la activación en lugar de una clave de licencia de servidor.

## Actualización 11.7.0

Kaspersky Endpoint Security para Windows 11.7.0 ofrece las siguientes funciones y mejoras nuevas:

1. La [interfaz de Kaspersky Endpoint Security para Windows](#) se actualiza.
2. [Soporte de Windows 11, Windows 10 21H2 y Windows Server 2022](#).
3. Nuevos componentes añadidos:
  - Se añadió [un agente integrado para integración con Kaspersky Sandbox](#). *La solución Kaspersky Sandbox* detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Kaspersky 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. Kaspersky Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Kaspersky Sandbox). Para obtener más información acerca de la solución, consulte la [Ayuda de Kaspersky Sandbox](#).

Ya no necesita Kaspersky Endpoint Agent para utilizar Kaspersky Sandbox. Kaspersky Endpoint Security puede realizar todas las funciones de Kaspersky Endpoint Agent. Para migrar las directivas de Kaspersky Endpoint Agent, utilice el [Asistente de migración](#). Necesita Kaspersky Security Center 13.2 para que todas las funciones de Kaspersky Sandbox estén disponibles. Para obtener información acerca de la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, consulte la [ayuda de la aplicación](#).

- [Se añadió el agente integrado para respaldar el funcionamiento de la solución Kaspersky Endpoint Detection and Response Optimum](#). *Kaspersky Endpoint Detection and Response Optimum* es una solución para proteger la infraestructura de TI de la organización de las amenazas cibernéticas avanzadas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. Para obtener más información sobre la solución, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#).

Ya no necesita Kaspersky Endpoint Agent para utilizar Kaspersky Endpoint Detection and Response. Kaspersky Endpoint Security puede realizar todas las funciones de Kaspersky Endpoint Agent. Para migrar las directivas y tareas de Kaspersky Endpoint Agent, utilice el [Asistente de migración](#). Para utilizar todas las funciones, Kaspersky Endpoint Detection and Response Optimum requiere Kaspersky Security Center 13.2. Para obtener información acerca de la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, consulte la [ayuda de la aplicación](#).

4. Se añadió el [Asistente de migración](#) de directivas y tareas de Kaspersky Endpoint Agent. El Asistente de migración crea directivas y tareas nuevas unificadas para Kaspersky Endpoint Security para Windows. El asistente permite cambiar las soluciones de Detection and Response desde Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Las soluciones de Detection and Response incluyen Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) y Kaspersky Managed Detection and Response (MDR).

5. [Kaspersky Endpoint Agent](#), que se incluye en el Kit de distribución, se actualiza a la versión 3.11.

Al actualizar Kaspersky Endpoint Security, la aplicación detecta la versión y la finalidad designada de Kaspersky Endpoint Agent. Si se designa Kaspersky Endpoint Agent para el funcionamiento de Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) y Kaspersky Endpoint Detection and Response Optimum (EDR Optimum), Kaspersky Endpoint Security cambia el funcionamiento de estas soluciones al agente integrado de la aplicación. En el caso de Kaspersky Sandbox y EDR Optimum, la aplicación desinstala automáticamente Kaspersky Endpoint Agent. En el caso de MDR, puede desinstalar Kaspersky Endpoint Agent manualmente. Si la aplicación está designada para el funcionamiento de Kaspersky Endpoint Detection and Response Expert (EDR Expert), Kaspersky Endpoint Security actualiza la versión de Kaspersky Endpoint Agent. Para obtener más detalles sobre la aplicación, consulte la documentación de las soluciones de Kaspersky compatibles con Kaspersky Endpoint Agent.

6. Se mejoró la funcionalidad de cifrado de BitLocker:

- El PIN optimizado ahora se puede usar con el [Cifrado de unidad BitLocker](#). El *PIN optimizado* permite utilizar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.
- Se ha añadido una función para [desactivar la autenticación de BitLocker para actualizar el sistema operativo o instalar paquetes de actualización](#). La instalación de actualizaciones puede requerir el reinicio del equipo varias veces. Para instalar las actualizaciones correctamente, puede desactivar temporalmente la autenticación de BitLocker y volver a activar la autenticación después de instalar las actualizaciones.
- Ahora, puede [establecer un tiempo de caducidad para el PIN o contraseña de cifrado de BitLocker](#). Cuando la contraseña o el PIN caduca, Kaspersky Endpoint Security solicita al usuario una nueva contraseña.

7. Ahora, puede configurar el número máximo de intentos de autorización del teclado para la Prevención de ataques de BadUSB. Cuando se alcanza [el número configurado de intentos fallidos para introducir el código de autorización](#), el dispositivo USB se bloquea temporalmente.

8. Se mejoró la funcionalidad del Firewall:

- Ahora, puede configurar un rango de direcciones IP para las [Reglas para paquetes de Firewall](#). Puede introducir un rango de direcciones en formato IPv4 o IPv6. Por ejemplo, 192.168.1.1-192.168.1.100 o 12:34::2-12:34::99.
- Ahora, puede introducir nombres DNS para las [Reglas para paquetes de Firewall](#) en lugar de direcciones IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web.

9. Búsqueda mejorada de [Reglas de Control Web](#). Para buscar una regla de acceso a recursos web, además del nombre de la regla, puede utilizar la URL del sitio web, un nombre de usuario, una categoría de contenido o un tipo de datos.

10. Se optimizó la tarea de *Análisis antivirus*:

- Se optimizó la tarea de [Análisis antivirus en modo inactivo](#). Si ha reiniciado el equipo durante el análisis, Kaspersky Endpoint Security ejecuta automáticamente la tarea, continuando desde el punto donde se interrumpió el análisis.
- Se optimizó la tarea de [Análisis antivirus](#). De forma predeterminada, Kaspersky Endpoint Security ejecuta el análisis solo cuando el equipo está inactivo. Puede configurar cuándo se ejecuta el análisis del equipo en las propiedades de la tarea.

11. Ahora puede restringir el acceso de los usuarios a los datos proporcionados por la [Supervisión de la actividad de aplicaciones](#). Supervisión de la Actividad de Aplicaciones es una herramienta diseñada para ver información sobre la actividad de las aplicaciones en el equipo de un usuario en tiempo real. El administrador puede ocultar la Supervisión de la actividad de aplicaciones al usuario en las propiedades de la directiva de la aplicación.

12. [Se mejoró la seguridad para administrar la aplicación a través de la API REST](#). Ahora Kaspersky Endpoint Security valida la firma de las solicitudes enviadas mediante la API REST. Para administrar el programa, debe instalar un certificado de identificación de solicitudes.

## [Actualización 11.6.0](#)



Kaspersky Endpoint Security 11.6.0 para Windows ofrece las siguientes características y mejoras:

1. [Soporte para Windows 10 21H1](#). Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows 10, visite la [Base de conocimientos del Servicio de soporte técnico](#).
2. [Se añadió el componente Managed Detection and Response](#). Este componente facilita la interacción con la solución denominada Kaspersky Managed Detection and Response. Kaspersky Managed Detection and Response (MDR) brinda protección las 24 horas contra un número creciente de amenazas capaces de eludir los mecanismos de protección automatizados para organizaciones que tienen dificultades y no encuentran expertos altamente cualificados o que tengan recursos internos limitados. Para obtener información detallada sobre cómo funciona la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.
3. [Kaspersky Endpoint Agent](#), que se incluye en el Kit de distribución, se ha actualizado a la versión 3.10. Kaspersky Endpoint Agent 3.10 proporciona nuevas funciones, resuelve algunos problemas anteriores y ha mejorado la estabilidad. Para obtener más detalles sobre la aplicación, consulte la documentación de las soluciones de Kaspersky compatibles con Kaspersky Endpoint Agent.
4. Ahora proporciona la capacidad de administrar la protección frente a ataques, como inundación de red y ataques de tipo "Port scan" en [Ajustes de la Protección frente a amenazas en la red](#).
5. Se añadió un nuevo método para crear reglas de red para el firewall. Puede [añadir reglas de paquetes y reglas de aplicación](#) para las conexiones que se muestran en la ventana [Monitor de red](#). Sin embargo, los ajustes de conexión de regla de red se configurarán automáticamente.
6. La interfaz del [Monitor de red](#) ya está mejorada. Se añadió la información sobre la actividad de la red: ID de proceso (que inicia la actividad de la red), tipo de red (red local o Internet); puertos locales. De manera predeterminada, la información sobre el tipo de red está oculta.
7. Ahora existe la capacidad de crear automáticamente cuentas del Agente de autenticación para nuevos usuarios de Windows. El agente permite al usuario completar la autenticación para acceder a las unidades que fueron [cifradas con la tecnología Cifrado de disco de Kaspersky](#) y cargar el sistema operativo. La aplicación verifica la información sobre las cuentas de usuario de Windows en el equipo. Si Kaspersky Endpoint Security detecta una cuenta de usuario de Windows que no tiene una cuenta de Agente de autenticación, la aplicación creará una nueva cuenta para acceder a las unidades cifradas. Esto significa que no es necesario [añadir manualmente cuentas de Agente de autenticación](#) para equipos con unidades cifradas.
8. Ahora existe la capacidad de supervisar el proceso de cifrado del disco en la interfaz de la aplicación en los equipos de los usuarios (Cifrado de disco de Kaspersky y BitLocker). Puede ejecutar la herramienta Monitor de cifrado desde la [ventana principal de la aplicación](#).

## [Actualización 11.5.0](#)






Kaspersky Endpoint Security 11.5.0 para Windows ofrece las siguientes características y mejoras:

1. [Soporte para Windows 10 20H2](#). Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows 10, visite la [Base de conocimientos del Servicio de soporte técnico](#).
2. [Interfaz de la aplicación](#) actualizada. También se actualizó el [icono de la aplicación en el área de notificación](#), las notificaciones de la aplicación y los cuadros de diálogo.
3. Interfaz mejorada del complemento web de Kaspersky Endpoint Security para los componentes Control de aplicaciones, Control de dispositivos y Control de anomalías adaptativo.
4. Funcionalidad añadida para importar y exportar listas de reglas y exclusiones en formato XML. El formato XML permite editar listas después de exportarlas. Puede administrar las listas solo en la Consola de Kaspersky Security Center. Las siguientes listas están disponibles para exportar/importar:
  - [Detección de comportamiento \(lista de exclusiones\)](#).
  - [Protección frente a amenazas web \(lista de direcciones web de confianza\)](#).
  - [Protección frente a amenazas en el correo \(lista de extensiones de filtrado de adjuntos\)](#).
  - [Protección frente a amenazas en la red \(lista de exclusiones\)](#).
  - [Firewall \(lista de reglas de paquetes de red\)](#).
  - [Control de aplicaciones \(lista de reglas\)](#).
  - [Control web \(lista de reglas\)](#).
  - [Supervisión de puertos de red \(listas de puertos y aplicaciones supervisadas por Kaspersky Endpoint Security\)](#).
  - [Cifrado de disco de Kaspersky \(lista de exclusiones\)](#).
  - [Cifrado de unidades extraíbles \(lista de reglas\)](#).
5. La información del objeto MD5 se añadió al [informe de detección de amenazas](#). En versiones anteriores de la aplicación, Kaspersky Endpoint Security mostraba solo el SHA256 de un objeto.
6. Capacidad añadida para [asignar la prioridad para las reglas de acceso a dispositivos](#) en la configuración de Control de dispositivos. La asignación de prioridades permite una configuración más flexible del acceso de los usuarios a los dispositivos. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 0 al grupo de administradores y asigne una prioridad de 1 al grupo Todos. Puede configurar la prioridad solo para dispositivos que tienen un sistema de archivos. Esto incluye discos duros, unidades extraíbles, disquetes, unidades de CD/DVD y dispositivos portátiles (MTP).
7. Nuevas funcionalidades añadidas:
  - [Administrar notificaciones de audio](#).
  - Redes con reconocimiento del coste - Kaspersky Endpoint Security limita su propio tráfico de red si la conexión a Internet es limitada (por ejemplo, a través de una conexión móvil).

- [Administrar la configuración de Kaspersky Endpoint Security a través de aplicaciones de confianza de administración remota](#) (como TeamViewer, LogMeIn y Remotely Anywhere). Puede utilizar aplicaciones de administración remota para iniciar Kaspersky Endpoint Security y administrar la configuración en la interfaz de la aplicación.
  - [Administrar la configuración para analizar el tráfico seguro en Firefox y Thunderbird](#). Puede seleccionar el almacenamiento de certificados que utilizará Mozilla: el almacenamiento de certificados de Windows o el almacenamiento de certificados de Mozilla. Esta funcionalidad está disponible solo para equipos que no tienen una directiva aplicada. Si se aplica una directiva a un equipo, Kaspersky Endpoint Security activa automáticamente el uso del almacenamiento de certificados de Windows en Firefox y Thunderbird.
8. Capacidad añadida para [configurar el modo de análisis de tráfico seguro](#): analice siempre el tráfico, incluso si los componentes de protección están desactivados, o analice el tráfico cuando lo soliciten los componentes de protección.
  9. Procedimiento revisado para [eliminar información de informes](#). Un usuario sólo puede eliminar todos los informes. En versiones anteriores de la aplicación, un usuario podía seleccionar componentes específicos de la aplicación cuya información se eliminaría de los informes.
  10. Procedimiento revisado para [importar un archivo de configuración que contiene la configuración de Kaspersky Endpoint Security](#) y procedimiento revisado para [restaurar la configuración de la aplicación](#). Antes de importar o restaurar, Kaspersky Endpoint Security muestra solo una advertencia. En versiones anteriores de la aplicación, se podían ver los valores de la nueva configuración antes de que se aplicaran.
  11. Simplificación del [Procedimiento para restaurar el acceso a una unidad cifrada por BitLocker](#). Después de completar el procedimiento de recuperación de acceso, Kaspersky Endpoint Security solicita al usuario que establezca una nueva contraseña o código PIN. Después de establecer una nueva contraseña, BitLocker cifrará la unidad. En la versión anterior de la aplicación, el usuario tenía que restablecer manualmente la contraseña en la configuración de BitLocker.
  12. Los usuarios ahora tienen la capacidad de crear 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. Un administrador puede permitir o bloquear el uso de exclusiones locales o aplicaciones de confianza locales. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.
  13. Capacidad añadida para [introducir comentarios en las propiedades de aplicaciones de confianza](#). Los comentarios ayudan a simplificar las búsquedas y la clasificación de aplicaciones de confianza.
  14. [Administrar la aplicación a través de la API REST](#):
    - Ahora existe la capacidad de establecer la configuración de la extensión Protección frente a amenazas en el correo para Outlook.
    - Está prohibido desactivar la detección de virus, gusanos y troyanos.

## [Actualización 11.4.0](#)

Kaspersky Endpoint Security 11.4.0 para Windows ofrece las siguientes características y mejoras:



1. Nuevo diseño del [icono de la aplicación en el área de notificaciones de la barra de tareas](#). El nuevo  ahora se muestra en lugar del antiguo icono . Si el usuario necesita realizar una acción (por ejemplo, reiniciar el equipo después de actualizar la aplicación), el icono cambiará a . Si los componentes de protección de la aplicación están desactivados o han sufrido un error de funcionamiento, el icono cambiará a  o . Si pasa el cursor sobre el icono, Kaspersky Endpoint Security mostrará una descripción del problema en la protección del equipo.
2. Kaspersky Endpoint Agent, que se incluye en el Kit de distribución, se ha actualizado a la versión 3.9. Kaspersky Endpoint Agent 3.9 admite la integración con las nuevas soluciones de Kaspersky. Para obtener más detalles sobre la aplicación, consulte la documentación de las soluciones de Kaspersky compatibles con Kaspersky Endpoint Agent.
3. Se ha añadido el estado *No compatible con la licencia* a los componentes de Kaspersky Endpoint Security. Puede ver el estado de los componentes en la lista de componentes de la [ventana principal de la aplicación](#).
4. Se han añadido nuevos eventos de [Prevención de exploits](#) a los [informes](#).
5. Los controladores para la [tecnología Cifrado de disco de Kaspersky](#) ahora se añaden automáticamente al entorno de recuperación de Windows (WinRE) cuando se inicia el cifrado de unidad. La versión anterior de Kaspersky Endpoint Security ha añadido controladores al instalar la aplicación. Añadir controladores a WinRE puede mejorar la estabilidad de la aplicación al restaurar el sistema operativo en equipos protegidos por la tecnología Cifrado de disco de Kaspersky.

El componente Endpoint Sensor se ha desinstalado de Kaspersky Endpoint Security. Todavía puede configurar Endpoint Sensor en una directiva siempre que la versión de Kaspersky Endpoint Security instalada en el equipo sea de la 11.0.0 a la 11.3.0.

# Kaspersky Endpoint Security para Windows

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

## Tecnologías de detección de amenazas

 <h3>Aprendizaje automático</h3> <p>Kaspersky Endpoint Security utiliza un modelo basado en el aprendizaje automático. El modelo está desarrollado por expertos de Kaspersky. Luego, el modelo se alimenta continuamente con datos de amenazas de KSN (capacitación de modelos).</p>  <h3>Análisis de nube</h3> <p>Kaspersky Endpoint Security recibe datos de amenazas de <a href="#">Kaspersky Security Network</a>. <i>Kaspersky Security Network (KSN)</i> 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.</p>  <h3>Análisis experto</h3> <p>Kaspersky Endpoint Security utiliza datos de amenazas añadidos por los analistas de virus de Kaspersky. Los analistas de virus evalúan los objetos si la reputación de un objeto no se puede determinar automáticamente.</p>	 <h3>Análisis de comportamiento</h3> <p>Kaspersky Endpoint Security analiza la actividad de un objeto en tiempo real.</p>  <h3>Análisis automático</h3> <p>Kaspersky Endpoint Security recibe datos del sistema automático de análisis de objetos. El sistema procesa todos los objetos que se envían a Kaspersky. Luego, el sistema determina la reputación del objeto y añade los datos a las bases de datos antivirus. Si el sistema no puede determinar la reputación del objeto, el sistema consulta a los analistas de virus de Kaspersky.</p>  <h3>Kaspersky Sandbox</h3> <p>Kaspersky Endpoint Security procesa el objeto en una máquina virtual. Kaspersky Sandbox analiza el comportamiento de un objeto y decide acerca de su reputación. Esta tecnología solo está disponible si se utiliza la <a href="#">solución Kaspersky Sandbox</a>.</p>
---	--

## Árbol de selección

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

Árbol de selección

Sección	Componente
	<h3>Protección frente a amenazas en archivos</h3> <p>El componente Protección frente a amenazas en archivos le permite evitar la infección del sistema de archivos del equipo. De forma predeterminada, el componente Protección frente a amenazas en archivos permanece todo el tiempo en la RAM del equipo. El componente analiza los archivos en todas las unidades del equipo, así como en las unidades conectadas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el <a href="#">servicio en la nube Kaspersky Security Network</a> y el análisis heurístico.</p> <h3>Protección frente a amenazas web</h3>

El componente Protección frente a amenazas web evita la descarga de archivos maliciosos de Internet y también bloquea los sitios web maliciosos y de phishing. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

### Protección frente a amenazas en el correo

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. El componente también analiza los mensajes en busca de enlaces maliciosos y de phishing. De forma predeterminada, el componente Protección frente a amenazas en el correo permanece todo el tiempo en la RAM del equipo y analiza todos los mensajes recibidos o enviados usando los protocolos POP3, SMTP, IMAP o NNTP, o el programa de correo Microsoft Office Outlook (MAPI). El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

### Protección frente a amenazas en la red

El componente Protección frente a amenazas en la red analiza el tráfico de red entrante en busca de actividad habitual en los ataques de red. Cuando Kaspersky Endpoint Security detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante. Las bases de datos de Kaspersky Endpoint Security ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos. La lista de ataques de red que detecta el componente Protección frente a amenazas en la red se actualiza durante [las actualizaciones de módulos de aplicaciones y bases de datos](#).

### Firewall

Firewall bloquea las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local. Firewall también controla la actividad de red de las aplicaciones en el equipo. Esto le permite proteger su red de área local corporativa del robo de identidad y otros ataques. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y *reglas de red* predefinidas.

### Prevención de ataques de BadUSB

El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.

### Protección AMSI

El componente de protección AMSI está diseñado para ser compatible con 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.

## Protección frente a amenazas avanzadas



### Kaspersky Security Network

*Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security podrá utilizar los servicios de KSN para conocer la categoría y la reputación de los archivos analizados u obtener información sobre la reputación de las direcciones web que se analicen.

### Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones de su equipo y ofrece esta información a otros componentes de protección mejorar su rendimiento. El componente Detección de comportamientos utiliza firmas de patrones de actividad peligrosa (Behavior stream signatures, BSS) para aplicaciones. Si la actividad de la aplicación coincide con una BSS Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security basada en bases de datos de reglas heurísticas ofrece protección proactiva al equipo.

#### Prevención de exploits

El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malicioso. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

#### Prevención de intrusiones en el host

El componente Prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus y el servicio en la nube Kaspersky Security Network.

#### Motor de reparación

El Motor de reparación permite a Kaspersky Endpoint Security anular acciones que han sido realizadas por el malware en el sistema operativo.

Controles de seguridad



#### Control de aplicaciones

El Control de aplicaciones gestiona el inicio de aplicaciones en los equipos de los usuarios. Esto le permite implementar una directiva corporativa de seguridad al usar aplicaciones. El Control de aplicaciones también reduce el riesgo de infección del equipo al restringir el acceso a las aplicaciones.

#### Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi). Esto le permite proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos.

#### Control Web

Control web permite regular el acceso de los usuarios a los recursos web. El componente ayuda a reducir tanto el volumen de tráfico como el tiempo que se malgasta en actividades no laborales. Cuando un usuario intenta abrir un sitio web que se ha restringido mediante Control web, Kaspersky Endpoint Security bloquea el acceso o muestra una advertencia.

#### Control de anomalías adaptativo

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos en una red de la empresa. El Control de anomalías adaptativo utiliza un conjunto de reglas para supervisar el comportamiento inusual (por ejemplo, la regla *Inicio de Microsoft PowerShell desde la aplicación Office*). Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa. Puede configurar el modo en que el Control de anomalías adaptativo gestiona cada regla y, por ejemplo, permitir la ejecución de scripts de PowerShell que automatizan determinadas tareas de flujo de trabajo. Kaspersky Endpoint Security actualiza el conjunto de reglas junto con las bases de datos de la aplicación.

Tareas

Análisis antivirus



Kaspersky Endpoint Security analiza el equipo para detectar virus y otras amenazas. El Análisis antivirus ayuda a descartar la posibilidad de que se propague malware que los componentes de protección no hayan detectado, por ejemplo, debido a un nivel de seguridad bajo.

### Actualización

Kaspersky Endpoint Security descarga bases de datos y módulos de la aplicación actualizados. La actualización mantiene el equipo protegido contra los virus más recientes y otras amenazas. De forma predeterminada, la aplicación se actualiza automáticamente, pero, si es necesario, puede actualizar las bases de datos y los módulos de la aplicación manualmente.

### Reversión de la última actualización

Kaspersky Endpoint Security revierte la última actualización de bases de datos y módulos. Esto le permite revertir las bases de datos y los módulos de aplicación a sus versiones anteriores cuando sea necesario, por ejemplo, si la nueva versión de la base de datos contiene una firma no válida que hace que Kaspersky Endpoint Security bloquee una aplicación segura.

### Comprobación de integridad

Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en la carpeta de instalación de la aplicación en busca de datos corruptos o modificaciones. Si un módulo de la aplicación tiene una firma digital incorrecta, el módulo se considera corrupto.

## Cifrado de datos



### Cifrado de archivos

El componente permite crear reglas de cifrado de archivos. Puede seleccionar carpetas predeterminadas para el cifrado, seleccionar una carpeta manualmente o seleccionar archivos individuales por extensión.

### Cifrado de disco completo

El componente permite cifrar el disco duro mediante el Cifrado de disco de Kaspersky o el Cifrado de unidad BitLocker.

### Cifrado de unidades extraíbles

El componente permite proteger datos en unidades extraíbles. Puede utilizar el Cifrado de disco completo (FDE) o Cifrado de archivos (FLE).

## Detection and Response



### Endpoint Detection and Response Optimum

Agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante también "EDR Optimum"). *Kaspersky Endpoint Detection and Response* es una *solución* para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. Para obtener más información sobre la solución, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#).

### Endpoint Detection and Response Expert

Agente integrado para la solución Kaspersky Endpoint Detection and Response Expert (en adelante también "EDR Expert"). EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre la solución, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

### Kaspersky Sandbox



Agente integrado para la solución Kaspersky Sandbox. La *solución Kaspersky Sandbox* detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Kaspersky 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. Kaspersky Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Kaspersky Sandbox). Para obtener más información acerca de la solución, consulte la [Ayuda de Kaspersky Sandbox](#).

#### **Managed Detection and Response**

Agente integrado para respaldar el funcionamiento de la solución Kaspersky Managed Detection and Response. La solución *Kaspersky Managed Detection and Response (MDR)* detecta y analiza automáticamente los incidentes de seguridad en su infraestructura. Para hacerlo, MDR utiliza datos de telemetría recibidos de endpoints y aprendizaje automático. MDR envía datos de incidentes a los expertos de Kaspersky. Luego, los expertos pueden procesar el incidente y, por ejemplo, añadir una nueva entrada a las bases de datos antivirus. De manera alternativa, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aisle el equipo de la red. Para obtener información detallada sobre cómo funciona la solución, consulte la [Ayuda de Kaspersky Managed Detection and Response](#).

## Funciones de servicio de la aplicación

Kaspersky Endpoint Security incluye varias funciones de servicio. Las funciones de servicio se proporcionan para mantener actualizada la aplicación, ampliar su funcionalidad y ayudar al usuario durante el funcionamiento de la aplicación.

- **Informes.** Cuando está en funcionamiento, la aplicación mantiene un informe sobre cada componente de la aplicación. Entre otros usos, los informes permiten conocer el resultado de las tareas completadas. Los informes contienen listas de los eventos ocurridos durante la operación de Kaspersky Endpoint Security y de todas las operaciones que realiza la aplicación. Si se produce un incidente, puede enviar informes a Kaspersky, donde los especialistas del Soporte técnico pueden analizar el problema con más detenimiento.
- **Copia de seguridad.** Si la aplicación detecta archivos infectados mientras se analiza el equipo en busca de virus y otras amenazas, los bloqueará. Kaspersky Endpoint Security almacena copias de los archivos desinfectados y eliminados en *Copia de seguridad*. Kaspersky Endpoint Security mueve los archivos que no se procesan por algún motivo a la *lista de amenazas activas*. Puede analizar archivos, restaurarlos en sus carpetas originales y vaciar el almacenamiento de datos.
- **Notificaciones.** El servicio de notificaciones ayuda al usuario a realizar un seguimiento de los eventos que influyen en el estado de protección del equipo y en la operación de Kaspersky Endpoint Security. Las notificaciones se pueden mostrar en la pantalla o se pueden enviar por correo electrónico.
- **Kaspersky Security Network.** La participación del usuario en Kaspersky Security Network mejora la eficiencia de la protección del equipo a través del uso en tiempo real de información enviada por usuarios de todo el mundo sobre la reputación de archivos, recursos web y software.
- **Licencia.** La compra de una licencia desbloquea la funcionalidad completa de la aplicación, proporciona acceso a las actualizaciones de la base de datos y de los módulos de la aplicación, y ofrece soporte por teléfono o a través de correo electrónico para problemas relacionados con la instalación, la configuración y el uso de la aplicación.
- **Soporte.** Todos los usuarios registrados de Kaspersky Endpoint Security pueden ponerse en contacto con los especialistas del Soporte técnico para obtener ayuda. Puede enviar una solicitud al Soporte técnico de Kaspersky a través del portal de Kaspersky CompanyAccount o llamar al Soporte técnico por teléfono.

## Kit de distribución

El kit de distribución incluye los siguientes paquetes de distribución:

- **Cifrado seguro (AES256)**

Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado AES (Advanced Encryption Standard) con una longitud de clave efectiva de 256 bits.

- **Cifrado Lite (AES56)**

Este paquete de distribución contiene herramientas criptográficas que implementan el algoritmo de cifrado AES con una longitud de clave efectiva de 56 bits.

Cada paquete de distribución contiene los siguientes archivos:

kes_win.msi	Paquete de instalación de Kaspersky Endpoint Security.
setup_kes.exe	Archivos necesarios para <a href="#">instalar la aplicación</a> mediante cualquiera de los métodos disponibles.
kes_win.kud	Archivo para <a href="#">crear paquetes de instalación para Kaspersky Endpoint Security</a> .
klcfginst.msi	Paquete de instalación del Complemento de administración de Kaspersky Endpoint Security para Kaspersky Security Center.
bases.cab	Archivos del paquete de actualización que se utilizan durante la instalación.
cleaner.cab	Archivos para eliminar software no compatible.
incompatible.txt	Archivo que contiene una lista de software no compatible.
ksn_<language_ID>.txt	Archivo que detalla las condiciones de participación en Kaspersky Security Network.
license.txt	Archivo que detalla el <a href="#">Contrato de Licencia de Usuario Final</a> y la Política de privacidad.
installer.ini	Archivo que contiene la configuración interna del kit de distribución.
endpointagent.msi	Paquete de instalación para <a href="#">Kaspersky Endpoint Agent</a> , requerida para la integración con otras soluciones de Kaspersky (por ejemplo, Kaspersky Sandbox).
NDP<versión>-<propiedades del paquete>	Paquete de instalación de Microsoft .NET Framework.
keswin_web_plugin.zip	Archivo comprimido que contiene los archivos necesarios para instalar el <a href="#">complemento web de Kaspersky Endpoint Security</a> .

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

## Requisitos de hardware y software

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

Requisitos generales mínimos:

- 2 GB de espacio libre en el disco duro;
- CPU:
  - Estación de trabajo: 1 GHz;
  - Servidor: 1,4 GHz;
  - Soporte para el conjunto de instrucciones SSE2.
- RAM:
  - Estación de trabajo (x86): 1 GB;
  - Estación de trabajo (x64): 2 GB;
  - Servidor: 2 GB.

## Estaciones de trabajo

Sistemas operativos admitidos para estaciones de trabajo:

- Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1 o versiones posteriores;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisesión;
- Windows 11.

Microsoft ha dejado de utilizar el algoritmo de firma del módulo SHA-1. Se requiere la actualización KB4474419 para la correcta instalación de Kaspersky Endpoint Security en un equipo con el sistema operativo Microsoft Windows 7. Para obtener más detalles acerca de esta actualización, visite el [sitio web de soporte técnico de Microsoft](#).

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 11.8.0 añade compatibilidad con los componentes principales de la aplicación en equipos con sistema operativo Windows para servidores. Ahora puede utilizar Kaspersky Endpoint Security para Windows en lugar de Kaspersky Security para Windows Server en servidores y clústeres de su organización. El modo básico se admite con [limitaciones](#).

Sistemas operativos admitidos para servidores:

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

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

- Windows MultiPoint Server 2011 (64 bits);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 o versiones posteriores;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Microsoft ha dejado de utilizar el algoritmo de firma del módulo SHA-1. Se requiere la actualización KB4474419 para la correcta instalación de Kaspersky Endpoint Security en un equipo con el sistema operativo Microsoft Windows Server 2008 R2. Para obtener más detalles acerca de esta actualización, visite el [sitio web de soporte técnico de Microsoft](#).

Para más información sobre la compatibilidad con Microsoft Windows Server 2016 y Microsoft Windows Server 2019, visite 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](#).

## Servidores de terminales

Tipos de servidores de terminales admitidos:

- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2008 R2 SP1;
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2012;
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2012 R2;
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2016;

- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2019.

## Plataformas virtuales

Plataformas virtuales compatibles:

- VMware Workstation 16.1.2;
- VMware ESXi 7.0 Update 3;
- Microsoft Hyper-V Servidor 2019;
- Citrix Virtual Apps and Desktops 7 2106;
- Citrix Provisioning Services 2109;
- Citrix Hypervisor 8.2 (revisión XS82E033).

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

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 revisión A;
- Kaspersky Security Center 12 revisión B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2.

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

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

Comparación de las funciones de Kaspersky Endpoint Security

Función	Estación de trabajo	Servidor
<b>Protección frente a amenazas avanzadas</b>		
Kaspersky Security Network	✓	✓
Detección de comportamiento	✓	✓
Prevención de exploits	✓	✓

Prevención de intrusiones en el host	✓	–
Motor de reparación	✓	✓
<b>Protección frente a amenazas básicas</b>		
Protección frente a amenazas en archivos	✓	✓
Protección frente a amenazas web	✓	✓
Protección frente a amenazas en el correo	✓	✓
Firewall	✓	✓
Protección frente a amenazas en la red	✓	✓
Prevención de ataques de BadUSB	✓	✓
Protección AMSI	✓	✓
<b>Controles de seguridad</b>		
Control de aplicaciones	✓	✓
Control de dispositivos	✓	✓
Control Web	✓	✓
Control de anomalías adaptativo	✓	–
<b>Cifrado de datos</b>		
Cifrado de disco de Kaspersky	✓	–
Cifrado de unidad BitLocker	✓	✓
Cifrado de archivos	✓	–
Cifrado de unidades extraíbles	✓	–
<b>Detection and Response</b>		
Kaspersky Endpoint Agent	✓	✓
Endpoint Detection and Response Optimum	✓	✓
Endpoint Detection and Response Expert	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response	✓	✓

## Comparación: disponibilidad de características por herramienta de administración

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

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

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

administración.

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

Comparación de las funciones de Kaspersky Endpoint Security

Función	Kaspersky Security Center		Kaspersky Security Center
	Consola de administración	Web Console	Cloud Console
<b>Protección frente a amenazas avanzadas</b>			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Detección de comportamiento	✓	✓	✓
Prevención de exploits	✓	✓	✓
Prevención de intrusiones en el host	✓	✓	✓
Motor de reparación	✓	✓	✓
<b>Protección frente a amenazas básicas</b>			
Protección frente a amenazas en archivos	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓
Protección frente a amenazas en el correo	✓	✓	✓
Firewall	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓
Protección AMSI	✓	✓	✓
<b>Controles de seguridad</b>			
Control de aplicaciones	✓	✓	✓
Control de dispositivos	✓	✓	✓
Control Web	✓	✓	✓
Control de anomalías adaptativo	✓	✓	✓
<b>Cifrado de datos</b>			
Cifrado de disco de Kaspersky	✓	✓	–
Cifrado de unidad BitLocker	✓	✓	✓
Cifrado de archivos	✓	✓	–
Cifrado de unidades extraíbles	✓	✓	–
<b>Detection and Response</b>			

Kaspersky Endpoint Agent	✓	✓	✓
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert	–	–	✓
Kaspersky Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
<b>Tareas</b>			
Añadir clave	✓	✓	✓
Cambiar componentes de la aplicación	✓	✓	✓
Inventario	✓	✓	✓
Actualización	✓	✓	✓
Reversión de actualizaciones	✓	✓	✓
Análisis antivirus	✓	✓	✓
Comprobación de integridad	✓	✓	–
Eliminación de datos	✓	✓	✓
Administrar cuentas del Agente de autenticación (Cifrado de disco de Kaspersky)	✓	✓	–
Análisis de IOC (EDR)	–	✓	✓
Mover archivo a cuarentena (EDR)	–	✓	✓
Obtener archivo (EDR)	–	✓	✓
Eliminar archivo (EDR)	–	✓	✓
Inicio del proceso (EDR)	–	✓	✓
Terminar proceso (EDR)	–	✓	✓

## Compatibilidad con otras aplicaciones

Antes de la instalación, Kaspersky Endpoint Security comprueba el equipo para buscar aplicaciones de Kaspersky. La aplicación también analiza el equipo en busca de software incompatible. La lista de software no compatible está disponible en el archivo incompatible.txt que se incluye en el [kit de distribución](#).

 [DESCARGAR EL ARCHIVO INCOMPATIBLE.TXT](#)

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

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.



- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (incluido el componente Sensor de Endpoint).
- Kaspersky Sandbox (incluido Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (incluido el componente Sensor de Endpoint).

Si el componente Endpoint Agent está instalado en un equipo que utiliza las herramientas de despliegue de otras aplicaciones de Kaspersky, los componentes se eliminarán automáticamente durante la instalación de Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede incluir el componente Sensor de Endpoint/Kaspersky Endpoint Agent si ha seleccionado Endpoint Agent en la lista de componentes de la aplicación.

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

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

# Instalación y eliminación de la aplicación

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

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

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

1. los ajustes recibidos del archivo [setup.ini](#),
2. los ajustes recibidos del archivo installer.ini,
3. los ajustes recibidos de la [línea de comando](#).

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

## Despliegue a través de Kaspersky Security Center

Kaspersky Endpoint Security puede desplegarse de varias maneras en los equipos de una red corporativa. Puede elegir el escenario de despliegue más adecuado para su organización o combinar varios escenarios de despliegue al mismo tiempo. Kaspersky Security Center admite los siguientes métodos de despliegue principales:

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

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

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

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

1. [Creación de un paquete de instalación](#).
2. [Creación de una tarea de instalación remota](#).

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

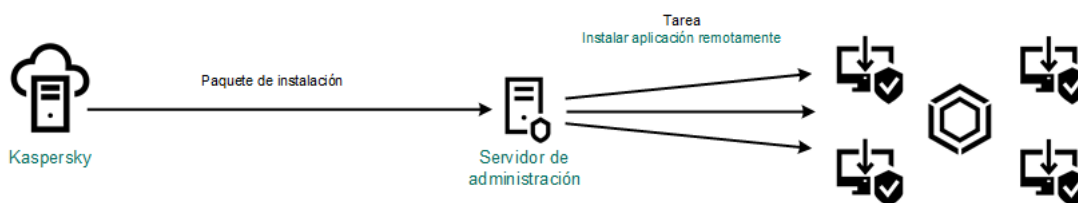
## Instalación estándar de la aplicación

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

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

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

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



Despliegue de Kaspersky Endpoint Security

[Cómo ejecutar el Asistente de despliegue de protección en la Consola de administración \(MMC\)](#)

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Avanzado** → **Instalación remota**.
2. Haga clic en el enlace **Desplegar paquete de instalación en los dispositivos administrados (estaciones de trabajo)**.

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

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

### Paso 1. Seleccionar un paquete de instalación.

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

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

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

### Paso 2. Selección de dispositivos para realizar la instalación

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

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

### Paso 3. Definir la configuración de la tarea de instalación remota

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

- **Forzar la descarga del paquete de instalación.** Seleccionar el método para instalar la aplicación:
  - **Usando el Agente de red.** Si el Agente de red no se ha instalado en el equipo, primero se instalará el Agente de red utilizando las herramientas del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.

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

#### Paso 4. Selección de una clave de licencia

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

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

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

#### Paso 6. Eliminación de aplicaciones incompatibles antes de instalar la aplicación

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

#### Paso 7. Selección de una cuenta para acceder a los dispositivos

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

## Paso 8. Inicio de la instalación

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

[Cómo iniciar el Asistente de despliegue de la protección en Web Console y Cloud Console](#) 

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

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

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

## Paso 1. Seleccionar un paquete de instalación.

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

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

## Paso 2. Selección de una clave de licencia

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

## Paso 3. Selección de un agente de red

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

## Paso 4. Selección de dispositivos para realizar la instalación

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

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

## Paso 5. Configuración de los parámetros avanzados

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

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

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

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

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

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

## Paso 8. Asignación a un grupo de administración

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

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



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

## Paso 10. Inicio de la instalación

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

## Creación de un paquete de instalación

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

[Cómo crear un paquete de instalación en la Consola de administración \(MMC\)](#) 

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

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

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

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

### Paso 1. Seleccionar el tipo de paquete de instalación

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

### Paso 2. Definir el nombre del paquete de instalación

Introduzca el nombre del paquete de instalación, por ejemplo, *Kaspersky Endpoint Security para Windows 11.8.0*.

### Paso 3. Seleccionar el paquete de distribución para la instalación

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

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

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

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

El paquete de instalación se creará y se añadirá a Kaspersky Security Center. Mediante el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación. En la configuración del paquete de instalación, puede seleccionar los componentes de la aplicación y configurar los parámetros de instalación del programa (consulte la siguiente tabla). El paquete de instalación contiene bases de datos antivirus del repositorio del Servidor de administración. Puede [actualizar las bases de datos en el paquete de instalación](#) para reducir el consumo de tráfico al actualizar las bases de datos después de instalar Kaspersky Endpoint Security.

[Cómo crear un paquete de instalación en Web Console y Cloud Console](#) 

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

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

2. Haga clic en el botón **Añadir**.

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**.

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

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

## Paso 2. Paquetes de instalación

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

El paquete de instalación se creará y se añadirá a Kaspersky Security Center. Mediante el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación. En la configuración del paquete de instalación, puede seleccionar los componentes de la aplicación y configurar los parámetros de instalación del programa (consulte la siguiente tabla). El paquete de instalación contiene bases de datos antivirus del repositorio del Servidor de administración. Puede [actualizar las bases de datos en el paquete de instalación](#) para reducir el consumo de tráfico al actualizar las bases de datos después de instalar Kaspersky Endpoint Security.

### Ajustes del paquete de instalación

Sección	Descripción
<b>Componentes de protección</b>	<p>En esta sección, puede seleccionar qué componentes de la aplicación estarán disponibles. El <a href="#">conjunto de componentes puede modificarse</a> posteriormente a través de la tarea <i>Cambiar componentes de la aplicación</i>. El componente Prevención de ataques de BadUSB, el componente Detection and Response, y los componentes de cifrado de datos no se instalan de forma predeterminada. Estos componentes se pueden añadir en la configuración del paquete de instalación.</p> <p>Si necesita instalar los componentes de Detection and Response, Kaspersky Endpoint Security admite las siguientes configuraciones:</p> <ul style="list-style-type: none"><li>• Solo Endpoint Agent</li><li>• Solo Endpoint Detection and Response Optimum</li><li>• Solo Endpoint Detection and Response Expert</li><li>• Solo Kaspersky Sandbox</li></ul>

	<ul style="list-style-type: none"> <li>• Endpoint Detection and Response Optimum y Kaspersky Sandbox</li> <li>• Endpoint Detection and Response Expert y Kaspersky Sandbox</li> </ul> <p>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.</p>
<b>Clave de licencia</b>	<p>En esta sección, puede activar la aplicación. Para activar la aplicación, debe seleccionar una clave de licencia. Antes de hacerlo, debe añadir la clave al Servidor de administración. Para obtener más información sobre cómo añadir una clave al Servidor de administración de Kaspersky Security Center, consulte la <a href="#">Ayuda de Kaspersky Security Center</a>.</p>
<b>Aplicaciones incompatibles</b>	<p>Lea atentamente la lista de aplicaciones incompatibles y permita la eliminación de estas aplicaciones. Si hay aplicaciones incompatibles instaladas en el equipo, la instalación de Kaspersky Endpoint Security terminará con un error.</p>
<b>Configuración de la instalación</b>	<p><b>Añadir ubicación de la aplicación a la variable del entorno %PATH%.</b> Puede añadir la ruta de instalación a la variable %PATH% para un <a href="#">uso conveniente de la interfaz de línea de comandos</a>.</p> <p><b>No proteger el proceso de instalación.</b> La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Escritorio remoto de Windows), se aconseja que desactive la protección del proceso de instalación.</p> <p><b>Asegurar la compatibilidad con Citrix PVS (esto solo es necesario cuando se trabaja con Citrix PVS).</b> Puede habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual.</p> <p><b>Ruta a la carpeta de instalación de la aplicación.</b> Puede cambiar la ruta de instalación de Kaspersky Endpoint Security en un equipo cliente. De forma predeterminada, la aplicación se instala en la carpeta %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security para Windows.</p> <p><b>Archivo de configuración.</b> Puede subir un archivo que defina la configuración de Kaspersky Endpoint Security. Puede <a href="#">crear un archivo de configuración en la interfaz local de la aplicación</a>.</p>

## Actualización de bases de datos en el paquete de instalación

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

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

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

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

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

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

2. Abra las propiedades del paquete de instalación.
3. En la sección **General**, haga clic en el botón **Actualizar bases de datos**.

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

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

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

Esto abre una lista de paquetes de instalación descargados en Web Console.

2. Haga clic en el nombre del paquete de instalación de Kaspersky Endpoint Security en el que desea actualizar las bases de datos antivirus.

Se abre la ventana de propiedades del paquete de instalación.

3. En la pestaña **Información general**, haga clic en el enlace **Actualizar bases de datos**.

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

## Creación de una tarea de instalación remota

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

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

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

## Paso 1. Selección del tipo de tarea

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

## Paso 2. Seleccionar un paquete de instalación.

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

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

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

## Paso 3. Adicional

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

## Paso 4. Configuración

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

- **Forzar la descarga del paquete de instalación.** Seleccionar el método para instalar la aplicación:
  - **Usando el Agente de red.** Si el Agente de red no se ha instalado en el equipo, primero se instalará el Agente de red utilizando las herramientas del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.
  - **Usando los recursos del sistema operativo mediante puntos de distribución.** El paquete de instalación se entrega a los equipos cliente mediante recursos del sistema operativo a través de puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la [Ayuda de Kaspersky Security Center](#).
  - **Usando los recursos del sistema operativo mediante el Servidor de administración.** Los archivos se entregarán a los equipos cliente mediante los recursos del sistema operativo a través del Servidor de Administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.

- **Comportamiento para dispositivos administrados a través de otros Servidores de administración.** Seleccione el método de instalación de Kaspersky Endpoint Security. Si la red tiene más de un Servidor de administración instalado, estos Servidores de administración pueden ver los mismos equipos cliente. Esto puede causar, por ejemplo, que una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes servidores de administración, o puede generar otros conflictos.
- **No reinstalar la aplicación si ya se encuentra instalada.** Desactive esta casilla de verificación si, por ejemplo, desea instalar una versión anterior de la aplicación.

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

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

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

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

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

## Paso 7. Selección de la cuenta para ejecutar la tarea

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



## Paso 8. Configurar una planificación de inicio de tarea

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

## Paso 9. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Desinstalar Kaspersky Endpoint Security para Windows 11.8.0*.

## Paso 10. Finalización de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. La aplicación se instalará en modo silencioso. Después de la instalación, el icono  aparecerá en el 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 **Dispositivos** → **Tareas**.

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

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

## Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.

2. En la lista desplegable **Tipo de tarea**, seleccione **Instalar aplicación en remoto**.

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

4. En la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

## Paso 2. Selección de equipos para realizar la instalación

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

## Paso 3. Configuración de un paquete de instalación

En este paso, configure el paquete de instalación:

1. Seleccione el paquete de instalación de Kaspersky Endpoint Security para Windows (11.8.0).

2. Seleccione el paquete de instalación del Agente de red.

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

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

- **Usando el Agente de red.** Si el Agente de red no se ha instalado en el equipo, primero se instalará el Agente de red utilizando las herramientas del sistema operativo. Luego, Kaspersky Endpoint Security se instalará mediante las herramientas del Agente de red.
- **Usando los recursos del sistema operativo mediante puntos de distribución.** El paquete de instalación se entrega a los equipos cliente mediante recursos del sistema operativo a través de puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la [Ayuda de Kaspersky Security Center](#).
- **Usando los recursos del sistema operativo mediante el Servidor de administración.** Los archivos se entregarán a los equipos cliente mediante los recursos del sistema operativo a través del Servidor de



Administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.

4. En el campo **Número máximo de descargas concurrentes**, establezca un límite para el número de solicitudes de descarga de paquetes de instalación que se envían al Servidor de administración. Limitar el número de solicitudes ayudará a evitar que la red se sobrecargue.
5. En el campo **Número máximo de intentos de instalación**, establezca un límite para el número de intentos de instalación de la aplicación. Si la instalación de Kaspersky Endpoint Security termina con un error, la tarea volverá a empezar automáticamente.
6. Si es necesario, desactive la casilla **No reinstalar la aplicación si ya se encuentra instalada**. Permite, por ejemplo, instalar una de las versiones anteriores de la aplicación.
7. Si es necesario, desactive la casilla **Verificar el tipo de sistema operativo antes de descargar**. Esto le permite evitar la descarga de un paquete de distribución de aplicaciones si el sistema operativo del equipo no cumple los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple los requisitos de software, puede omitir esta verificación.
8. Si es necesario, active la casilla **Asignar instalación del Agente de red 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 **Indicar a los usuarios que cierren las aplicaciones en ejecución**. La instalación de Kaspersky Endpoint Security consume recursos del equipo. Para comodidad del usuario, el Asistente de instalación de la aplicación le pide que cierre las aplicaciones en ejecución antes de iniciar la instalación. Esto ayuda a evitar interrupciones en el funcionamiento de las demás aplicaciones y evita posibles fallos en el equipo.
10. En la sección **Comportamiento para dispositivos administrados a través de otros Servidores de administración**, seleccione el método de instalación de Kaspersky Endpoint Security. Si la red tiene más de un Servidor de administración instalado, estos Servidores de administración pueden ver los mismos equipos cliente. Esto puede causar, por ejemplo, que una aplicación se instale de forma remota en el mismo equipo cliente varias veces a través de diferentes servidores de administración, o puede generar otros conflictos.

#### Paso 4. Selección de la cuenta para ejecutar la tarea

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

#### Paso 5. Conclusión de la creación de tareas

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

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

La interfaz del Asistente de configuración de aplicaciones consta de una secuencia de ventanas correspondientes a los pasos de instalación de la aplicación.

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

1. Copie la carpeta del [kit de distribución](#) al equipo del usuario.
2. Ejecute setup\_ks.exe.

Se iniciará el Asistente de instalación.

## Preparativos para la instalación

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

- Si hay software incompatible instalado (la lista de software incompatible se encuentra en el archivo incompatible.txt, que forma parte del [kit de distribución](#)).
- Si se cumplen o no los [requisitos de hardware y software](#).
- Si el usuario tiene los derechos necesarios para instalar el producto de software.

Si alguno de los requisitos previos no se cumple, se muestra una notificación pertinente en pantalla.

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

Si las aplicaciones detectadas incluyen versiones anteriores de Kaspersky Endpoint Security, todos los datos que se pueden migrar (por ejemplo, datos de activación y configuración de la aplicación) se conservan y se usan durante la instalación de Kaspersky Endpoint Security 11.8.0 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 10 Service Pack 2 Maintenance Release 3 para Windows (compilación 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 para Windows (compilación 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 para Windows (compilación 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 para Windows (compilación 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 para Windows SF1 (compilación 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 para Windows (compilación 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 para Windows (compilación 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 para Windows (compilación 11.2.0.2254).

- Kaspersky Endpoint Security 11.2.0 para Windows CF1 (compilación 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 para Windows (compilación 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 para Windows (compilación 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 para Windows (compilación 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 para Windows (compilación 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 para Windows (compilación 11.7.0.669).

## Los componentes de Kaspersky Endpoint Security

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

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

- [Prevención de ataques de BadUSB](#).
- [Componentes de cifrado de datos](#).
- Componentes de Detection and Response.

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

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

- Solo Endpoint Agent
- Solo Endpoint Detection and Response Optimum
- Solo Endpoint Detection and Response Expert
- Solo Kaspersky Sandbox
- Endpoint Detection and Response Optimum y Kaspersky Sandbox
- Endpoint Detection and Response Expert y Kaspersky Sandbox

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.

## Configuración avanzada

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

**Asegurar la compatibilidad con Citrix PVS (esto solo es necesario cuando se trabaja con Citrix PVS).** Puede habilitar el soporte de Citrix Provisioning Services para instalar Kaspersky Endpoint Security en una máquina virtual.

**Añadir ubicación de la aplicación a la variable del entorno %PATH%.** Puede añadir la ruta de instalación a la variable %PATH% para un [uso conveniente de la interfaz de línea de comandos](#).

## Instalando remotamente la aplicación usando System Center Configuration Manager

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

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

1. Abra la consola de Configuration Manager.
2. En la parte derecha de la consola, en la sección **Administración de aplicaciones**, seleccione **Paquetes**.
3. En la parte superior de la consola del panel de control, haga clic en el botón **Crear paquete**.  
Esto inicia el *Asistente de nuevo paquete y aplicación*.
4. En el Asistente de nuevo paquete y aplicación:
  - a. En la sección **Paquete**:
    - En el campo **Nombre**, introduzca el nombre del paquete de instalación.
    - En el campo **Carpeta de origen**, especifique la ruta a la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security.
  - b. En la sección **Tipo de aplicación**, seleccione la opción **Programa estándar**.
  - c. En la sección **Programa estándar**:
    - En el campo **Nombre**, introduzca el nombre único para el paquete de instalación (por ejemplo, el nombre de la aplicación que incluye la versión).
    - En el campo **Línea de comandos**, especifique las opciones de instalación de Kaspersky Endpoint Security en la línea de comandos.
    - Haga clic en el botón **Examinar** para especificar la ruta al archivo ejecutable de la aplicación.
    - Asegúrese de que la lista **Modo de ejecución** tenga seleccionado el elemento **Ejecutar con derechos administrativos**.
  - d. En la sección **Requisitos**:

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

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

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

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

Este paso es opcional.

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

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

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

Esto inicia el *Asistente de implementación*.

6. En el Asistente de implementación:

- a. En la sección **General**:

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

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

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

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

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

## Descripción de la configuración de instalación del archivo setup.ini

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



[DESCARGAR EL ARCHIVO SETUP.INI](#)

El archivo setup.ini contiene las siguientes secciones:

- **[Setup]**: configuración general de instalación de la aplicación.
- **[Componentes]**: selección de los componentes de la aplicación que se van a instalar. Si no se especifica ningún componente, se instalarán todos los componentes que estén disponibles en el sistema operativo. Protección frente a amenazas en archivos es un componente obligatorio y se instala en el equipo al margen de la configuración indicada en esta sección. En este bloque, tampoco aparece el componente Managed Detection and Response. Para instalarlo, debe [activar Managed Detection and Response en la Consola de Kaspersky Security Center](#).
- **[Tasks]**: selección de tareas que se incluirán en la lista de tareas de Kaspersky Endpoint Security. Si no se especifica la tarea, se incluirán todas las tareas de la lista de tareas de Kaspersky Endpoint Security.

Las alternativas al valor 1 son los valores `yes`, `on`, `enable` y `enabled`.

Las alternativas al valor 0 son los valores `no`, `off`, `disable` y `disabled`.

#### Configuración del archivo setup.ini

Sección	Parámetro	Descripción
[Setup]	InstallDir	Ruta a la carpeta de instalación de la aplicación.
	ActivationCode	Código de activación de Kaspersky Endpoint Security.
	EULA=1	<p>Aceptación de las condiciones del Contrato de licencia de usuario final. El contenido del Contrato de licencia se incluye en el <a href="#">kit de distribución de Kaspersky Endpoint Security</a>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Se requiere la aceptación de los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar la versión de esta.</p> </div>
	PrivacyPolicy=1	<p>Aceptación de la Política de privacidad. El texto de la Política de privacidad se incluye en el <a href="#">Kit de distribución de Kaspersky Endpoint Security</a>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Para instalar la aplicación o actualizar su versión, debe aceptar la Política de privacidad.</p> </div>
	KSN	<p>Aceptación o rechazo de la participación en Kaspersky Security Network (KSN). Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security solicitará la confirmación de su consentimiento o el rechazo de la participación en KSN cuando se inicie Kaspersky Endpoint Security por primera vez. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: aceptación de la participación en KSN.</li> <li>• 0: rechazo de la participación en KSN (valor predeterminado).</li> </ul>

		<p>El paquete de distribución de Kaspersky Endpoint Security se optimiza para su uso con Kaspersky Security Network. Si optara por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que la instalación se haya completado.</p>
	Login	<p>Configure el nombre de usuario para acceder a las funciones y ajustes de Kaspersky Endpoint Security (el componente <a href="#">Protección con contraseña</a>). El nombre de usuario se configura junto con los parámetros Password y PasswordArea. El nombre de usuario KLAdmin se utiliza de forma predeterminada.</p>
	Contraseña	<p>Especifique una contraseña para acceder a las funciones y ajustes de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros Login y PasswordArea).</p> <p>Si especificó una contraseña, pero no especificó un nombre de usuario con el parámetro Nombre de usuario, se utiliza de forma predeterminada el nombre de usuario KLAdmin.</p>
	PasswordArea	<p>Especifique el alcance de la contraseña para acceder a Kaspersky Endpoint Security. Cuando un usuario intenta realizar una acción que está dentro de este alcance, Kaspersky Endpoint Security solicita las credenciales de la cuenta del usuario (parámetros Login y Password). Si necesita especificar más de un valor, use el carácter ";".</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> <li>• SET: modificar la configuración de la aplicación.</li> <li>• EXIT: salir de la aplicación.</li> <li>• DISPROTECT: desactivar componentes de protección y detener tareas de análisis.</li> <li>• DISPOLICY: desactivar la directiva de Kaspersky Security Center.</li> <li>• UNINST: eliminar la aplicación del equipo.</li> <li>• DISCTRL: desactivar componentes de control.</li> <li>• REMOVELIC: eliminar la clave.</li> <li>• REPORTS: consultar informes.</li> </ul>
	SelfProtection	<p>Activación o desactivación del mecanismo que protege la instalación de la aplicación. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: se activa el mecanismo de protección de la instalación de la aplicación (valor predeterminado).</li> <li>• 0: se desactiva el mecanismo de protección de la instalación de la aplicación.</li> </ul>



		<p>La protección de la instalación incluye protección contra la sustitución del paquete de distribución por aplicaciones maliciosas, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Escritorio remoto de Windows), se aconseja que desactive la protección del proceso de instalación.</p>
	Reboot=1	<p>Reinicio automático del equipo, si es necesario después de la instalación o la actualización de la aplicación. Si no se establece ningún valor para este parámetro, se bloquea el reinicio automático del equipo.</p> <p>Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.</p>
	AddEnvironment	<p>En la variable del sistema %PATH%, añada la ruta hacia los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: la variable del sistema %PATH% se complementa con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security.</li> <li>• 0: la variable del sistema %PATH% no se complementa con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security.</li> </ul>
	AMPPL	<p>Activa o desactiva el uso de la tecnología AM-PPL (Anti-Malware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para obtener más información sobre la tecnología AM-PPL, visite el <a href="#">sitio web de Microsoft</a>.</p> <p>La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019.</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: los procesos de Kaspersky Endpoint Security se protegen con la tecnología AM-PPL.</li> <li>• 0: los procesos de Kaspersky Endpoint Security no se protegen con la tecnología AM-PPL.</li> </ul>
	SetupReg	<p>Permite que se graben en el Registro las claves del archivo setup.reg. SetupReg: valor del parámetro setup.reg.</p>
	EnableTraces	<p>Activar o desactivar el rastreo de la aplicación. Una vez que Kaspersky Endpoint Security se inicia, los archivos</p>

		<p>de seguimiento se guardan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: el rastreo está activado.</li> <li>• 0: el rastreo está desactivado (valor predeterminado).</li> </ul>
	TracesLevel	<p>Nivel de detalle del seguimiento. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 100 (crítico). Solo mensajes sobre errores graves.</li> <li>• 200 (alto). Mensajes sobre todos los errores, incluidos los errores graves.</li> <li>• 300 (diagnóstico). Mensajes sobre todos los errores, además de las advertencias.</li> <li>• 400 (importante). Todos los mensajes de error y de advertencia, así como otra información adicional.</li> <li>• 500 (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado).</li> <li>• 600 (bajo). Todos los mensajes.</li> </ul>
	RESTAPI	<p>Administrar la aplicación a través de la API REST. Para administrar la aplicación a través de la API REST, debe especificar el nombre de usuario (parámetro RESTAPI_User).</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: se permite la administración a través de la API REST.</li> <li>• 0: se bloquea la administración a través de la API REST (valor predeterminado).</li> </ul> <p>Para administrar la aplicación a través de la API REST, debe permitirse la administración mediante sistemas de administración. Para ello, configure el parámetro AdminKitConnector=1. Si administra la aplicación a través de la API REST, no es posible administrarla mediante los sistemas de administración de Kaspersky.</p>
	RESTAPI_User	<p>Nombre de usuario de la cuenta de dominio de Windows utilizada para administrar la aplicación a través de la API REST. La administración de la aplicación a través de la API REST solo está disponible para este usuario. Introduzca el nombre de usuario con el formato &lt;DOMINIO&gt;\&lt;NombreUsuario&gt; (por ejemplo, RESTAPI_User=EMPRESA\Administrador). Solo puede seleccionar un usuario para que funcione con la API REST.</p>

		Añadir un nombre de usuario es un requisito previo para poder administrar la aplicación a través de la API REST.
	RESTAPI_Port	Puerto utilizado para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782.
	RESTAPI_Certificate	Certificado para identificar solicitudes (por ejemplo, RESTAPI_Certificate=C:\cert.pem). La interacción segura de Kaspersky Endpoint Security con el cliente REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga útil de cada solicitud.
[Components]	ALL	<p>Instalación de todos los componentes. Si se especifica el valor del parámetro 1, todos los componentes se instalarán sin tener en cuenta la configuración de la instalación de componentes concretos.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Debido a la forma de compatibilidad de las soluciones de Detection and Response, los componentes de Endpoint Detection and Response Optimum, así como de Kaspersky Sandbox, se instalan en el equipo. Los componentes Endpoint Detection and Response Expert y Endpoint Agent no son compatibles con esta configuración.</p> </div>
	MailThreatProtection	Protección frente a amenazas en el correo.
	WebThreatProtection	Protección frente a amenazas web.
	AMSI	Protección AMSI.
	HostIntrusionPrevention	Prevención de intrusiones en el host.
	BehaviorDetection	Detección de comportamiento.
	ExploitPrevention	Prevención de vulnerabilidades.
	RemediationEngine	Motor de reparación.
	Firewall	Firewall.
	NetworkThreatProtection	Protección frente a amenazas en la red.
	WebControl	Control web.
	DeviceControl	Control de dispositivos.
	ApplicationControl	Control de aplicaciones.
	AdaptiveAnomaliesControl	Control de anomalías adaptativo.
	FileEncryption	Bibliotecas de cifrado de archivos.
	DiskEncryption	Bibliotecas de cifrado de disco completo.
	BadUSBAttackPrevention	Prevención de ataques de BadUSB.
	AntiAPT	Endpoint Agent. Endpoint Agent instala Kaspersky Endpoint Agent. Kaspersky Endpoint Agent es compatible con <a href="#">soluciones de Detection and Response</a>

		<p>para detección avanzada de amenazas (por ejemplo, Kaspersky Sandbox).</p> <p>El componente no es compatible con los componentes EDR Optimum (EDR), EDR Expert (EDRCloud) y Kaspersky Sandbox (SB).</p>
	EDR	<p>Endpoint Detection and Response Optimum (EDR Optimum).</p> <p>El componente no es compatible con los componentes Endpoint Agent (AntiAPT) y EDR Expert (EDRCloud).</p>
	EDRCloud	<p>Endpoint Detection and Response Expert (EDR Expert).</p> <p>El componente no es compatible con los componentes Endpoint Agent (AntiAPT) y EDR Optimum (EDR).</p>
	SB	<p>Kaspersky Sandbox.</p> <p>El componente es incompatible con el componente Endpoint Agent (AntiAPT).</p>
	AdminKitConnector	<p>Administración de aplicaciones mediante sistemas de administración. Los sistemas de administración incluyen, por ejemplo, Kaspersky Security Center. Además de los sistemas de administración de Kaspersky, puede usar soluciones de terceros. Kaspersky Endpoint Security proporciona una API para este fin.</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: se permite la administración de aplicaciones con la ayuda de sistemas de administración (valor predeterminado).</li> <li>• 0: se permite la administración de aplicaciones solo a través de la interfaz local.</li> </ul>
[Tasks]	ScanMyComputer	<p>Tarea de Análisis completo. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.</li> <li>• 0: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.</li> </ul>

	ScanCritical	Tarea de Análisis de áreas críticas. Valores disponibles: <ul style="list-style-type: none"> <li>• 1: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.</li> <li>• 0: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.</li> </ul>
	Updater	Tarea de actualización. Valores disponibles: <ul style="list-style-type: none"> <li>• 1: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.</li> <li>• 0: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.</li> </ul>

## Cambiar componentes de la aplicación

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

- De forma local, utilizando el Asistente de instalación.

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

- De forma remota utilizando Kaspersky Security Center.

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

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

- En los equipos que ejecutan Windows Server, no puede [instalar todos los componentes de Kaspersky Endpoint Security](#) (por ejemplo, el componente Control de anomalías adaptativo no está disponible).
- Si los discos duros de su equipo están protegidos por la característica [Cifrado de disco completo \(FDE\)](#), no puede eliminar el componente Cifrado de disco completo. Para eliminar el componente Cifrado de disco completo, descifre todos los discos duros del equipo.
- Si el equipo tiene [archivos cifrados \(FLE\)](#) o el usuario utiliza [unidades extraíbles cifradas \(FDE o FLE\)](#), no se podrá acceder a los archivos y unidades extraíbles después de que se eliminen los componentes de Cifrado de datos. Puede acceder a los archivos y unidades extraíbles volviendo a instalar los componentes de Cifrado de datos.

[Cómo añadir o quitar componentes de la aplicación en la Consola de administración \(MMC\)](#) 

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

## Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)** → **Cambiar componentes de la aplicación**.

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

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

Seleccione la casilla **Eliminar aplicaciones de terceros incompatibles**. La lista de aplicaciones incompatibles puede verse en `incompatible.txt`, que se incluye en el [kit de distribución](#). Si hay aplicaciones incompatibles instaladas en el equipo, la instalación de Kaspersky Endpoint Security terminará con un error.

De ser necesario, habilite la [protección con contraseña](#) para realizar la tarea:

1. Haga clic en el botón **Avanzado**.

2. Active la casilla **Usar una contraseña para modificar el conjunto de componentes de la aplicación**.

3. Escriba las credenciales de la cuenta de usuario KAdmin.

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

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

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

## Paso 4. Configurar una planificación de inicio de tarea

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

## Paso 5. Definir el nombre de la tarea

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

## Paso 6. Conclusión de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

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

[Cómo añadir o quitar componentes de la aplicación en Web Console y Cloud Console](#) 

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

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

## Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

2. En la lista desplegable **Tipo de tarea**, seleccione **Cambiar componentes de la aplicación**.

3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Añadir el componente Control de aplicaciones*).

4. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

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

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

## Paso 3. Conclusión de la creación de tareas

Seleccione la casilla **Abrir los detalles de la tarea cuando se complete la creación** y finalice el Asistente. En las propiedades de la tarea, seleccione la pestaña **Configuración de la aplicación** y seleccione los componentes de la aplicación que estarán disponibles.

De ser necesario, habilite la [protección con contraseña](#) para realizar la tarea:

1. En el bloque **Configuración avanzada**, seleccione la casilla de verificación **Usar una contraseña para modificar el conjunto de componentes de la aplicación**.

2. Escriba las credenciales de la cuenta de usuario KLAdmin.

Guarde los cambios y ejecute la tarea.

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

## Actualización de una versión anterior de la aplicación



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

- Se recomienda cerrar todas las aplicaciones activas antes de realizar la actualización.
- Si el equipo tiene discos duros cifrados utilizando el [Cifrado de disco completo \(FDE\)](#), necesita descifrar todos los discos duros cifrados para actualizar Kaspersky Endpoint Security de la versión 10 a la versión 11.0.0 o posterior.

Antes de que comience la actualización, Kaspersky Endpoint Security bloqueará la característica de cifrado de disco completo. Si el cifrado de disco completo no se pudiera bloquear, la instalación de actualización no se iniciará. El cifrado de disco completo se desbloqueará una vez que concluya la actualización.

Puede actualizar las siguientes versiones de Kaspersky Endpoint Security:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 para Windows (compilación 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 para Windows (compilación 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 para Windows (compilación 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 para Windows (compilación 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 para Windows SF1 (compilación 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 para Windows (compilación 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 para Windows (compilación 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 para Windows (compilación 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 para Windows CF1 (compilación 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 para Windows (compilación 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 para Windows (compilación 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 para Windows (compilación 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 para Windows (compilación 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 para Windows (compilación 11.7.0.669).

Cuando Kaspersky Endpoint Security 10 Service Pack 2 para Windows se actualiza a Kaspersky Endpoint Security 11.8.0 para Windows, los archivos colocados tanto en Cuarentena como en la Copia de seguridad de la versión anterior se transfieren a la Copia de seguridad de la versión nueva. Para versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, los archivos que se colocaron en Copia de seguridad y Cuarentena en una versión anterior de la aplicación no se migran a la versión más reciente.

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

- de forma local, utilizando el [Asistente de instalación](#):

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

Si la aplicación que se utiliza en la red corporativa presenta un conjunto de componentes distintos del conjunto predeterminado, actualizar la aplicación a través de la Consola de administración (MMC) es diferente de actualizar la aplicación a través de Web Console y Cloud Console. Cuando actualice Kaspersky Endpoint Security, tenga en cuenta lo siguiente:

- Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.  
Si ha creado un paquete de instalación para la nueva versión de la aplicación con el conjunto de componentes predeterminado, el conjunto de componentes en el equipo de un usuario no cambiará. Para usar Kaspersky Endpoint Security con el conjunto de componentes predeterminado, debe [abrir las propiedades del paquete de instalación](#), cambiar el conjunto de componentes y, después, volver al conjunto de componentes original y guardar los cambios.
- Consola de administración de Kaspersky Security Center.  
El conjunto de componentes de la aplicación después de la actualización coincidirá con el conjunto de componentes en el paquete de instalación. Siempre que la nueva versión de la aplicación tenga el conjunto de componentes predeterminado, entonces, por ejemplo, la prevención de ataques de BadUSB se eliminará del equipo, ya que este componente se excluye del conjunto predeterminado. Para seguir utilizando la aplicación con el mismo conjunto de componentes que antes de la actualización, seleccione los componentes necesarios en la [configuración del paquete de instalación](#).

## Eliminar la aplicación

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

Kaspersky Endpoint Security se puede desinstalar del equipo de varias maneras:

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

Si seleccionó el componente Endpoint Agent durante la instalación de la aplicación, las siguientes dos aplicaciones se instalarán en el equipo: Kaspersky Endpoint Security y Kaspersky Endpoint Agent. Después de desinstalar Kaspersky Endpoint Security, Kaspersky Endpoint Agent también se desinstalará automáticamente.

## Desinstalación 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 quitar la aplicación mediante la Consola de administración \(MMC\)](#) 

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

### Paso 1. Selección del tipo de tarea

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

### Paso 2. Selección de la aplicación que se quitará

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

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

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

### Paso 4. Desinstalación de la configuración de utilidades

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

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

Si la operación para desinstalar la aplicación está [protegida con contraseña](#), haga lo siguiente:

1. Active la casilla **Utilizar contraseña de desinstalación**.

2. Haga clic en el botón **Editar**.

3. Escriba la contraseña de la cuenta KLAdmin.

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

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

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

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

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

## Paso 7. Selección de la cuenta para ejecutar la tarea

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

## Paso 8. Configurar una planificación de inicio de tarea

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

## Paso 9. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Desinstalar Kaspersky Endpoint Security 11.8.0*.

## Paso 10. Finalización de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

La aplicación se desinstalará en modo silencioso.

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

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

## Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.

2. En la lista desplegable **Tipo de tarea**, seleccione **Desinstalar aplicación en remoto**.

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

4. En la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

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

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

## Paso 3. Configuración de los parámetros para desinstalar la aplicación

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

1. Seleccione **Desinstalar aplicación administrada**.

2. Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

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

- **Usando el Agente de red**. Si el Agente de red no se ha instalado en el equipo, primero se instalará el Agente de red utilizando las herramientas del sistema operativo. Kaspersky Endpoint Security se desinstalará entonces con las herramientas del Agente de red.
- **Usando los recursos del sistema operativo mediante el Servidor de administración**. La utilidad se enviará a los equipos cliente a través del Servidor de administración, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.
- **Usando los recursos del sistema operativo mediante puntos de distribución**. La utilidad se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si existe al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, consulte la [Ayuda de Kaspersky Security Center](#).

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

número de solicitudes ayudará a evitar que la red se sobrecargue.

5. En el campo **Número máximo de intentos de desinstalación**, establezca un límite a la cantidad de veces que se intentará desinstalar la aplicación. Cuando la desinstalación de Kaspersky Endpoint Security finaliza con un error, la tarea hace un nuevo intento automáticamente.
6. Si es necesario, desactive la casilla **Verificar el tipo de sistema operativo antes de descargar**. Esto evitará que la utilidad de desinstalación se descargue si el sistema operativo del equipo no cumple con los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple los requisitos de software, puede omitir esta verificación.

#### Paso 4. Selección de la cuenta para ejecutar la tarea

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

#### Paso 5. Conclusión de la creación de tareas

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

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

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

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

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea **Desinstalar aplicación en remoto** de Kaspersky Security Center.  
Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Active la casilla **Utilizar contraseña de desinstalación**.
5. Escriba la contraseña de la cuenta KLAdmin.
6. Guarde los cambios.

## Desinstalación de la aplicación mediante el Asistente de instalación

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

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

Los datos que puede guardar son los siguientes:

- **Datos de activación.** Si conserva estos datos, no necesitará volver a activar la aplicación. Mientras la licencia siga vigente al momento de realizar la instalación, Kaspersky Endpoint Security añadirá una clave de licencia automáticamente.
- **Archivos de la copia de seguridad.** Estos son los archivos que la aplicación analizó y guardó en Copia de seguridad.

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

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

- **Parámetros operativos 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.



## Licencias de la aplicación

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

### Acerca del Contrato de licencia de usuario final

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

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

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

- Al [instalar la aplicación de Kaspersky Endpoint Security en modo interactivo](#).
- Mediante la lectura del archivo license.txt. Este documento se incluye en el [kit de distribución de la aplicación](#) y también se encuentra en la carpeta de instalación de la aplicación %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security para Windows\Doc\

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

### Acerca de la licencia

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

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

Se proporcionan los siguientes tipos de licencia:

- *Licencia de evaluación*: Licencia gratuita destinada a probar la aplicación.  
La licencia de evaluación suele durar poco tiempo. Cuando finaliza la licencia de evaluación, se desactivan todas las funciones de Kaspersky Endpoint Security. Para seguir utilizando la aplicación, debe comprar una licencia comercial.  
Puede activar la aplicación con una licencia de prueba solo una vez.
- *Licencia comercial*: Licencia de pago que se facilita cuando compra Kaspersky Endpoint Security.  
La funcionalidad de la aplicación que está disponible con licencia comercial depende del tipo de producto elegido. El producto seleccionado se indica en el [Certificado de licencia](#). Encontrará información sobre los productos disponibles en el [sitio web de Kaspersky](#).  
Cuando la licencia comercial expira, las funciones clave de la aplicación se desactivan. Para seguir utilizando la aplicación, debe renovar la licencia comercial. Si no tiene pensado renovar la licencia, debe eliminar la aplicación del equipo.

## Acerca del certificado de la licencia

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

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

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

## Acerca de la suscripción

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

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

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

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

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

## Sobre una clave de licencia

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

Un [certificado de la licencia](#) no se proporciona para una clave añadida mediante suscripción.

Puede añadir una clave de licencia a la aplicación aplicando un archivo clave o introduciendo un código de activación.

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

Existen dos tipos de claves: activa y de reserva.

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

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

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

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

## Acerca del código de activación

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

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

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

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

## Acerca del archivo clave

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

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

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

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

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

- Póngase en contacto con el vendedor de la licencia.
- Obtenga un archivo clave en el [sitio web de Kaspersky](#) según su código de activación existente.

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

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

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

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

Comparación de las funciones de Kaspersky Endpoint Security

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
<b>Protección frente a amenazas avanzadas</b>						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓
Prevención de	✓	✓	✓	✓	✓	✓

intrusiones en el host						
Motor de reparación	✓	✓	✓	✓	✓	✓
<b>Protección frente a amenazas básicas</b>						
Protección frente a amenazas en archivos	✓	✓	✓	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en el correo	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓	✓	✓	✓
Protección AMSI	✓	✓	✓	✓	✓	✓
<b>Controles de seguridad</b>						
Control de aplicaciones	✓	✓	✓	✓	✓	✓
Control de dispositivos	✓	✓	✓	✓	✓	✓
Control Web	✓	✓	✓	✓	✓	✓
Control de anomalías adaptativo	-	✓	✓	✓	✓	✓
<b>Cifrado de datos</b>						
Cifrado de disco de Kaspersky	-	✓	✓	✓	✓	✓
Cifrado de unidad BitLocker	-	✓	✓	✓	✓	✓
Cifrado de archivos	-	✓	✓	✓	✓	✓
Cifrado de unidades extraíbles	-	✓	✓	✓	✓	✓
<b>Detection and Response</b>						

Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox <i>(La licencia de Kaspersky Sandbox se debe comprar por separado)</i>	✓	✓	✓	✓	✓	✓

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

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

[Consulte también la comparación de la funcionalidad de la aplicación para estaciones de trabajo](#)

Comparación de las funciones de Kaspersky Endpoint Security

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
<b>Protección frente a amenazas avanzadas</b>						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓
Prevención de intrusiones en el host	–	–	–	–	–	–
Motor de reparación	✓	✓	✓	✓	✓	✓
<b>Protección frente a amenazas básicas</b>						

Protección frente a amenazas en archivos	✓	✓	✓	✓	✓	✓
Protección frente a amenazas web	–	✓	✓	✓	✓	✓
Protección frente a amenazas en el correo	–	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓	✓	✓	✓
Prevención de ataques de BadUSB	✓	✓	✓	✓	✓	✓
Protección AMSI	✓	✓	✓	✓	✓	✓
<b>Controles de seguridad</b>						
Control de aplicaciones	–	✓	✓	✓	✓	✓
Control de dispositivos	–	✓	✓	✓	✓	✓
Control Web	–	✓	✓	✓	✓	✓
Control de anomalías adaptativo	–	–	–	–	–	–
<b>Cifrado de datos</b>						
Cifrado de disco de Kaspersky	–	–	–	–	–	–
Cifrado de unidad BitLocker	–	✓	✓	✓	✓	✓
Cifrado de archivos	–	–	–	–	–	–
Cifrado de unidades extraíbles	–	–	–	–	–	–
<b>Detection and Response</b>						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky	✓	✓	✓	✓	✓	✓

Sandbox (La licencia de Kaspersky Sandbox se debe comprar por separado)						
--	--	--	--	--	--	--

## Activación de la aplicación

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

Puede activar la aplicación de una de las siguientes formas:

- Localmente en la interfaz de la aplicación, con el [Asistente de activación](#). Puede añadir la clave activa y la clave de reserva de esta manera.
- En forma remota con el [conjunto de software de Kaspersky Security Center](#) al crear y luego iniciar una tarea para añadir una clave de licencia. Puede añadir la clave activa y la clave de reserva de esta manera.
- En forma remota, distribuyendo a los equipos cliente archivos clave y códigos de activación que estén almacenados en el depósito de claves del Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la distribución de claves, consulte la [Ayuda de Kaspersky Security Center](#). Puede añadir la clave activa y la clave de reserva de esta manera.

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

- Mediante la [línea de comandos](#).

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

## Activación de la aplicación a través de Kaspersky Security Center

Puede activar la aplicación en forma remota mediante Kaspersky Security Center de las siguientes maneras:

- Uso de la tarea *Añadir clave*.  
Este método puede usarse para añadir una clave tanto en un equipo específico como en una serie de equipos pertenecientes a un grupo de administración.
- Distribuyendo a los equipos una clave almacenada en el Servidor de administración de Kaspersky Security Center.



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


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

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

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

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

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

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

[Cómo activar la aplicación en la Consola de administración \(MMC\)](#)

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

## Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)** → **Añadir clave**.

## Paso 2. Añadir una clave

Introduzca un [código de activación](#) o seleccione un archivo clave.

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

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

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

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

## Paso 4. Configurar una planificación de inicio de tarea

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

## Paso 5. Definir el nombre de la tarea

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

## Paso 6. Conclusión de la creación de tareas

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

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

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

### Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Añadir clave**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Activación de Kaspersky Endpoint Security para Windows*).
4. En la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea. Ir al paso siguiente.

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

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

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

### Paso 3. Selección de una licencia

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

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

### Paso 4. Conclusión de la creación de tareas

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

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

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

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Licencias de Kaspersky**.  
Se mostrará una lista de claves de licencia.
2. Abra las propiedades de la clave de licencia.
3. En la sección **General**, seleccione la casilla **Clave de licencia distribuida automáticamente**.
4. Guarde los cambios.

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

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

1. En la ventana principal de Web Console, seleccione **Operaciones** → **Licencias** → **Licencias de Kaspersky**.  
Se mostrará una lista de claves de licencia.
2. Abra las propiedades de la clave de licencia.
3. En la pestaña **General**, active el interruptor **Implementar clave de licencia automáticamente**.
4. Guarde los cambios.

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

## Uso del asistente de activación para activar la aplicación

*Para activar Kaspersky Endpoint Security mediante el asistente de activación:*

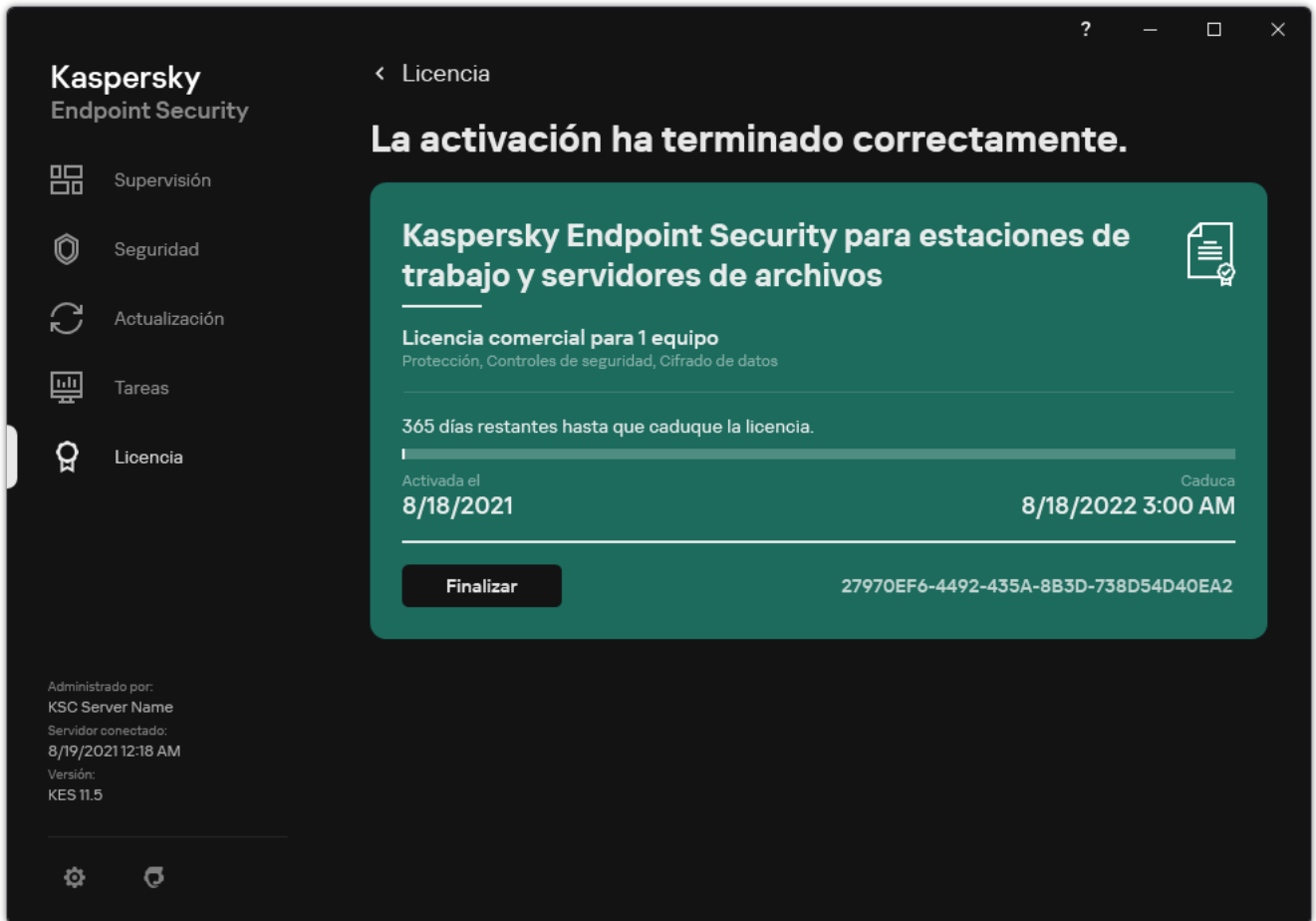
1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.
2. Haga clic en el botón **Activar la aplicación con una licencia nueva**.

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

## Visualización de información de la licencia

Visualización de información sobre una licencia:

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



Ventana Licencia

La sección muestra los siguientes detalles:

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

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

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

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

- **Comprar licencia/Renovar la licencia.** Abre la tienda en línea de Kaspersky, un sitio web donde podrá comprar o renovar una licencia. Para hacer un pedido, deberá escribir los datos de su empresa y realizar el pago.
- **Activar la aplicación con una licencia nueva.** Abre el Asistente de activación de la aplicación. Use el asistente para añadir una clave con un código de activación o un archivo clave. El Asistente de activación de la aplicación le permitirá añadir una clave de licencia activa y un máximo de una clave de licencia de reserva.

## Compra de una licencia

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

*Para adquirir una licencia:*

1. En la ventana principal de la aplicación, vaya a la sección **Licencia**.
2. Realice una de las siguientes acciones:
  - Si no se ha añadido ninguna clave o se ha añadido una clave de una licencia de evaluación, haga clic en el botón **Comprar licencia**.
  - Si se ha añadido la clave de una licencia comercial, haga clic en el botón **Renovar la licencia**.

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

## Renovación de suscripciones

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

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

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

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

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

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

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

## Provisión de datos

### Provisión de datos según el Contrato de licencia de usuario final

Si se aplica un [código de activación](#) para activar Kaspersky Endpoint Security, acepta que la siguiente información se transmitirá a Kaspersky en forma periódica y automática con el fin de que se verifique el uso correcto de la aplicación:

- tipo, versión y localización de Kaspersky Endpoint Security;
- versiones de las actualizaciones instaladas para Kaspersky Endpoint Security;
- ID del equipo e ID de la instalación específica de Kaspersky Endpoint Security en el equipo;
- el número de serie del certificado e identificador de la clave de licencia activa;
- tipo, versión y velocidad de bits del sistema operativo, y nombre del entorno virtual (si Kaspersky Endpoint Security está instalado en un entorno virtual);
- ID de los componentes de Kaspersky Endpoint Security que están activos cuando se transmite la información.

Kaspersky también puede usar esta información para generar estadísticas sobre la difusión y el uso del software de Kaspersky.

Al usar un código de activación, acepta transmitir automáticamente los datos indicados anteriormente. Si no acepta transmitir esta información a Kaspersky, debe usar un [archivo clave](#) para activar Kaspersky Endpoint Security.

Al aceptar las condiciones del Contrato de licencia de usuario final, acepta transmitir automáticamente la siguiente información:

- Al actualizar Kaspersky Endpoint Security:
  - versión de Kaspersky Endpoint Security;
  - ID de Kaspersky Endpoint Security;
  - clave activa;
  - ID exclusivo de la ejecución de la tarea de actualización;
  - ID exclusivo de la instalación de Kaspersky Endpoint Security.
- Al seguir los enlaces desde la interfaz de Kaspersky Endpoint Security:
  - versión de Kaspersky Endpoint Security;
  - versión del sistema operativo;
  - fecha de activación de Kaspersky Endpoint Security;
  - fecha de caducidad de la licencia;



- fecha de creación de la clave;
- fecha de instalación de Kaspersky Endpoint Security;
- ID de Kaspersky Endpoint Security;
- ID de la vulnerabilidad detectada en el sistema operativo;
- ID de la última actualización instalado para Kaspersky Endpoint Security;
- hash del archivo detectado como amenaza y el nombre de esta amenaza según la clasificación de Kaspersky;
- categoría del error de activación de Kaspersky Endpoint Security;
- código del error de activación de Kaspersky Endpoint Security;
- número de días antes del vencimiento de la clave;
- número de días que han pasado desde que se añadió la clave;
- número de días que han pasado desde que se caducó la licencia;
- número de equipos en los que se aplica la licencia activa;
- clave activa;
- período de validez de la licencia de Kaspersky Endpoint Security;
- estado actual de la licencia;
- tipo de licencia activa;
- tipo de aplicación;
- ID exclusivo de la ejecución de la tarea de actualización;
- ID exclusivo de la instalación de Kaspersky Endpoint Security en el equipo;
- idioma de la interfaz de Kaspersky Endpoint Security.

La información recibida cuenta con protección de Kaspersky de acuerdo con la ley, los requisitos y las normativas aplicables de Kaspersky. Los datos se transmiten a través de canales de comunicación cifrados.

Puede leer el Contrato de licencia de usuario final y visitar el [sitio web de Kaspersky](#) para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn\_<ID de idioma>.txt con el texto del Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network se incluyen en el [kit de distribución](#) de la aplicación.

## Provisión de datos al usar Kaspersky Security Network

El conjunto de datos que Kaspersky Endpoint Security envía a Kaspersky depende del tipo de licencia y de la configuración de uso de Kaspersky Security Network.

## Uso de KSN bajo licencia en no más de 4 equipos

Al aceptar la Declaración de Kaspersky Security Network, acepta transmitir automáticamente la siguiente información:

- información sobre las actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida, código de error de la actualización de la configuración;
- información sobre los archivos y las direcciones URL que deben escanearse: las sumas de comprobación del archivo escaneado (MD5, SHA2-256, SHA1) y el patrón del archivo (MD5), el tamaño del patrón, el tipo de amenaza detectada y su nombre de acuerdo con la clasificación del Titular de los derechos; el identificador de las bases de datos antivirus, la dirección URL en la que se solicita la reputación, así como la dirección URL de referencia, el identificador del protocolo de conexión y el número del puerto utilizado;
- ID de la tarea de análisis que detectó la amenaza;
- información sobre los certificados digitales que se usaron y que se necesitaba para verificar su autenticidad: las sumas de comprobación (SHA256) del certificado que se usó para firmar el objeto analizado y la clave pública del certificado;
- identificador del componente de software que realiza el análisis;
- identificadores de las bases de datos antivirus y de los registros de estas bases de datos antivirus;
- información sobre la activación del Software en el ordenador: encabezado del ticket firmado por el servicio de activación (identificador del centro de activación regional, suma de control del código de activación, suma de control del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket, estado de la licencia, fecha y hora de inicio y fin de la validez del ticket, identificador único de la licencia, versión de la licencia), identificador del certificado utilizado para firmar el encabezado del ticket, suma de control (MD5) del archivo clave;
- Información sobre el Titular de los derechos del Software: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

## Uso de KSN bajo licencia en 5 o más equipos

Al aceptar la Declaración de Kaspersky Security Network, acepta transmitir automáticamente la siguiente información:

Si se selecciona la casilla de verificación **Kaspersky Security Network** y se desactiva la casilla **Activar el modo ampliado de KSN**, la aplicación envía la siguiente información:

- información sobre las actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida, código de error de la actualización de la configuración;
- información sobre los archivos y las direcciones URL que deben escanearse: las sumas de comprobación del archivo escaneado (MD5, SHA2-256, SHA1) y el patrón del archivo (MD5), el tamaño del patrón, el tipo de amenaza detectada y su nombre de acuerdo con la clasificación del Titular de los derechos; el identificador de las bases de datos antivirus, la dirección URL en la que se solicita la reputación, así como la dirección URL de referencia, el identificador del protocolo de conexión y el número del puerto utilizado;
- ID de la tarea de análisis que detectó la amenaza;
- información sobre los certificados digitales que se usaron y que se necesitaba para verificar su autenticidad: las sumas de comprobación (SHA256) del certificado que se usó para firmar el objeto analizado y la clave pública del certificado;

- identificador del componente de software que realiza el análisis;
- identificadores de las bases de datos antivirus y de los registros de estas bases de datos antivirus;
- información sobre la activación del Software en el ordenador: encabezado del ticket firmado por el servicio de activación (identificador del centro de activación regional, suma de control del código de activación, suma de control del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket, estado de la licencia, fecha y hora de inicio y fin de la validez del ticket, identificador único de la licencia, versión de la licencia), identificador del certificado utilizado para firmar el encabezado del ticket, suma de control (MD5) del archivo clave;
- Información sobre el Titular de los derechos del Software: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

Si se selecciona **Activar el modo ampliado de KSN** además de la casilla **Kaspersky Security Network**, la aplicación también enviará la información indicada a continuación, además de la enumerada arriba:

- información sobre los resultados de la categorización de los recursos web solicitados, lo que contiene la URL procesada y la dirección IP del host, la versión del componente del Software que realizó la categorización, el método de categorización y el conjunto de categorías que definió el recurso web;
- información sobre el software instalado en el equipo: nombres de las aplicaciones de software y de los proveedores de software, claves de registro y sus valores, información sobre los archivos de los componentes de software instalados (sumas de comprobación [MD5, SHA2-256, SHA1], nombre, ruta al archivo en el equipo, tamaño, versión y firma digital);
- información sobre el estado de la protección antivirus del equipo: las versiones y las marcas de tiempo de lanzamiento de las bases de datos antivirus que se utilizan, el ID de la tarea y el ID del Software que realiza el análisis;
- información sobre los archivos descargados por el Usuario final: la dirección URL y la dirección IP de la descarga y dirección URL de la página que se visitó antes de la página de descarga, el identificador del protocolo de descarga y el número de puerto de conexión, el estado de las direcciones URL como maliciosas o no, los atributos de archivo, el tamaño y las sumas de comprobación (MD5, SHA2-256, SHA1), información sobre el proceso que ha descargado el archivo (sumas de comprobación [MD5, SHA2-256, SHA1], la fecha y la hora de creación/compilación, el estado de reproducción automática, los atributos, los nombres de compresores, información sobre las firmas, el indicador de archivo ejecutable, el identificador de formato y el tipo de cuenta utilizada para iniciar el proceso), información sobre el archivo del proceso (nombre, ruta de archivo y tamaño), el nombre del archivo y su ruta en el equipo, la firma digital del archivo y la fecha y la hora de su generación, la dirección URL donde se produjo la detección, el número de script en la página que parece sospechosa o dañina e información sobre las peticiones HTTP generadas y la respuesta a las mismas;
- información sobre las aplicaciones que se ejecutan y sus módulos: los datos sobre procesos que se ejecutan en el sistema (el identificador del proceso [PID], el nombre del proceso; la información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, el indicio de programa o proceso de confianza, la ruta de acceso completa a los archivos del proceso y sus sumas de comprobación (MD5, SHA2-256, SHA1), y la línea de comandos de inicio; el nivel de integridad del proceso; una descripción del producto al que pertenece el proceso [el nombre del producto y la información sobre el editor], así como los certificados digitales utilizados y la información necesaria para verificar su autenticidad o la información acerca de la ausencia de la firma digital de un archivo); información sobre los módulos cargados en los procesos (sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación [MD5, SHA2-256, SHA1], las rutas de acceso a estos en el equipo); información sobre el encabezado del archivo PE, los nombres de los empaquetadores (si el archivo estaba empaquetado);
- información sobre todos los objetos y actividades potencialmente maliciosos: nombre del objeto detectado y ruta completa al objeto en el equipo, sumas de comprobación de los archivos procesados (MD5, SHA2-256, SHA1), fecha y hora de detección, nombres y tamaños de los archivos infectados y rutas a estos archivos, código de plantilla de la ruta, indicador de si el objeto es un contenedor o no, indicador de archivo ejecutable,

nombre del compresor (si el archivo estaba comprimido), código del tipo de archivo, ID del formato de archivo, lista de acciones realizadas por el malware y decisión tomada por el software y el usuario en respuesta, identificadores de las bases de datos antivirus y de los registros en estas bases de datos antivirus usados para tomar la decisión, indicador de objeto potencialmente malicioso, nombre de la amenaza detectada según la clasificación del titular de los derechos, nivel de peligro, estado y método de detección, razón por la que se incluyó en el contexto analizado y número de secuencia del archivo en el contexto, sumas de comprobación (MD5, SHA2-256, SHA1), nombre y atributos del archivo ejecutable de la aplicación a través del que se transmitió el mensaje o enlace infectado, direcciones IP despersonalizadas (IPv4 e IPv6) del host del objeto bloqueado, entropía del archivo, indicador de archivo autoejecutable, hora en que el archivo se detectó por primera vez en el sistema, número de veces que se ha ejecutado el archivo desde que se enviaron las últimas estadísticas, información sobre el nombre, sumas de comprobación (MD5, SHA2-256, SHA1) y tamaño del cliente de correo a través del que se recibió el objeto malicioso, ID de la tarea de software que realizó el análisis, indicador de si se comprobaron la reputación del archivo y la firma o no, resultado de procesamiento del archivo, suma de comprobación (MD5) del patrón obtenido para el objeto, tamaño del patrón en bytes y especificaciones técnicas de las tecnologías de detección aplicadas;

- información sobre los objetos analizados: el grupo de confianza asignado en el que se ubicó el archivo o desde el que se ubicó; el motivo por el que el archivo se ubicó en esa categoría; el identificador de la categoría; la información sobre el origen de las categorías y la versión de la base de datos de la categoría; la marca de certificado de confianza del archivo; el nombre del proveedor del archivo; la versión del archivo; el nombre y la versión de la aplicación de software que contiene el archivo;
- información sobre las vulnerabilidades detectadas: el identificador de la vulnerabilidad en la base de datos de vulnerabilidades, la clase de riesgo de la vulnerabilidad;
- información acerca de la emulación del archivo ejecutable: el tamaño del archivo y sus sumas de comprobación (MD5, SHA2-256, SHA1); la versión del componente de la emulación, la profundidad de la emulación, el conjunto de propiedades de los bloques lógicos y las funciones situadas dentro de estos bloques que se obtuvieron durante la emulación; los datos provenientes de los encabezados de PE del archivo ejecutable;
- las direcciones IP del equipo atacante (IPv4 e IPv6), el número del puerto del equipo al que se dirige el ataque de red, el identificador del protocolo del paquete IP que contiene el ataque, el objetivo del ataque (nombre de la organización, sitio web), la marca de la reacción ante el ataque, la ponderación del ataque y el nivel de confianza;
- información sobre ataques asociados a recursos de red falsificados, y las direcciones IP (IPv4 e IPv6) y DNS de los sitios web visitados;
- direcciones IP (IPv4 o IPv6) y DNS del recurso web solicitado; la información sobre el archivo y el cliente web que accede al recurso web; información sobre el archivo y el cliente web que accede al recurso web; el nombre, el tamaño y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo, ruta completa al archivo y código de plantilla de la ruta, el resultado de la comprobación de la firma digital y su estado de conformidad con KSN;
- información sobre reversión de acciones de malware: los datos del archivo cuya actividad se ha revertido (el nombre del archivo, ruta entera al archivo, su tamaño y sumas de comprobación (MD5, SHA2-256, SHA1)), datos de acciones correctas y fallidas a eliminar, renombra y copia archivos y restaura los valores en el registro (los nombres de las claves de registro y sus valores), e información sobre los archivos del sistema modificados por el malware, antes y después de la reversión.
- información sobre las exclusiones establecidas para el componente de Control de anomalías adaptativo: la identificación y el estado de la regla que se ejecutó, la acción llevada a cabo por el Software cuando se ejecutó la regla, el tipo de cuenta de usuario con la cual el proceso o el hilo lleva a cabo una actividad sospechosa, información sobre el proceso que realizó o recibió la actividad sospechosa (identificación de la secuencia o nombre del archivo del proceso, ruta de acceso completa al archivo del proceso, código del patrón de la ruta, sumas de comprobación [MD5, SHA2-256, SHA1] del archivo del proceso); información sobre el objeto que llevó a cabo las actividades sospechosas, así como sobre el objeto que quedó sujeto a acciones sospechosas (nombre de la clave de registro o nombre del archivo, ruta completa al archivo, código del patrón de la ruta, y sumas de comprobación [MD5, SHA2-256, SHA1] del archivo);

- Información sobre los módulos de software cargados: nombre, tamaño y sumas de comprobación (MD5, SHA2-256, SHA1) del archivo del módulo, la ruta completa hacia el archivo y código de la plantilla de la ruta, configuración de la firma digital del archivo del módulo, fecha y hora de la creación de la firma, nombre del asunto y organización que firmó el archivo del módulo, ID del proceso en el cual se cargó el módulo, nombre del proveedor del módulo y número de secuencia del módulo en la cola que carga.
- información sobre la calidad de la interacción del Software con los servicios KSN: fecha y hora de comienzo y finalización del periodo en el que se generaron las estadísticas, información sobre la calidad de las solicitudes y conexión con cada uno de los servicios KSN utilizados (identificador del servicio KSN, cantidad de solicitudes exitosas, cantidad de solicitudes con respuestas del caché, cantidad de solicitudes no exitosas (problemas de red, KSN desactivado en la configuración del Software, ruta incorrecta), intervalo de tiempo de las solicitudes exitosas, intervalo de tiempo de las solicitudes canceladas, intervalo de tiempo de las solicitudes con límite de tiempo excedido, cantidad de conexiones a KSN tomadas del caché, cantidad de conexiones exitosas a KSN, cantidad de conexiones no exitosas a KSN, cantidad de transacciones exitosas, cantidad de transacciones no exitosas, intervalo de tiempo de las conexiones exitosas a KSN, intervalo de tiempo de las conexiones no exitosas a KSN, intervalo de tiempo de las transacciones exitosas, intervalo de tiempo de las transacciones no exitosas);
- si se detecta un objeto posiblemente malicioso, se debe proporcionar información sobre los datos en la memoria de los procesos: los elementos de la jerarquía de los objetos del sistema (ObjectManager), los datos de la memoria EFI BIOS, los nombres de las claves del registro y sus valores;
- información sobre los eventos en los registros de los sistemas: la marca de tiempo del evento, el nombre del registro en el que se encontró el evento, el tipo y la categoría del evento, el nombre de la fuente del evento y su descripción;
- información sobre las conexiones de red: la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo desde el que se inició el proceso de apertura del puerto, la ruta de acceso al archivo del proceso y su firma digital, las direcciones IP locales y remotas, la cantidad de puertos de conexión local y remota, el estado de conexión, y la marca de tiempo de apertura del puerto;
- información sobre la fecha de instalación y activación del Software en el equipo: el ID del socio que vendió la licencia, el número de serie de la licencia, el encabezado firmado del ticket del servicio de activación (el ID de un centro de activación regional, el suma de control del código de activación, las suma de comprobación del ticket, la fecha de creación del ticket, el ID único del ticket, la versión del ticket, el estado de la licencia, la fecha y hora de inicio/finalización del ticket, el ID único de la licencia, la versión de la licencia), el ID del certificado utilizado para firmar el encabezado del ticket, la suma de comprobación (MD5) del archivo clave, el ID único de la instalación del software en el equipo, el tipo y el ID de la aplicación que se actualiza, el ID del tarea de actualización;
- información sobre el conjunto de todas las actualizaciones instaladas y el conjunto de las últimas actualizaciones instaladas o eliminadas, el tipo de evento que ocasionó que se enviara la información de actualización, el tiempo transcurrido desde la instalación de la última actualización, y la información sobre las bases de datos antivirus instaladas;
- información sobre el funcionamiento del software en el equipo: datos de uso de la CPU, datos de uso de memoria (Bytes Privados, grupo no paginado, grupo paginado), número de amenazas activas en el proceso de software y amenazas pendientes y el tiempo de funcionamiento del software antes del error.
- cantidad de volcados de software y volcados del sistema (BSOD) desde que se instaló el Software y a partir del momento de la última actualización, identificador y la versión del módulo del Software en la que se produjo el error, la pila de memoria del proceso del Software e información sobre las bases de datos antivirus en el momento en que se generó el error;
- datos acerca del volcado del sistema (BSOD): la marca que refleja su aparición en el equipo, el nombre del controlador que provocó el BSOD, la dirección y la pila de memoria del controlador, la marca que refleja la duración de la sesión del SO antes de que ocurriera el BSOD, la pila de memoria de los controladores que se bloquearon, el tipo de volcado de la memoria almacenada, la marca de la sesión del SO antes de que el BSOD se prolongara por más de 10 minutos, el identificador único del volcado y la marca de tiempo del BSOD;

- información sobre los errores o problemas de rendimiento que tuvieron lugar durante la operación de los componentes del Software: identificación del estado del Software, tipo de error, código y causa, así como el horario en el que ocurrió el error, identificador del componente, módulo y proceso del producto en el que tuvo lugar el error, identificador de la tarea o categoría de actualización en el que tuvo lugar el error, registros de los controladores que utiliza el Software (código de error, nombre del módulo, nombre del archivo de origen y línea en la que ocurrió el error);
- información sobre las actualizaciones de bases de datos de antivirus y componentes del Software: nombre, fecha y horario de los archivos de índice descargados durante la última actualización y en descarga en la actualización vigente;
- información sobre la terminación anormal de la operación del Software: marca de tiempo de la creación del volcado, su tipo, tipo de evento que provocó la terminación anormal del funcionamiento del Software (cierre inesperado, error en la aplicación de terceros), fecha y horario del cierre inesperado;
- información sobre la compatibilidad de los controladores del Software con el hardware y el Software: información sobre las propiedades del sistema operativo que limitan la funcionalidad de los componentes del Software (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), tipo de Software de descarga instalado (UEFI, BIOS), identificador de módulo de plataforma segura (TPM), versión de especificación de TPM, información sobre el CPU instalado en el equipo, modo operativo y parámetros de la Integridad del Código y la Protección de Dispositivos, modo de funcionamiento de los controladores y motivo para utilizar el modo actual, versión de los controladores del Software, estado de soporte de virtualización del software y del hardware del equipo;
- información acerca de las aplicaciones externas que generaron el error: su nombre, la versión y la ubicación; el código de error y la información sobre este, proveniente del registro de aplicaciones del sistema; la dirección de la aparición del error y la pila de la memoria de la aplicación externa; la marca que representa la aparición del error en el componente del Software; el período durante el cual funcionó la aplicación externa antes de que se produjera el error; las sumas de comprobación (MD5, SHA2-256, SHA1) de la imagen del proceso de la aplicación en el cual ocurrió el error; la ruta de acceso a la imagen del proceso de la aplicación y el código del patrón de la ruta de acceso; la información del registro del sistema, con una descripción del error asociado a la aplicación; la información sobre el módulo de la aplicación en la que se produjo el error (el identificador de la excepción, la ubicación del error en la memoria como un desplazamiento del módulo de la aplicación, el nombre y la versión del módulo, el identificador del error de la aplicación en el complemento del Titular de los derechos y la pila de memoria del error, y la duración de la sesión de aplicación antes de que se produjera el error);
- versión del componente de actualización del Software y la cantidad de errores que ocurrieron en este componente durante la ejecución de tareas de actualización durante su ciclo de vida, el identificador de los tipos de tareas de actualización, la cantidad de intentos fallidos que realizó el componente de actualización a fin de completar las tareas correspondientes;
- información sobre el funcionamiento de los componentes de monitoreo del sistema del Software: versiones completas de los componentes, fecha y hora en que se iniciaron los componentes, código del evento que desbordó la cola de eventos y la cantidad de dichos eventos, cantidad total de eventos de desborde de la cola, información sobre el archivo del proceso del iniciador del evento (nombre de archivo y su ruta en el equipo, código de plantilla de la ruta del archivo, sumas de comprobación (MD5, SHA2-256, SHA1) del proceso asociado con el archivo, versión del archivo), identificador de la intercepción del evento que tuvo lugar, versión completa del filtro de intercepción, identificador del tipo de evento interceptado, tamaño de la cola del evento y la cantidad de eventos entre el primer evento de la cola y el evento actual, cantidad de eventos vencidos en la cola, información sobre el archivo del proceso del iniciador del evento actual (nombre del archivo y su ruta en el equipo, código de patrón de la ruta del archivo, sumas de comprobación (MD5, SHA2-256, SHA1) del proceso asociado con el archivo), duración del procesamiento del evento, duración máxima del procesamiento del evento, probabilidad del envío de estadísticas, información sobre los eventos del sistema operativo respecto de los cuales se excedió el límite de tiempo de procesamiento (fecha y hora del evento, cantidad de inicializaciones reiteradas de las base de datos de antivirus, fecha y hora de la inicialización repetida por última vez de las base de datos de antivirus después de su actualización, tiempo de demora de procesamiento del evento para cada uno de los componentes de monitoreo del sistema, cantidad de eventos en cola, cantidad de eventos procesados, cantidad de eventos demorados del tipo actual, tiempo de demora total para los eventos del tipo actual, tiempo de demora total para todos los eventos);

- información de la herramienta de seguimiento de eventos de Windows (Event Tracing for Windows, ETW) en caso de que se presenten problemas de rendimiento con el Software, proveedores de eventos SysConfig/SysConfigEx/WinSATAssessment de Microsoft: información sobre el equipo (modelo, fabricante, factor de forma del alojamiento, versión), información sobre las métricas de rendimiento de Windows (evaluaciones WinSAT, índice de rendimiento de Windows), nombre de dominio, información sobre los procesadores físicos y lógicos (cantidad de procesadores físicos y lógicos, fabricante, modelo, nivel de revisión, cantidad de núcleos, frecuencia del reloj, CUID, 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 reinicializable, dirección de desplazamiento de la partición en relación con el inicio del disco), información sobre la placa madre BIOS (fabricante, fecha de lanzamiento, versión), información sobre la placa madre (fabricante, modelo, tipo), información sobre la memoria física (capacidad compartida y libre), información sobre los servicios del sistema operativo (nombre, descripción, estado, etiqueta, información sobre los procesos [nombre y PID]), parámetros de consumo de energía para el equipo, configuración del controlador de interrupción, ruta a las carpetas del sistema de Windows (Windows y System32), información sobre el sistema operativo (versión, edición, fecha de lanzamiento, nombre, tipo, fecha de instalación), tamaño del archivo de página, información sobre monitores (cantidad, fabricante, permiso de pantalla, capacidad de resolución, tipo), información sobre el controlador de la tarjeta de video (fabricante, fecha de lanzamiento, versión);
- información sobre ETW, proveedores de eventos EventTrace/EventMetadata de Microsoft: información sobre la secuencia de eventos del sistema (tipo, horario, fecha, zona horaria), metadatos sobre el archivo con resultados de rastreo (nombre, estructura, parámetros de rastreo, desglose de la cantidad de operaciones de pista por tipo), información sobre el sistema operativo (nombre, tipo, versión, edición, fecha de lanzamiento, hora de inicio);
- información de ETW, proveedores de eventos de Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power de Microsoft: información sobre los procesos iniciados y completos (nombre, PID, parámetros de inicio, línea de comando, código de retorno, parámetros de administración de la energía, horario de inicio y compleción, tipo de token de acceso, SID, SessionID, cantidad de descriptores instalados), información sobre los cambios en las prioridades del hilo (TID, prioridad, horario), información sobre las operaciones de disco del proceso (tipo, horario, capacidad, cantidad), historial de cambios en la estructura y capacidad de procesos de memoria utilizable;
- información de ETW, proveedores de eventos StackWalk/Perfinfo de Microsoft; información sobre los contadores de rendimiento (rendimiento de secciones de código individual, secuencia de llamadas de función, PID, TID, direcciones y atributos de ISR y DPC);
- información de ETW, proveedor de eventos KernelTraceControl-ImageID de Microsoft: información sobre los archivos ejecutables y las bibliotecas dinámicas (nombre, tamaño de la imagen, ruta completa), información sobre archivos PDB (nombre, identificador), datos de recursos VERSIONINFO para los archivos ejecutables (nombre, descripción, creador, ubicación, versión e identificador de la aplicación, versión del archivo e identificador);
- información de ETW; proveedores de eventos FileIo/DiskIo/Image/Windows Kernel Disk de Microsoft: información sobre el archivo y las operaciones del disco (tipo, capacidad, horario de inicio, horario de compleción, duración, estado de compleción, PID, TID, direcciones de llamada de la función del controlador, Paquete de Solicitud de E/S (IRP), atributos de objeto de archivo de Windows), información sobre los archivos

que forman parte de operaciones de archivo y disco (nombre, versión, tamaño, ruta completa, atributos, desplazamiento, suma de comprobación de la imagen, acciones abiertas y de acceso);

- información de ETW, proveedor de eventos PageFault de Microsoft: información sobre los errores de acceso de la página de memoria (dirección, horario, capacidad, PID, TID, atributos del objeto de archivo de Windows, parámetros de distribución de la memoria);
- información de ETW, proveedor de eventos de hilo de Microsoft: información sobre la creación/compleción del hilo, información sobre hilos iniciados (PID, TID, tamaño de la pila, prioridades y asignación de recursos del CPU, recursos de E/S, páginas de memoria entre hilos, dirección de la pila, dirección de la función init, dirección del Thread Environment Block [TEB], etiqueta de servicios de Windows);
- información de ETW, proveedor de eventos Microsoft Windows Kernel Memory de Microsoft: información sobre las operaciones de administración de la memoria (estado de compleción, hora, cantidad, PID), estructura de asignación de la memoria (tipo, capacidad, SessionID, PID);
- información sobre el funcionamiento del Software en caso de problemas de rendimiento: identificador de la instalación del Software, tipo y valor de caída en el rendimiento, información sobre la secuencia de eventos en el Software (hora, zona horaria, tipo, estado de compleción, identificador del componente de Software, identificador del escenario operativo del Software, TID, PID, direcciones de llamada de funciones), información sobre las conexiones de red a verificarse (URL, dirección de la conexión, tamaño del paquete de red), información sobre los archivos PDB (nombre, identificador, tamaño de imagen del archivo ejecutable), información sobre los archivos a verificarse (nombre, ruta completa; suma de comprobación), parámetros de monitoreo del rendimiento del Software;
- información sobre el último reinicio fallido del SO: la cantidad de reinicios fallidos desde la instalación del SO, datos sobre el volcado del sistema (el código y los parámetros del error; el nombre, la versión y la suma de comprobación [CRC32] del módulo que generó el error en el funcionamiento del SO; la ubicación del error como un desplazamiento en el módulo; las sumas de comprobación [MD5, SHA2-256, SHA1] del volcado del sistema);
- información para verificar la autenticidad de los certificados digitales que se utilizan para firmar archivos: la huella digital del certificado, el algoritmo de la suma de comprobación, la clave pública y el número de serie del certificado, el nombre del emisor del certificado, el resultado de la validación del certificado y el identificador de la base de datos del certificado;
- información sobre el proceso que ejecuta el ataque a la autoprotección del software: el nombre y el tamaño del archivo del proceso, sus sumas de comprobación (MD5, SHA2-256, SHA1), la ruta completa al archivo del proceso y el código de plantilla de la ruta del archivo, las marcas de fecha de creación y compilación, indicador de archivo ejecutable, atributos del archivo de proceso, información sobre el certificado utilizado para firmar el archivo del proceso, código de la cuenta utilizada para iniciar el proceso, identificador de operaciones realizadas para acceder al proceso, tipo de recurso sobre el que se realiza la operación (proceso, archivo, objeto de registro, función de búsqueda FindWindow), nombre del recurso sobre el que se realiza la operación, indicador del éxito de la operación, estado del archivo del proceso y su firma según KSN;
- información sobre el Software del Titular de los derechos: versión completa, tipo, ubicación y estado de funcionamiento del Software utilizado, versiones de los componentes del Software instalados y su estado de funcionamiento, información sobre las actualizaciones de Software instaladas, el valor del filtro TARGET, la versión del protocolo utilizado para conectarse a los servicios del Titular de los derechos;
- información sobre el hardware instalado en el equipo: el tipo, el nombre, el nombre del modelo, la versión del firmware, los parámetros de los dispositivos integrados y conectados, el identificador único del Equipo con el Software instalado;
- información sobre las versiones del sistema operativo y las actualizaciones instaladas, el tamaño de las palabras, la edición y los parámetros del modo de ejecución del SO, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del SO, fecha y horario de inicio del SO;



- archivos ejecutables y no ejecutables, total o parcialmente;
- porciones de la RAM del equipo;
- sectores involucrados en el proceso de arranque del sistema operativo;
- paquetes de datos de tráfico de red;
- páginas web y correos electrónicos que contienen objetos sospechosos y maliciosos;
- descripción de las clases e instancias de clases del repositorio WMI;
- informes de actividad de la aplicación:
  - el nombre, tamaño y versión del archivo que se envía, su descripción y sumas de comprobación (MD5, SHA2-256, SHA1), identificador de formato de archivo, el nombre del proveedor del archivo, el nombre del producto al que pertenece el archivo, ruta completa al archivo en el equipo, código de plantilla de la ruta, la creación y modificación de las marcas de tiempo del archivo;
  - fecha/hora de inicio y finalización del período de validez del certificado (si el archivo tiene una firma digital), la fecha y la hora de la firma, el nombre del emisor del certificado, información sobre el titular del certificado, la huella dactilar, la clave pública del certificado y los algoritmos correspondientes y el número de serie del certificado;
  - el nombre de la cuenta desde la que se ejecuta el proceso;
  - sumas de comprobación (MD5, SHA2-256, SHA1) del nombre del equipo en la que se ejecuta el proceso;
  - títulos de las ventanas de proceso;
  - Identificador de las bases de datos antivirus, nombre de la amenaza detectada según la clasificación del Titular de los derechos;
  - datos sobre la licencia instalada, su identificador, tipo y fecha de caducidad;
  - hora local del equipo en el momento de la provisión de información;
  - nombres y rutas de los archivos a los que accedió el proceso;
  - nombres de claves de registro y sus valores a los que accedió el proceso;
  - Direcciones URL e IP a las que accedió el proceso;
  - Direcciones URL e IP desde las que se descargó el archivo en ejecución.

## Provisión de datos al usar soluciones de Detection and Response

En equipos con Kaspersky Endpoint Security instalado, los datos preparados para el envío automático a los servidores de [Kaspersky Endpoint Detection and Response](#) y [Kaspersky Sandbox](#) se almacenan. Los archivos se almacenan en los equipos de forma simple, no encriptada.

El conjunto específico de datos depende de la solución en la que se utilice Kaspersky Endpoint Security.

# Kaspersky Endpoint Detection and Response

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

## Datos recibidos como resultado la ejecución de la tarea Análisis de IOC (tarea estándar)

Kaspersky Endpoint Security envía automáticamente datos sobre los resultados de la ejecución de la tarea *Análisis de IOC* a Kaspersky Security Center.

Los datos de los resultados de la ejecución de la tarea *Análisis de IOC* pueden contener la siguiente información:

- Dirección IP de la tabla ARP
- Dirección física de la tabla ARP
- Tipo y nombre del registro de DNS
- Dirección IP del equipo protegido
- Dirección física (dirección MAC) del equipo protegido
- Identificador en la entrada del registro de eventos
- Nombre del origen de los datos del registro
- Nombre de registro
- Hora del evento
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo (ruta incluida)
- Tamaño del archivo
- Dirección IP remota y puerto al que se estableció la conexión durante el análisis
- Dirección IP del adaptador local
- Puerto abierto en el adaptador local
- Protocolo como un número (de acuerdo con el estándar IANA)
- Nombre del proceso
- Argumentos del proceso
- Ruta al archivo de proceso

- Identificador de Windows (PID) del proceso
- Identificador de Windows (PID) del proceso principal
- Cuenta de usuario que inició el proceso
- Fecha y hora en que se inició el proceso
- Nombre del servicio
- Descripción del servicio
- Ruta y nombre del servicio DLL (para svchost)
- Ruta y nombre del archivo ejecutable del servicio
- Identificador de Windows (PID) del servicio
- Tipo de servicio (por ejemplo, un controlador o adaptador de kernel)
- Estado del servicio
- Modo de lanzamiento del servicio
- Nombre de la cuenta de usuario
- Nombre del volumen
- Letra del volumen
- Tipo de volumen
- Valor del registro de Windows
- Valor de colmena de registro
- Ruta de la clave de registro (sin nombre de colmena ni de valor)
- Configuración del registro
- Sistema (entorno)
- Nombre y versión del sistema operativo instalado en el equipo
- Nombre de red del equipo protegido
- Dominio o grupo al que pertenece el equipo protegido
- Nombre del navegador
- Versión del navegador
- Hora en que se accedió por última vez al recurso web
- URL de la solicitud HTTP

- Nombre de la cuenta utilizada para la solicitud HTTP
- Nombre de archivo del proceso que realizó la solicitud HTTP
- Ruta completa al archivo del proceso que realizó la solicitud HTTP
- Identificador de Windows (PID) del proceso que realizó la solicitud HTTP
- Referencia HTTP (URL de origen de la solicitud HTTP)
- URI del recurso solicitado a través de HTTP
- Información sobre el agente de usuario HTTP (la aplicación que realizó la solicitud HTTP)
- Tiempo de ejecución de la solicitud HTTP
- Identificador único del proceso que realizó la solicitud HTTP

## Datos para crear una cadena de desarrollo de la amenaza

De forma predeterminada, los datos para crear una cadena de desarrollo de la amenaza se almacenan durante siete días. Los datos se envían automáticamente a Kaspersky Security Center.

Los datos para crear una cadena de desarrollo de la amenaza pueden contener la siguiente información:

- Fecha y hora del incidente
- Nombre de detección
- Modo de análisis
- Estado de la última acción relacionada con la detección
- Motivo por el que falló el procesamiento de la detección
- Tipo de objeto detectado
- Nombre del objeto detectado
- Estado de amenaza después de que se procese el objeto
- Razón por la que falló la ejecución de acciones en el objeto
- Acciones realizadas para revertir acciones maliciosas
- Información sobre el objeto procesado:
  - Identificador único del proceso
  - Identificador único del proceso principal
  - Identificador único del archivo de proceso
  - Identificador de proceso de Windows (PID)

- Línea de comando del proceso
- Cuenta de usuario que inició el proceso
- Código de la sesión de inicio de sesión en la que se está ejecutando el proceso
- Tipo de sesión en la que se está ejecutando el proceso
- Nivel de integridad del proceso que se está procesando
- Membresía de la cuenta de usuario que inició el proceso en los grupos locales y de dominio con privilegios
- Identificador del objeto procesado
- Nombre completo del objeto procesado
- Identificador del dispositivo protegido
- Nombre completo del objeto (nombre de archivo local o dirección web del archivo descargado)
- Hash MD5 o SHA256 del objeto procesado
- Tipo de objeto procesado
- Fecha de creación del objeto procesado
- Fecha en que se modificó por última vez el objeto procesado
- Tamaño del objeto procesado
- Atributos del objeto procesado
- Organización que firmó el objeto procesado
- Resultado de la verificación del certificado digital del objeto procesado
- Identificador de seguridad (SID) del objeto procesado
- Identificador de zona horaria del objeto procesado
- Dirección web de la descarga del objeto procesado (solo para archivos en disco)
- Nombre de la aplicación que descargó el archivo
- Hashes MD5 y SHA256 de la aplicación que descargó el archivo
- Nombre de la aplicación que modificó por última vez el archivo
- Hashes MD5 y SHA256 de la aplicación que modificó por última vez el archivo
- Número de inicios de objetos procesados
- Fecha y hora en que se inició por primera vez el objeto
- Identificadores únicos del archivo

- Nombre completo del archivo (nombre del archivo local o dirección web del archivo descargado)
- Ruta a la variable del registro de Windows procesada
- Nombre de la variable del registro de Windows procesada
- Valor de la variable del registro de Windows procesada
- Tipo de la variable del registro de Windows procesada
- Indicador de la membresía de la clave de registro procesada en el punto de ejecución automática
- Dirección web de la solicitud web procesada
- Origen del enlace de la solicitud web procesada
- Agente de usuario de la solicitud web procesada
- Tipo de solicitud web procesada (GET o POST).
- Puerto IP local de la solicitud web procesada
- Puerto IP remoto de la solicitud web procesada
- Dirección de conexión (entrante o saliente) de la solicitud web procesada
- Identificador del proceso en el que se incrustó el código malicioso

## Kaspersky Sandbox

Todos los datos que la aplicación almacena localmente en el equipo se eliminan del mismo cuando Kaspersky Endpoint Security se desinstala.

### Datos de servicio

Kaspersky Endpoint Security almacena los siguientes datos procesados durante la respuesta automática:

- Archivos procesados y datos ingresados por el usuario durante la configuración del agente integrado de Kaspersky Endpoint Security:
  - Archivos en Cuarentena
  - Clave pública del certificado utilizado para la integración con Kaspersky Sandbox
- Caché del agente integrado de Kaspersky Endpoint Security:
  - Hora en que los resultados del análisis se escribieron en la memoria caché
  - Hash MD5 de la tarea de análisis

- Identificador de tarea de análisis
- Resultado del análisis del objeto
- Cola de solicitudes de análisis de objetos:
  - ID del objeto en la cola
  - Hora en que el objeto se colocó en la cola
  - Estado de procesamiento del objeto en la cola
  - ID de la sesión de usuario en el sistema operativo donde se creó la tarea de análisis de objetos
  - Identificador del sistema (SID) del usuario del sistema operativo cuya cuenta se utilizó para crear la tarea
  - Hash MD5 de la tarea de análisis de objetos
- Información sobre las tareas para las que el agente integrado de Kaspersky Endpoint Security espera los resultados del análisis de Kaspersky Sandbox:
  - Hora en que se recibió la tarea de análisis de objetos
  - Estado de procesamiento del objeto
  - ID de la sesión de usuario en el sistema operativo donde se creó la tarea de análisis de objetos
  - Identificador de la tarea de análisis de objetos
  - Hash MD5 de la tarea de análisis de objetos
  - Identificador del sistema (SID) del usuario del sistema operativo cuya cuenta se utilizó para crear la tarea
  - Esquema XML de la IOC creada automáticamente
  - Hash MD5 o SHA256 del objeto analizado
  - Errores de procesamiento
  - Nombres de los objetos para los que se creó la tarea
  - Resultado del análisis del objeto

## Datos en solicitudes a Kaspersky Sandbox

Los siguientes datos de las solicitudes del agente integrado de Kaspersky Endpoint Security a Kaspersky Sandbox se almacenan localmente en el equipo:

- Hash MD5 de la tarea de análisis
- Identificador de tarea de análisis
- Objeto analizado y todos los archivos relacionados

## Datos recibidos como resultado de la ejecución de la tarea Análisis de IOC (tarea independiente)

Kaspersky Endpoint Security envía automáticamente datos sobre los resultados de la ejecución de la tarea *Análisis de IOC* a Kaspersky Security Center.

Los datos de los resultados de la ejecución de la tarea *Análisis de IOC* pueden contener la siguiente información:

- Dirección IP de la tabla ARP
- Dirección física de la tabla ARP
- Tipo y nombre del registro de DNS
- Dirección IP del equipo protegido
- Dirección física (dirección MAC) del equipo protegido
- Identificador en la entrada del registro de eventos
- Nombre del origen de los datos del registro
- Nombre de registro
- Hora del evento
- Hashes MD5 y SHA256 del archivo
- Nombre completo del archivo (ruta incluida)
- Tamaño del archivo
- Dirección IP remota y puerto al que se estableció la conexión durante el análisis
- Dirección IP del adaptador local
- Puerto abierto en el adaptador local
- Protocolo como un número (de acuerdo con el estándar IANA)
- Nombre del proceso
- Argumentos del proceso
- Ruta al archivo de proceso
- Identificador de Windows (PID) del proceso
- Identificador de Windows (PID) del proceso principal
- Cuenta de usuario que inició el proceso
- Fecha y hora en que se inició el proceso
- Nombre del servicio



- Descripción del servicio
- Ruta y nombre del servicio DLL (para svchost)
- Ruta y nombre del archivo ejecutable del servicio
- Identificador de Windows (PID) del servicio
- Tipo de servicio (por ejemplo, un controlador o adaptador de kernel)
- Estado del servicio
- Modo de lanzamiento del servicio
- Nombre de la cuenta de usuario
- Nombre del volumen
- Letra del volumen
- Tipo de volumen
- Valor del registro de Windows
- Valor de colmena de registro
- Ruta de la clave de registro (sin nombre de colmena ni de valor)
- Configuración del registro
- Sistema (entorno)
- Nombre y versión del sistema operativo instalado en el equipo
- Nombre de red del equipo protegido
- Dominio o grupo al que pertenece el equipo protegido
- Nombre del navegador
- Versión del navegador
- Hora en que se accedió por última vez al recurso web
- URL de la solicitud HTTP
- Nombre de la cuenta utilizada para la solicitud HTTP
- Nombre de archivo del proceso que realizó la solicitud HTTP
- Ruta completa al archivo del proceso que realizó la solicitud HTTP
- Identificador de Windows (PID) del proceso que realizó la solicitud HTTP
- Referencia HTTP (URL de origen de la solicitud HTTP)

- URI del recurso solicitado a través de HTTP
- Información sobre el agente de usuario HTTP (la aplicación que realizó la solicitud HTTP)
- Tiempo de ejecución de la solicitud HTTP
- Identificador único del proceso que realizó la solicitud HTTP

## Cumplimiento de la legislación de la Unión Europea (GDPR)

Kaspersky Endpoint Security puede transmitir datos a Kaspersky en los siguientes escenarios:

- Uso de Kaspersky Security Network.
- Activar la aplicación con un código de activación.
- Actualización de módulos de aplicaciones y bases de datos antivirus.
- Al seguir enlaces en la interfaz de la aplicación.
- Escritura de volcado.

Independientemente de la clasificación de datos y el territorio desde el que se reciben los datos, Kaspersky se adhiere a altos estándares de seguridad de datos y emplea diversas medidas legales, organizativas y técnicas para proteger los datos de los usuarios, para garantizar la seguridad y confidencialidad de los datos y, también, para garantizar el cumplimiento de los derechos de los usuarios garantizados por la legislación aplicable. El texto de la Política de privacidad se incluye en el [kit de distribución de la aplicación](#) y está disponible en el [sitio web de Kaspersky](#).

Antes de utilizar Kaspersky Endpoint Security, lea atentamente la descripción de los datos transmitidos en el [Contrato de licencia de usuario final](#) y la [Declaración de Kaspersky Security Network](#). Si los datos específicos transmitidos desde Kaspersky Endpoint Security en cualquiera de los escenarios descritos pueden clasificarse como datos personales de acuerdo con su legislación o estándar local, debe asegurarse de que dichos datos se procesen legalmente y obtener el consentimiento de los usuarios finales para la recopilación y transmisión de tales datos.

Puede leer el Contrato de licencia de usuario final y visitar el [sitio web de Kaspersky](#) para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn\_<ID de idioma>.txt con el texto del Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network se incluyen en el [kit de distribución](#) de la aplicación.

Si no desea transmitir datos a Kaspersky, puede desactivar la provisión de datos.

### Usar Kaspersky Security Network

Al utilizar Kaspersky Security Network, acepta proporcionar automáticamente los datos enumerados en la [Declaración de Kaspersky Security Network](#). Si no acepta proporcionar estos datos a Kaspersky, utilice KSN privada o [desactive el uso de KSN](#). Para más información sobre KSN Privada, consulte la documentación de Kaspersky Private Security Network.

### Activar la aplicación con un código de activación

Al utilizar un código de activación, acepta proporcionar automáticamente los datos enumerados en el [Contrato de licencia de usuario final](#). Si no acepta proporcionar estos datos a Kaspersky, utilice un [archivo clave para activar Kaspersky Endpoint Security](#).

## Actualización de módulos de aplicaciones y bases de datos antivirus

Al utilizar los servidores de Kaspersky, acepta proporcionar automáticamente los datos enumerados en el [Contrato de licencia de usuario final](#). Kaspersky requiere esta información para verificar que Kaspersky Endpoint Security se esté utilizando legítimamente. Si no acepta proporcionar esta información a Kaspersky, utilice [Kaspersky Security Center para actualizaciones de la base de datos](#) o [Kaspersky Update Utility](#).

## Al seguir enlaces en la interfaz de la aplicación

Al utilizar enlaces en la interfaz de la aplicación, acepta proporcionar automáticamente los datos enumerados en el [Contrato de licencia de usuario final](#). La lista precisa de datos transmitidos en cada enlace específico depende de dónde se encuentra el enlace en la interfaz de la aplicación y del problema que pretende resolver. Si no acepta proporcionar estos datos a Kaspersky, utilice la [interfaz simplificada de la aplicación](#) u [oculte la interfaz de la aplicación](#).

## Escritura de volcado

Si ha [activado la escritura de volcado](#), Kaspersky Endpoint Security creará un archivo de volcado que contendrá todos los datos de la memoria de los procesos de la aplicación al momento en que se creó este archivo de volcado.

## Primeros pasos

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

- [Interfaz de la aplicación local](#).
- Consola de administración de Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

### Consola de administración de Kaspersky Security Center

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

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

Para obtener más información sobre cómo administrar la aplicación a través de Kaspersky Security Center, consulte la [Ayuda de Kaspersky Security Center](#).

### Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (en adelante también llamada *Web Console*) es una aplicación web con la que podrá 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 más información sobre Kaspersky Security Center Web Console, consulte la [Ayuda de Kaspersky Security Center](#).

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

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

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

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

# Acerca del Complemento de administración de Kaspersky Endpoint Security para Windows

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

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

De manera predeterminada, el complemento web no forma parte de la instalación de Kaspersky Security Center Web Console. A diferencia del complemento de administración para la Consola de administración de Kaspersky Security Center, que se instala en la estación de trabajo del administrador, el complemento web debe instalarse en el mismo equipo que 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. La lista de complementos web instalados puede consultarse mediante la interfaz Web Console: **Configuración de la consola** → **Complementos web**. Para más información sobre la compatibilidad de Web Console con las distintas versiones de complemento web, consulte la [Ayuda de Kaspersky Security Center](#).

## Instalación del complemento web

Puede instalar el complemento web de las siguientes maneras:

- Instale el complemento web mediante el Asistente de inicio rápido de Kaspersky Security Center Web Console. Web Console le pedirá que ejecute el Asistente de inicio rápido cuando se conecte Web Console al Servidor de administración por primera vez. También podrá abrir el Asistente de inicio rápido desde la interfaz de Web Console (**Detección y despliegue** → **Despliegue y asignación** → **Asistente de inicio rápido**). El Asistente de inicio rápido le permitirá, asimismo, verificar si los complementos web instalados son los más recientes y descargar las actualizaciones que sean necesarias. Para obtener más información sobre el Asistente de inicio rápido de Kaspersky Security Center Web Console, consulte la [Ayuda de Kaspersky Security Center](#).
- Instale el complemento web mediante la lista de paquetes de distribución disponibles en Web Console. Para instalar el complemento web, en la interfaz de Web Console, seleccione el paquete de distribución del complemento web de Kaspersky Endpoint Security: **Configuración de la consola** → **Complementos**. La lista de paquetes de distribución disponibles se actualiza automáticamente cada vez que se publican versiones nuevas de las aplicaciones de Kaspersky.
- Descargando el paquete de distribución a Web Console desde una ubicación externa. Para instalar el complemento web, añada el archivo ZIP correspondiente al paquete de distribución del complemento web de Kaspersky Endpoint Security en la interfaz de Web Console: **Configuración de la consola** → **Complementos**. El paquete de distribución del complemento web puede descargarse, por ejemplo, del sitio web de Kaspersky.

## Actualización del complemento de administración

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

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

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

Puede actualizar el complemento web de las siguientes maneras:

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

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

- Desde un archivo.

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

Si se abre algún elemento (por ejemplo, una directiva o una tarea), el complemento web comprueba su información de compatibilidad. Si la versión del complemento web es igual o posterior a la especificada en la información de compatibilidad, puede cambiar la configuración de este elemento. De lo contrario, no podrá usar el complemento web para cambiar la configuración del elemento seleccionado. Se recomienda actualizar el complemento web.

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

Puede administrar Kaspersky Endpoint Security a través de Kaspersky Security Center solo si tiene un complemento de administración cuya versión sea igual o posterior a la versión especificada en la información relacionada con la compatibilidad de Kaspersky Endpoint Security con el complemento de administración. Puede ver la versión mínima requerida del complemento de administración en el archivo `installer.ini` incluido en el [kit de distribución](#).

Si se abre algún elemento (por ejemplo, una directiva o una tarea), el complemento de administración comprueba su información de compatibilidad. Si la versión del complemento de administración es igual o superior a la especificada en la información de compatibilidad, puede cambiar la configuración de este elemento. De lo contrario, no podrá usar el complemento de administración para cambiar la configuración del elemento seleccionado. Se recomienda actualizar el complemento de administración.

Actualizar el Complemento de administración de Kaspersky Endpoint Security 10 para Windows

Si el complemento de administración de Kaspersky Endpoint Security 10 para Windows está instalado en la Consola de administración, considere lo siguiente al instalar el Complemento de administración de Kaspersky Endpoint Security 11 para Windows:


- El Complemento de administración de Kaspersky Endpoint Security 10 para Windows no se eliminará y estará disponible para la operación. Por lo tanto, podrá acceder a dos complementos de administración para trabajar con las versiones 10 y 11 de la aplicación.
- El Complemento de administración de Kaspersky Endpoint Security 11 para Windows no admite la administración de Kaspersky Endpoint Security 10 para Windows en los equipos de los usuarios.
- El Complemento de administración de Kaspersky Endpoint Security 11 para Windows no admite elementos (por ejemplo, directivas o tareas) creados con el Complemento de administración de Kaspersky Endpoint Security 10 para Windows.

Puede usar el Asistente de conversión en lote de directivas y tareas para convertir directivas y tareas de la versión 10 a la versión 11. Para obtener más información sobre la conversión de directivas y tareas, consulte la [Ayuda de Kaspersky Security Center](#).



## Actualizar el Complemento de administración de Kaspersky Endpoint Security 11 para Windows

Si el Complemento de administración de Kaspersky Endpoint Security 11 para Windows está instalado en la Consola de administración, considere lo siguiente al instalar una nueva versión del Complemento de administración de Kaspersky Endpoint Security 11 para Windows:

- La versión anterior del Complemento de administración de Kaspersky Endpoint Security 11 para Windows se eliminará.
- La nueva versión del Complemento de administración de Kaspersky Endpoint Security 11 para Windows admite la administración de la versión anterior de Kaspersky Endpoint Security 11 para Windows en los equipos de los usuarios.
- Puede utilizar la nueva versión del complemento de administración para cambiar la configuración de directivas, tareas y otros elementos creados con la versión anterior del complemento.
- Para los parámetros nuevos, la nueva versión del complemento de administración asigna los valores predeterminados cuando se guarda una directiva, un perfil de directiva o una tarea por primera vez.

Después de actualizar el complemento de administración, se recomienda comprobar y guardar los valores de la nueva configuración en directivas y perfiles de directiva. De no hacerlo así, los nuevos grupos de configuración de Kaspersky Endpoint Security en el equipo del usuario utilizarán los valores predeterminados y se podrán modificar (atributo ) . Se recomienda comprobar la configuración, empezando por las directivas y los perfiles de directiva en el nivel superior de la jerarquía. También se recomienda utilizar la cuenta de usuario que tenga derechos de acceso a todas las áreas funcionales de Kaspersky Security Center.

Para informarse sobre las nuevas funcionalidades de la aplicación, consulte las Notas de la versión o la [ayuda de aplicación](#).

- Si se ha añadido un nuevo parámetro a un grupo de configuración en la nueva versión del complemento de administración, no cambiará el estado definido anteriormente para el atributo /  de este grupo de configuración.

- Al actualizar el complemento de administración a la versión 11.2.0, debe abrir una directiva para convertirla automáticamente. Al hacerlo, Kaspersky Endpoint Security le solicitará confirmación para participar en KSN. Si ya ha actualizado la aplicación a la versión 11.20 en los equipos de su organización, la participación en KSN se deshabilitará hasta que acepte los términos de participación en KSN.

## Consideraciones especiales al utilizar protocolos cifrados para interactuar con servicios externos

Kaspersky Endpoint Security y Kaspersky Security Center utilizan un canal de comunicación cifrado con TLS (Transport Layer Security) para trabajar con servicios externos de Kaspersky. Kaspersky Endpoint Security utiliza servicios externos para las siguientes funciones:

- actualización de las bases de datos y módulos de la aplicación;
- activación de la aplicación con un código de activación (activación 2.0);
- uso de Kaspersky Security Network.

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

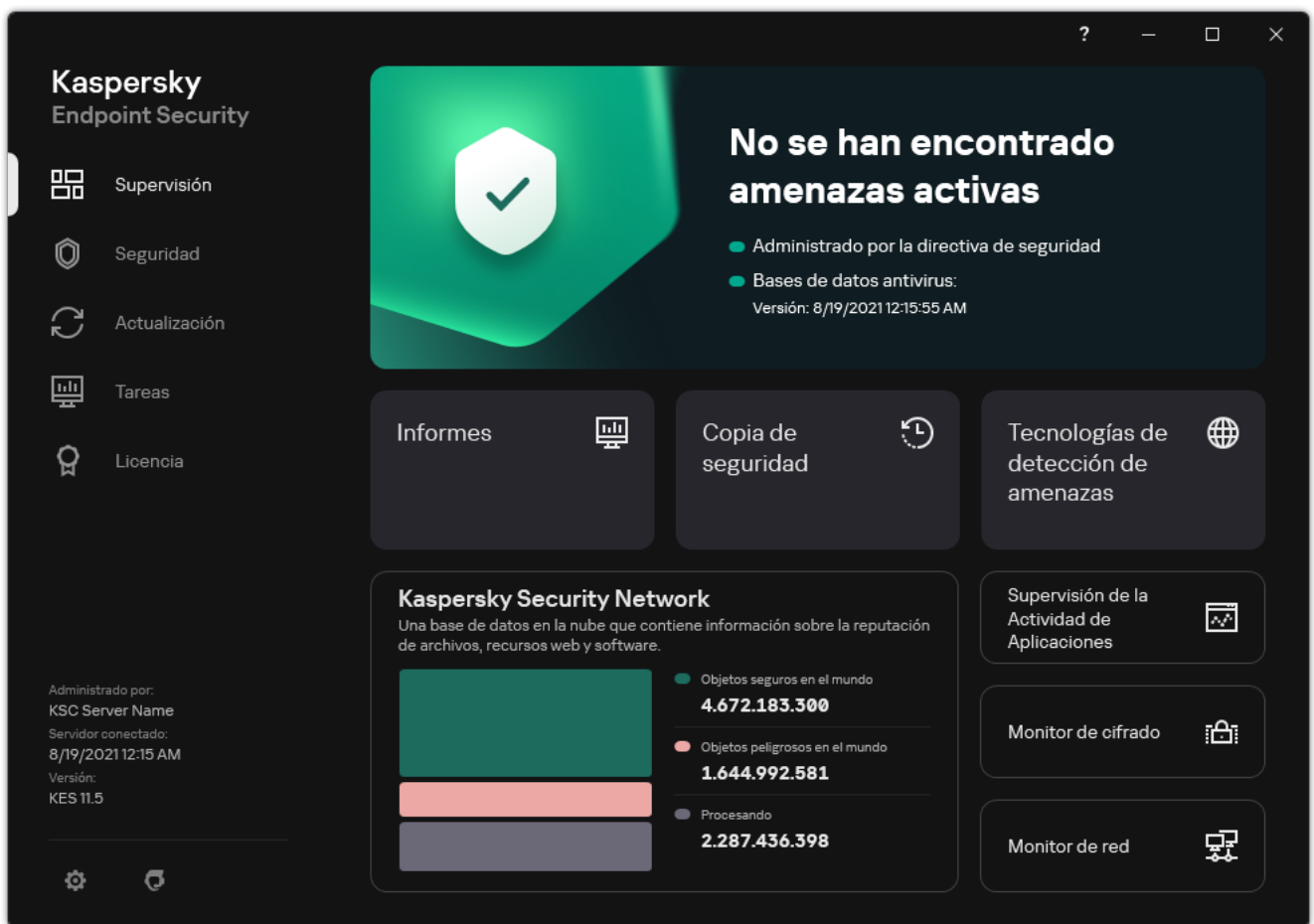
- Cifrado. Los contenidos de los mensajes son confidenciales y no se divulgan a terceros.
- Integridad. El destinatario del mensaje está seguro de que el contenido del mensaje no se ha modificado desde que el remitente lo reenvió.
- Autenticación. El destinatario está seguro de que la comunicación se establece solo con un servidor de Kaspersky de confianza.

Kaspersky Endpoint Security utiliza certificados de clave pública para la autenticación del servidor. Se requiere una infraestructura de clave pública (PKI) para trabajar con certificados. Una Autoridad de certificación es parte de una PKI. Kaspersky utiliza su propia Autoridad de certificación porque los servicios de Kaspersky son muy técnicos y no públicos. En este caso, cuando se revocan los certificados raíz de Thawte, VeriSign, GlobalTrust y otros, Kaspersky PKI permanece en condiciones de servicio y sin interrupciones.

Kaspersky Endpoint Security considera que los entornos que tienen MITM (herramientas de software y hardware que admiten el análisis del protocolo HTTPS) no son seguros. Es posible que se produzcan errores al trabajar con los servicios de Kaspersky. Por ejemplo, puede haber errores relacionados con el uso de certificados autofirmados. Estos errores pueden ocurrir porque una herramienta de inspección HTTPS de su entorno no reconoce a Kaspersky PKI. Para solucionar estos problemas, debe configurar [exclusiones para interactuar con servicios externos](#).

## Interfaz de la aplicación








Ventana principal de la aplicación

## Supervisión

- **Informes.** Ver eventos que ocurrieron durante el funcionamiento de la aplicación, componentes individuales y tareas.
- **Copia de seguridad.** Ver una lista de copias guardadas de archivos infectados que la aplicación ha eliminado.
- **Tecnologías de detección de amenazas.** Ver información sobre tecnologías de detección de amenazas y la cantidad de amenazas detectadas por estas tecnologías.
- **Kaspersky Security Network.** Estado de la conexión entre Kaspersky Endpoint Security y Kaspersky Security Network, y estadísticas globales de KSN. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security podrá utilizar los servicios de KSN para conocer la categoría y la reputación de los archivos analizados u obtener información sobre la reputación de las direcciones web que se analicen.
- **Supervisión de la actividad de aplicaciones.** Ver información sobre el funcionamiento de las aplicaciones instaladas. System Watcher realiza un seguimiento del archivo, el registro y los eventos del sistema asociados con una aplicación.
- **Monitor de red.** [Ver información sobre la actividad de red del equipo](#) en tiempo real.

	<ul style="list-style-type: none"> <li>• <b>Monitor de cifrado.</b> Supervisa el proceso de cifrado o descifrado del disco en tiempo real. El Monitor de cifrado está disponible si está instalado el componente Cifrado de disco de Kaspersky o el componente Cifrado de unidad BitLocker.</li> </ul>
<b>Seguridad</b>	Estado operativo de los componentes instalados. También puede proceder a configurar componentes o ver informes.
<b>Actualización</b>	Administrar las tareas de actualización de Kaspersky Endpoint Security. Puede <a href="#">actualizar las bases de datos antivirus y los módulos de la aplicación</a> y <a href="#">revertir la última actualización</a> . Un administrador puede <a href="#">ocultar la sección al usuario</a> o <a href="#">restringir la gestión de tareas</a> .
<b>Tareas</b>	Administrar las tareas de análisis de Kaspersky Endpoint Security. Puede ejecutar un <a href="#">análisis antivirus</a> y una <a href="#">comprobación de integridad de la aplicación</a> . Un administrador puede <a href="#">ocultar tareas a un usuario</a> o <a href="#">restringir la gestión de tareas</a> .
<b>Licencia</b>	Licencias de la aplicación. Puede <a href="#">adquirir una licencia</a> , <a href="#">activar la aplicación</a> o <a href="#">renovar una suscripción</a> . También puede <a href="#">ver información sobre la licencia actual</a> .
	Configurar parámetros de la aplicación. Un administrador puede <a href="#">prohibir cambios en la configuración de Kaspersky Security Center</a> .
	Información sobre la aplicación: versión actual de Kaspersky Endpoint Security, fecha de publicación de la base de datos, clave y otra información. También puede dirigirse a los recursos informativos de Kaspersky que ofrecen información útil y recomendaciones, además de respuestas a preguntas frecuentes sobre la manera de comprar, instalar y usar la aplicación.
	Mensajes que contienen información sobre actualizaciones disponibles y solicitudes de acceso a archivos y dispositivos cifrados.





## Icono de la aplicación en el área de notificaciones de la barra de tareas

Inmediatamente después de la instalación de Kaspersky Endpoint Security, su icono aparece en el área de notificaciones de la barra de tareas de Microsoft Windows.

El icono tiene las siguientes finalidades:

- Indica la actividad de la aplicación.
- Actúa como acceso directo al menú contextual y la ventana principal de la aplicación.

El funcionamiento de la aplicación se representa a través de los siguientes iconos de estado:

- El icono  indica que los componentes de protección fundamentales de la aplicación están activados. Kaspersky Endpoint Security mostrará una advertencia  si el usuario necesita realizar una acción, por ejemplo, reiniciar el equipo después de actualizar la aplicación.
- El icono  indica que los componentes de protección fundamentales de la aplicación están desactivados o han sufrido un error de funcionamiento. Los componentes de protección pueden sufrir un error de funcionamiento, por ejemplo, si la licencia ha caducado o como resultado de un error de la aplicación. Kaspersky Endpoint Security mostrará una advertencia  con una descripción del problema en la protección del equipo.

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

- **Kaspersky Endpoint Security para Windows.** Abre la ventana principal de la aplicación. En esta ventana puede ajustar el funcionamiento de los componentes y las tareas de la aplicación, así como ver las estadísticas de

archivos procesados y amenazas detectadas.

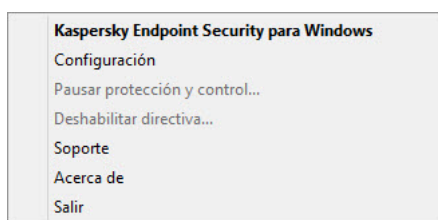
- **Pausar la protección/Reanudar la protección.** Permite poner en pausa todos los componentes de protección y control que no estén marcados con un candado (🔒) en la directiva. Recomendamos desactivar la directiva de Kaspersky Security Center antes de realizar esta operación.

Antes de pausar los componentes de protección y control, la aplicación le pedirá la [contraseña de acceso a Kaspersky Endpoint Security](#) (contraseña de cuenta o contraseña temporal). A continuación, podrá seleccionar la duración de la pausa. Los componentes pueden quedar en pausa por un tiempo específico, hasta que ocurra un reinicio o hasta que el usuario decida reanudarlos.

Este elemento del menú contextual está disponible si la [protección con contraseña está habilitada](#). Para que los componentes de protección y control comiencen a funcionar nuevamente, haga clic en **Reanudar la protección** en el menú contextual de la aplicación.

Pausar los componentes de protección y control no afecta el desempeño de las tareas de actualización y análisis. Tampoco suspende el uso de Kaspersky Security Network por parte de la aplicación.

- **Desactivar directiva/Activar directiva.** Desactivar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse. Si la directiva está desactivada, será necesario escribir la [contraseña de acceso a Kaspersky Endpoint Security](#) (contraseña de cuenta o contraseña temporal). Este elemento del menú contextual está disponible si la [protección con contraseña está habilitada](#). Para habilitar la directiva, seleccione **Activar directiva** en el menú contextual de la aplicación.
- **Configuración.** Permite abrir la ventana de configuración de la aplicación.
- **Soporte.** Esto abre una ventana que contiene la información necesaria para ponerse en contacto con el Soporte técnico de Kaspersky.
- **Acerca de.** Este elemento abre una ventana de información con detalles sobre la aplicación.
- **Salir.** Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este menú contextual, la aplicación se descarga de la RAM del equipo.



Menú contextual del icono de la aplicación

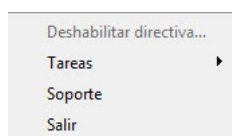
## Interfaz simplificada de la aplicación

Si una directiva de Kaspersky Security Center configurada para [visualizar la interfaz simplificada de la aplicación](#) se aplica a un equipo cliente con Kaspersky Endpoint Security instalado, la ventana principal de la aplicación no está disponible en este equipo cliente. Haga clic con el botón secundario para abrir el menú contextual del icono de Kaspersky Endpoint Security (consulte la siguiente figura) que contiene los elementos siguientes:

- **Desactivar directiva/Activar directiva.** Desactivar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse. Si la directiva está desactivada, será necesario escribir la [contraseña de acceso a Kaspersky Endpoint Security](#) (contraseña de cuenta o contraseña temporal).

Este elemento del menú contextual está disponible si la [protección con contraseña está habilitada](#). Para habilitar la directiva, seleccione **Activar directiva** en el menú contextual de la aplicación.

- **Tareas.** Lista desplegable que contiene los siguientes elementos:
  - **Comprobación de integridad.**
  - **Restauración de las bases de datos a su versión anterior.**
  - **Análisis completo.**
  - **Análisis personalizado.**
  - **Análisis de áreas críticas.**
  - **Actualización.**
- **Soporte.** Esto abre una ventana que contiene la información necesaria para ponerse en contacto con el Soporte técnico de Kaspersky.
- **Salir.** Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este menú contextual, la aplicación se descarga de la RAM del equipo.



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

## Configuración de la visualización de la interfaz de la aplicación

Puede configurar el modo de visualización de la interfaz de la aplicación para un usuario. El usuario puede interactuar con la aplicación de las siguientes formas:

- **Con la interfaz simplificada.** La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un [icono en el área de notificación de Windows](#). El usuario podrá [interactuar con Kaspersky Endpoint Security en forma limitada](#) a través del menú contextual de este icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
- **Con la interfaz completa.** En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al [icono ubicado en el área de notificaciones de Windows](#). El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
- **Sin interfaz.** No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El [icono del área de notificación de Windows](#) no estará disponible y tampoco se mostrará ninguna notificación.

[Cómo configurar el modo de visualización de la interfaz de la aplicación en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Interfaz**.
6. En el bloque **Interacción con el usuario**, lleve a cabo una de estas acciones:
  - Seleccione la casilla **Mostrar interfaz de usuario** si desea que los siguientes elementos de la interfaz se muestren en el equipo del cliente:
    - Carpeta que contiene el nombre de la aplicación en el menú **Iniciar**
    - [Icono de Kaspersky Endpoint Security](#) en el área de notificaciones de la barra de tareas de Microsoft Windows
    - Notificaciones emergentes

Si esta casilla está seleccionada, el usuario puede ver y (según los permisos disponibles) modificar la configuración de la aplicación en la interfaz de la aplicación.

  - Anule la selección de la casilla **Mostrar interfaz de usuario** si desea ocultar cualquier indicio de Kaspersky Endpoint Security en el equipo cliente.
7. En la sección **Interacción con el usuario**, seleccione la casilla **Mostrar interfaz simplificada** si desea que la [interfaz de aplicación simplificada](#) se muestre en un equipo cliente que tenga instalado Kaspersky Endpoint Security.

[Cómo configurar el modo de visualización de la interfaz de la aplicación en Web Console y en Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** → **Interfaz**.
5. En la sección **Interacción con el usuario**, configure cómo se mostrará la interfaz de la aplicación:
  - **Con la interfaz simplificada.** La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un [icono en el área de notificación de Windows](#). El usuario podrá [interactuar con Kaspersky Endpoint Security en forma limitada](#) a través del menú contextual de este icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
  - **Con la interfaz completa.** En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al [icono ubicado en el área de notificaciones de Windows](#). El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
  - **Sin interfaz.** No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El [icono del área de notificación de Windows](#) no estará disponible y tampoco se mostrará ninguna notificación.
6. Guarde los cambios.

## Primeros pasos

Una vez que se complete la implementación de Kaspersky Endpoint Security en los equipos cliente, deberá realizar las siguientes tareas para poder trabajar con la aplicación desde Kaspersky Security Center Web Console:

- Crear y configurar una directiva.  
Puede usar directivas para aplicar parámetros de Kaspersky Endpoint Security idénticos a todos los equipos cliente de un grupo de administración. El Asistente de inicio rápido de Kaspersky Security Center crea una directiva para Kaspersky Endpoint Security automáticamente.
- Crear las tareas *Actualización* y *Análisis antivirus*.  
La tarea *Actualización* permite que los equipos siempre cuenten con lo último en protección. Cuando se ejecuta esta tarea, Kaspersky Endpoint Security [actualiza sus bases de datos antivirus y sus módulos de software](#). La tarea *Actualización* se crea automáticamente al usar el Asistente de inicio rápido de Kaspersky Security Center. Para crear la tarea *Actualización*, instale el complemento web de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.  
La tarea *Análisis antivirus* se requiere para detectar virus y otras clases de malware a tiempo. La tarea *Análisis antivirus* se debe crear manualmente.

[Cómo crear una tarea de análisis antivirus en la Consola de administración \(MMC\)](#) 

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

## Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)** → **Análisis antivirus**.

## Paso 2. Cobertura del análisis

Crear la lista de objetos que Kaspersky Endpoint Security analizará mientras realiza una tarea de análisis.

## Paso 3. Acción de Kaspersky Endpoint Security

Seleccione la acción al detectar una amenaza:

- **Desinfectar; eliminar si la desinfección falla.** Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
- **Desinfectar; informar si falla la desinfección.** Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección no es posible, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.
- **Informar.** Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.
- **Ejecutar la desinfección avanzada de inmediato.** Cuando esta casilla está activada, Kaspersky Endpoint Security utiliza la tecnología de desinfección avanzada para tratar las amenazas activas durante el análisis.

El objetivo de *la tecnología de desinfección avanzada* consiste en eliminar del sistema operativo las aplicaciones maliciosas que ya han puesto en marcha sus procesos en la memoria RAM y que impiden que Kaspersky Endpoint Security las elimine por medio de otros métodos. Como consecuencia de ello, se neutraliza la amenaza. Cuando la desinfección avanzada está en curso, se recomienda que no ponga en marcha ningún proceso nuevo ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada emplea un número considerable de recursos del sistema operativo, lo que puede ralentizar el resto de las aplicaciones. Cuando se haya completado la desinfección avanzada, Kaspersky Endpoint Security reiniciará el equipo sin solicitar la confirmación del usuario.

Configure el modo de ejecución de la tarea con la casilla **Ejecutar solo cuando el equipo está inactivo**. Esta casilla activa o desactiva la función que suspende la tarea *Análisis antivirus* cuando los recursos del equipo son limitados. Kaspersky Endpoint Security pone en pausa la tarea *Análisis antivirus* cuando el salvapantallas está apagado y el equipo está desbloqueado.

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

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

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

### Paso 5. Selección de la cuenta para ejecutar la tarea

Seleccione una cuenta para ejecutar la tarea *Análisis antivirus*. De forma predeterminada, Kaspersky Endpoint Security inicia la tarea con los derechos de una cuenta de usuario local. Si la cobertura del análisis incluye unidades de red u otros objetos con acceso restringido, seleccione una cuenta de usuario con los derechos de acceso suficientes.

### Paso 6. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o después de descargar bases de datos antivirus al repositorio.

### Paso 7. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Análisis completo diario*.

### Paso 8. Conclusión de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, la tarea de análisis de virus se ejecutará en los equipos de usuario según la planificación especificada.

[Cómo crear una tarea de análisis antivirus en Web Console](#) 



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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

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

c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Análisis semanal*).

d. En la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Salga del Asistente.

La nueva tarea aparecerá en la lista de tareas.

6. Para configurar la planificación de la tarea, abra las propiedades de la tarea.

Se recomienda programar la tarea para que se ejecute al menos una vez por semana.

7. Active la casilla ubicada junto a la tarea.

8. Haga clic en el botón **Ejecutar**.

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 virus se ejecutará en los equipos de usuario según la planificación especificada.

## Gestión de directivas

Una *directiva* es un grupo de valores de configuración que se han definido para una aplicación y un grupo de administración específicos. Es posible configurar más de una directiva, cada una con valores distintos, para una misma aplicación. La aplicación puede funcionar con configuraciones distintas asociadas a grupos de administración distintos. Cada grupo puede tener su propia directiva para una aplicación.

La configuración de una directiva se envía a los equipos cliente a través del Agente de red durante la *sincronización*. De manera predeterminada, el Servidor de administración ejecuta el proceso de sincronización en cuanto se modifica una directiva. El puerto UDP 15000 en el equipo cliente se usa para la sincronización. El Servidor de administración realiza una sincronización cada 15 minutos de forma predeterminada. Si la sincronización falla después de cambiar la configuración de la directiva, el siguiente intento de sincronización se realizará según la planificación configurada.

## Directivas activa e inactiva

Una directiva está destinada a un grupo de equipos administrados y puede estar activa o inactiva. 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.



El número de directivas inactivas que pueden crearse es ilimitado. Estas no afectan la configuración de las aplicaciones instaladas en los equipos de la red. Están pensadas para usarse en situaciones de emergencia, como brotes de virus y otros casos. Por ejemplo, ante un ataque mediante unidades flash, puede activarse una directiva que impida el uso de unidades flash. En tal caso, la directiva activa cambia de estado a inactiva automáticamente.

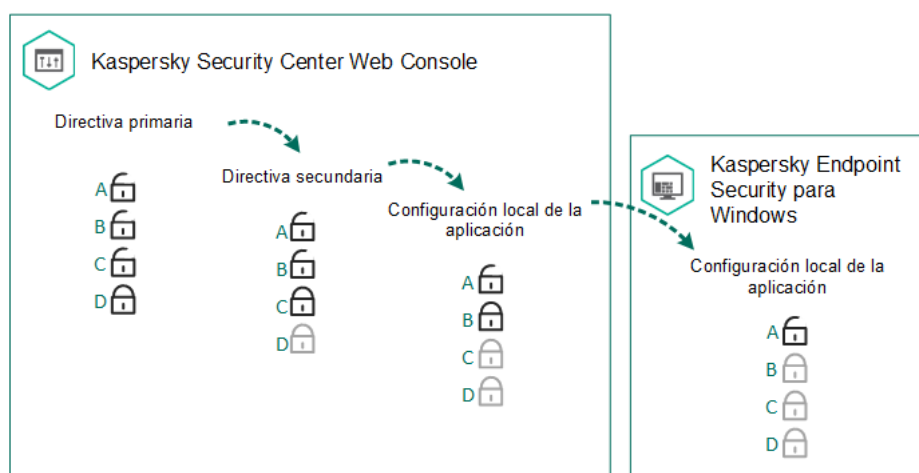
## Directiva fuera de la oficina

La directiva fuera de la oficina entra en vigor cuando un equipo abandona el perímetro de la red de la organización.

## Herencia de configuración

Las directivas, como los grupos de administración, se organizan en una jerarquía. De forma predeterminada, una directiva secundaria hereda la configuración de la directiva principal. La *directiva secundaria* es una directiva para niveles de jerarquía anidados, que es una directiva para grupos de administración anidados y servidores de administración secundarios. Puede deshabilitar la herencia de la configuración de la directiva principal.

Cada configuración de directiva tiene el atributo  que indica si esta configuración se puede modificar en las directivas secundarias o en la [configuración de la aplicación local](#). El  atributo solo se aplica si la herencia de la configuración de la directiva principal está habilitada para la directiva secundaria. Este tipo de directiva no afecta a las que se han creado para grupos de administración de otros niveles de la jerarquía.



Herencia de configuración




Los derechos de acceso a la configuración de las directivas (lectura, escritura, ejecución) se especifican para cada usuario que tenga acceso al servidor de administración de Kaspersky Security Center y, por separado, para cada cobertura funcional de Kaspersky Endpoint Security. Para configurar los derechos de acceso a la configuración de las directivas, vaya a la sección **Seguridad** de la ventana de propiedades del servidor de administración de Kaspersky Security Center.


## Creación de una directiva

[Cómo crear una directiva en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, seleccione la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Haga clic en el botón **Nueva directiva**.  
El Asistente de directivas se inicia.
5. Siga las instrucciones del Asistente de directivas.

[Cómo crear una directiva en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el botón **Añadir**.  
El Asistente de directivas se inicia.
3. Seleccione Kaspersky Endpoint Security y haga clic en **Siguiente**.
4. Lea y acepte los términos de la Declaración de Kaspersky Security Network (KSN) y haga clic en **Siguiente**.
5. En la pestaña **General**, puede realizar las siguientes acciones:
  - Cambiar el nombre de la directiva.
  - Seleccionar el estado de la directiva:
    - **Activa**. Después de la siguiente sincronización, la directiva se utilizará como directiva activa en el equipo.
    - **Inactiva**. Directiva de reserva. Puede convertirse en la directiva activa cuando resulta necesario.
    - **Fuera de la oficina**. La directiva se activa cuando un equipo abandona el perímetro de la red de la organización.
  - Configurar la herencia de configuración:
    - **Heredar configuración de la directiva 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 la configuración en las directivas secundarias**. Si el botón de alternancia está activado, los valores de la configuración de directiva se propagan a las directivas secundarias. En las propiedades de la directiva secundaria, el botón para **Heredar configuración de la directiva primaria** se activará automáticamente y no se podrá desactivar. La configuración de directiva secundaria se hereda de la directiva primaria, excepto para los ajustes marcados con . Los ajustes de la directiva secundaria no se pueden modificar si  está configurado para la directiva principal.
6. En la pestaña **Configuración de la aplicación**, puede modificar [la configuración de la directiva de Kaspersky Endpoint Security](#).
7. Guarde los cambios.

La configuración de Kaspersky Endpoint Security se aplicará en los equipos cliente cuando se realice la siguiente sincronización. Puede ver información sobre la directiva que se aplica al equipo en la interfaz de Kaspersky Endpoint Security haciendo clic en el botón  en la pantalla principal (por ejemplo, el nombre de la directiva). Para hacerlo, en la configuración de la directiva del Agente de red, tiene que activar la recepción de datos de directiva ampliados. Para obtener más información sobre una directiva del Agente de red, consulte la [Ayuda de Kaspersky Security Center](#).

## Indicador de nivel de seguridad

El indicador de nivel de seguridad se muestra en la parte superior de la ventana **Propiedades: <Nombre de directiva>**. El indicador puede tener uno de estos valores:

- **Nivel de protección alto.** El indicador toma este valor y se pone verde si todos los componentes de las siguientes categorías están activados:
  - **Crítico.** Esta categoría incluye los componentes siguientes:
    - Protección frente a amenazas en archivos.
    - Detección de comportamiento.
    - Prevención de vulnerabilidades.
    - Motor de reparación.
  - **Importante.** Esta categoría incluye los componentes siguientes:
    - Kaspersky Security Network.
    - Protección frente a amenazas web.
    - Protección frente a amenazas en el correo.
    - Prevención de intrusiones en el host.
- **Nivel de protección medio.** El indicador toma este valor y se pone amarillo si uno de los componentes de importantes está desactivado.
- **Nivel de protección bajo.** El indicador toma este valor y se pone rojo en uno de los casos siguientes:
  - Un componente crítico (o varios) está(n) desactivado(s).
  - Dos componentes importantes (o más) están desactivados.

Si el indicador tiene el valor **Nivel de protección medio** o **Nivel de protección bajo**, a la derecha del indicador aparece un enlace, que abre la ventana **Componentes de protección recomendados**. En esta ventana puede activar cualquiera de los componentes de protección recomendados.

## Gestión de tareas

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

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

Puede crear cualquier cantidad de tareas de grupo, tareas para una selección de equipos o tareas locales. Para más información sobre cómo trabajar con grupos de administración y selecciones de equipos, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Kaspersky Endpoint Security admite las siguientes tareas:

- **Análisis antivirus.** Kaspersky Endpoint Security analiza las áreas del equipo que se han especificado en la configuración de tareas para virus y otras amenazas. La tarea *Análisis antivirus*, necesaria para usar Kaspersky

Endpoint Security, se crea al utilizar el Asistente de inicio rápido. Se recomienda [programar la tarea para que se ejecute](#) al menos una vez por semana.

- **[Añadir clave](#)**. Kaspersky Endpoint Security añade una clave que le permite activarse, así como una clave adicional. Antes de ejecutar la tarea, asegúrese de que el número de equipos en los que la tarea vaya a ejecutarse no supere el número permitido por la licencia.
- **[Cambiar componentes de la aplicación](#)**. Kaspersky Endpoint Security instala o elimina componentes en equipos cliente según la lista de componentes especificados en la configuración de la tarea. El componente Protección frente a amenazas en archivos no puede eliminarse. La óptima elección de componentes de Kaspersky Endpoint Security ayuda a hacer un buen uso de los recursos del equipo.
- **[Inventario](#)**. Kaspersky Endpoint Security recibe información sobre todos los archivos ejecutables de aplicaciones almacenados en los equipos. La tarea *Inventario* se ejecuta usando el componente Control de aplicaciones. Si Control de aplicaciones no está instalado, la tarea finaliza con un error.
- **[Actualización](#)**. Kaspersky Endpoint Security actualiza sus bases de datos y módulos. La tarea *Actualización*, necesaria para usar Kaspersky Endpoint Security, se crea al utilizar el Asistente de inicio rápido. Recomendamos definir una planificación para que la tarea se ejecute al menos una vez al día.
- **[Eliminación de datos](#)**. Kaspersky Endpoint Security elimina archivos y carpetas de los equipos de los usuarios en forma inmediata o cuando no ha habido conexión con Kaspersky Security Center en mucho tiempo.
- **[Revertir actualización](#)**. Kaspersky Endpoint Security revierte la última actualización de sus bases de datos y módulos. Esto puede ser necesario, por ejemplo, cuando las bases de datos nuevas contienen datos incorrectos y Kaspersky Endpoint Security bloquea una aplicación segura en consecuencia.
- **[Comprobación de integridad](#)**. Kaspersky Endpoint Security analiza los archivos que forman parte de la aplicación, comprueba si tienen daños o modificaciones y verifica sus firmas digitales.
- **[Administrar cuentas del Agente de autenticación](#)**. Kaspersky Endpoint Security configura los ajustes de la cuenta del Agente de autenticación. Se necesita un Agente de autenticación para trabajar con unidades cifradas. Antes de que se cargue el sistema operativo, el usuario debe completar la autenticación con el Agente.

Las tareas se ejecutarán en un equipo únicamente si [Kaspersky Endpoint Security está en funcionamiento](#).

## Añadir una nueva tarea

### [Cómo crear una tarea en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. Seleccione la carpeta **Tareas** en el árbol de la consola de administración.
3. Haga clic en el botón **Nueva tarea**.  
El Asistente de tareas comienza.
4. Siga las instrucciones del Asistente de tareas.

### [Cómo crear una tarea en Web Console y Cloud Console](#)

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

b. En la lista desplegable **Tipo de tarea**, seleccione el tipo de tarea que desea ejecutar en los equipos de los usuarios.

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

d. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.

5. Salga del Asistente.

La nueva tarea aparecerá en la lista de tareas. La tarea tendrá la configuración predeterminada. Para modificar la configuración, abra las propiedades de la tarea. Para ejecutar una tarea, active la casilla a su lado y haga clic en el botón **Iniciar**. Una vez iniciada la tarea, puede suspenderla y reanudarla más tarde.

Puede utilizar la lista de tareas para llevar un control de sus resultados, ver el estado en que se encuentran, acceder a estadísticas sobre las tareas que se han ejecutado en los equipos y más. Para el mismo fin puede crear una selección de eventos (**Control e informes** → **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](#).

## Control de acceso a tareas

Los derechos de acceso a las tareas de Kaspersky Endpoint Security (lectura, escritura, ejecución) se especifican para cada usuario que tenga acceso al Servidor de administración de Kaspersky Security Center a través de la configuración del acceso a las áreas funcionales de Kaspersky Endpoint Security. Para configurar el acceso a las áreas funcionales de Kaspersky Endpoint Security, vaya a la sección **Seguridad** de la ventana de propiedades del servidor de administración de Kaspersky Security Center. Para obtener más información sobre la gestión de tareas a través de Kaspersky Security Center, consulte la [Guía de ayuda de Kaspersky Security Center](#).

Puede configurar los derechos de los usuarios para acceder a las tareas utilizando una directiva (*modo de gestión de tareas*). Por ejemplo, puede ocultar tareas de grupo en la interfaz de Kaspersky Endpoint Security.

[Cómo configurar el modo de gestión de tareas en la interfaz de Kaspersky Endpoint Security a través de la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Tareas locales** → **Gestión de tareas**.
6. Configure el modo de administración de tareas (consulte la tabla a continuación).
7. Guarde los cambios.

### [Cómo configurar el modo de gestión de tareas en la interfaz de Kaspersky Endpoint Security a través de Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Tareas locales** → **Gestión de tareas**.
5. Configure el modo de administración de tareas (consulte la tabla a continuación).
6. Guarde los cambios.

#### Parámetros de gestión de tareas

Parámetro	Descripción
<b>Permitir el uso de las tareas locales</b>	<p>Si se selecciona la casilla de verificación, se muestran tareas locales en la interfaz local de Kaspersky Endpoint Security. Cuando no existen restricciones adicionales de directivas, el usuario puede configurar y ejecutar tareas. Sin embargo, el usuario no puede programar la configuración y la ejecución de las tareas. El usuario puede ejecutar tareas solo manualmente.</p> <p>Si la casilla de verificación se desactiva, el uso de tareas locales se detiene. De este modo, las tareas locales no se ejecutan según la planificación. Las tareas no se pueden iniciar ni configurar en la interfaz local de Kaspersky Endpoint Security, ni con la línea de comandos.</p> <p>Aun así, un usuario puede iniciar un análisis antivirus de un archivo o carpeta seleccionando la opción <b>Buscar virus</b> en el menú contextual del archivo o la carpeta. La tarea de análisis se inicia con los valores de configuración predeterminados de la tarea de análisis personalizado.</p>
<b>Permitir que las tareas de grupo se muestren</b>	<p>Si se selecciona la casilla de verificación, se muestran tareas de grupo en la interfaz local de Kaspersky Endpoint Security. El usuario puede ver la lista de todas las tareas en la interfaz de la aplicación.</p> <p>Si se desactiva la casilla de verificación, Kaspersky Endpoint Security muestra una lista de tareas vacía.</p>




### Permitir gestión de tareas de grupo

Si se selecciona, los usuarios pueden iniciar y detener las tareas de grupo especificadas en Kaspersky Security Center. Los usuarios pueden iniciar y detener las tareas en la interfaz de la aplicación o en la interfaz de la aplicación simplificada.

Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no inicia las tareas planificadas automáticamente, o el administrador inicia las tareas manualmente en Kaspersky Security Center.

## Configuración de los ajustes locales de la aplicación

En Kaspersky Security Center, puede configurar los ajustes de Kaspersky Endpoint Security en un equipo determinado. Tales parámetros se denominan *configuración local de la aplicación*. No siempre es posible modificar todos los parámetros. Los parámetros que no pueden modificarse tienen el atributo de bloqueo  en las [propiedades de la directiva](#).

### [Cómo configurar los ajustes locales de la aplicación en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el equipo para el que desee configurar los ajustes de Kaspersky Endpoint Security.
5. En el menú contextual del equipo cliente, seleccione **Propiedades**.  
Se abre una ventana de propiedades del equipo cliente.
6. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.  
Aparecerá una lista de las aplicaciones de Kaspersky que se han instalado en el equipo cliente en la parte derecha de la ventana de propiedades del equipo cliente.
7. Seleccione Kaspersky Endpoint Security.
8. Haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.  
Esto abre la ventana **Configuración de la aplicación de Kaspersky Endpoint Security para Windows**.
9. En la sección **Configuración general**, configure Kaspersky Endpoint Security, además de Informes y Almacenes.  
Las demás secciones de la ventana **Configuración de la aplicación Kaspersky Endpoint Security para Windows** son las mismas que las de las secciones estándar de Kaspersky Security Center. Se ofrece una descripción de estas secciones en la ayuda de Kaspersky Security Center.

Si una aplicación está sujeta a una directiva que prohíbe cambiar parámetros específicos, no podrá modificarlos al configurar los parámetros de la aplicación en la sección **Configuración general**.

10. Guarde los cambios.

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
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 pestaña **Configuración de la aplicación**.
6. Haga los cambios que necesite en la configuración local de la aplicación.
7. Los ajustes locales de la aplicación son los mismos que los de la [directiva](#), excepto los ajustes de cifrado.

## Inicio y detención de Kaspersky Endpoint Security

Cuando termina de instalarse en el equipo de un usuario, Kaspersky Endpoint Security se abre automáticamente. De forma predeterminada, Kaspersky Endpoint Security se inicia después del inicio del sistema operativo. No se puede configurar el inicio automático de la aplicación en la configuración del sistema operativo.

La descarga de las bases de datos de Kaspersky Endpoint Security después de que se inicie el sistema operativo puede requerir hasta dos minutos según la capacidad del equipo. Durante este período, el nivel de protección del equipo se reduce. Cuando Kaspersky Endpoint Security se inicia en un sistema operativo que ya está en funcionamiento, descargar las bases de datos no afecta el nivel de protección.


## [Cómo configurar el inicio de Kaspersky Endpoint Security en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de la aplicación**.
6. Use la casilla **Ejecutar Kaspersky Endpoint Security para Windows al iniciarse el equipo** para configurar el inicio de la aplicación.
7. Guarde los cambios.

## Cómo configurar el inicio de Kaspersky Endpoint Security en Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Configuración de la aplicación**.
5. Use la casilla **Ejecutar Kaspersky Endpoint Security al iniciarse el equipo** para configurar el inicio de la aplicación.
6. Guarde los cambios.



## Cómo configurar el inicio de Kaspersky Endpoint Security en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. Use la casilla **Ejecutar Kaspersky Endpoint Security para Windows al iniciarse el equipo** para configurar el inicio de la aplicación.
4. Guarde los cambios.

Los expertos de Kaspersky no recomiendan detener manualmente Kaspersky Endpoint Security ya que, de hacerlo, el equipo y sus datos personales quedan expuestos a amenazas. Si fuera necesario, puede [suspender la protección del equipo](#) durante el tiempo que necesite, sin detener la aplicación.

Puede controlar el estado de la aplicación utilizando el widget **Estado de la protección**.

## Cómo iniciar o detener Kaspersky Endpoint Security en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el equipo en el que desee ejecutar o detener la aplicación.
5. Haga clic con el botón derecho del ratón para que aparezca el menú contextual del equipo cliente y seleccione **Propiedades**.
6. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.  
Aparecerá una lista de las aplicaciones de Kaspersky que se han instalado en el equipo cliente en la parte derecha de la ventana de propiedades del equipo cliente.
7. Seleccione Kaspersky Endpoint Security.
8. Haga lo siguiente:
  - Para iniciar la aplicación, haga clic en el botón  situado a la derecha de la lista de aplicaciones de Kaspersky.
  - Para detener la aplicación, haga clic en el botón  situado a la derecha de la lista de aplicaciones de Kaspersky.

### [Cómo iniciar o detener Kaspersky Endpoint Security en Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
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](#)

Para que la aplicación se pueda detener desde la línea de comandos, [active la administración externa de los servicios del sistema](#).



El archivo klpsm.exe, incluido en el kit de distribución de Kaspersky Endpoint Security, se usa para iniciar o detener la aplicación desde la línea de comandos.

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para iniciar la aplicación desde la línea de comandos, introduzca `klpsm.exe start_avp_service`.
4. Para detener la aplicación desde la línea de comandos, introduzca `klpsm.exe stop_avp_service`.

## Suspensión y reanudación de Protección y control del equipo

La suspensión de la protección y el control del equipo implica la desactivación de todos los componentes de protección y control de Kaspersky Endpoint Security durante un tiempo.

El estado de la aplicación se muestra mediante el [icono de la aplicación en el área de notificaciones de la barra de tareas](#).

- El icono  indica que Protección y control del equipo se ha suspendido.
- El icono  indica que Protección y control del equipo están activados.

La suspensión o reanudación de Protección y control del equipo no afecta a las tareas de análisis o actualización.

Si se establece alguna conexión de red al mismo tiempo que suspende o reanuda Protección y control del equipo, se muestra una notificación para indicar la finalización de dichas conexiones de red.

*Para pausar Protección y control del equipo:*

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

2. En el menú contextual, seleccione **Pausar la protección** (vea la figura a continuación).

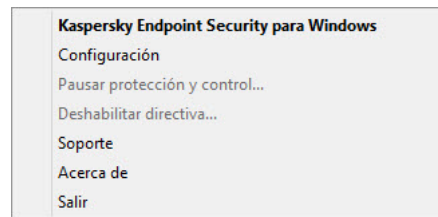
Este elemento del menú contextual está disponible si la [protección con contraseña está habilitada](#).

3. Seleccione una de las siguientes opciones:

- **Pausar durante <time period>**: la protección y el control del equipo se reanudarán una vez que haya transcurrido la cantidad de tiempo especificada en la siguiente lista desplegable.
- **Pausar hasta el reinicio de la aplicación**: la protección y el control del equipo se reanudarán después de reiniciar la aplicación o el sistema operativo. Debe activarse el inicio automático de la aplicación para utilizar esta opción.
- **Suspender**: protección y control del equipo se reanudará cuando decida volver a activarlo.

#### 4. Haga clic en el botón **Pausar la protección**.

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



Menú contextual del icono de la aplicación

*Para reanudar Protección y control del equipo:*

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En el menú contextual, seleccione **Reanudar la protección**.


Puede reanudar la protección y el control del equipo en cualquier momento, independientemente de la opción de suspensión de protección y control del equipo que haya seleccionado anteriormente.

## Crear y utilizar un archivo de configuración

Un archivo de configuración con los ajustes de Kaspersky Endpoint Security le permite llevar a cabo las tareas siguientes:

- Realice la instalación local de Kaspersky Endpoint Security mediante la línea de comandos con la configuración predefinida.  
Para ello, debe guardar el archivo de configuración en la misma carpeta donde se ubica el paquete de distribución.
- Realice la instalación remota de Kaspersky Endpoint Security mediante Kaspersky Security Center con la configuración predefinida.
- Migre la configuración de Kaspersky Endpoint Security de un equipo a otro.


*Para crear un archivo de configuración:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Administrar parámetros**.
3. Haga clic en el botón **Exportar**.
4. En la ventana que se abre, especifique la ruta en la cual desea guardar el archivo de configuración e introduzca su nombre.

Si desea usar el archivo de configuración para la instalación local o remota de Kaspersky Endpoint Security, lo debe denominar install.cfg.

5. Guarde el archivo.

*Para importar la configuración de Kaspersky Endpoint Security desde un archivo de configuración:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Administrar parámetros**.
3. Haga clic en el botón **Importar**.
4. En la ventana que se abre, introduzca la ruta del archivo de configuración.
5. Abra el archivo.

Todos los valores de la configuración de Kaspersky Endpoint Security se definirán según el archivo de configuración seleccionado.

## Restaurar la configuración predeterminada de la aplicación

Puede restaurar la configuración recomendada por Kaspersky para Endpoint Security en cualquier momento. Cuando se restablece la configuración, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección.

*Para restaurar la configuración predeterminada de la aplicación:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Administrar parámetros**.
3. Haga clic en el botón **Restaurar**.
4. Guarde los cambios.

## Análisis antivirus del equipo

Un análisis antivirus es fundamental para la seguridad del equipo. Realice análisis antivirus de forma periódica para ayudar a descartar la posibilidad de que se extienda el software malicioso (malware) que los componentes de protección no han detectado debido a una configuración de nivel de seguridad baja o a otros motivos.

Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive, y crea entradas de registro que indican que estos archivos no se han analizado.

### Análisis completo

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

- Memoria del núcleo;
- Objetos cargados en el inicio del sistema operativo
- Sectores de arranque;
- Copia de seguridad del sistema operativo
- Todas las unidades de disco duro y unidades extraíbles

Los expertos de Kaspersky recomiendan que no cambie 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 una tarea de análisis completo. El nivel de seguridad del equipo no se verá afectado.

### Análisis de áreas críticas

De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.

Los expertos de Kaspersky recomiendan que no cambie el alcance del análisis de la tarea *Análisis de áreas críticas*.

### Análisis personalizado

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

- Memoria del sistema
- Objetos cargados en el inicio del sistema operativo
- Copia de seguridad del sistema operativo



- Buzón de correo de Microsoft Outlook
- Unidades de disco duro, unidades extraíbles y unidades de red
- Cualquier archivo seleccionado

## Análisis en segundo plano

El *análisis en segundo plano* es uno de los modos de análisis disponibles en Kaspersky Endpoint Security. Cuando se realiza un análisis de este tipo, la aplicación no le muestra ninguna notificación al usuario. En comparación con otros tipos de análisis, como el análisis completo, un análisis en segundo plano tiene menos impacto en los recursos del equipo. En este modo, Kaspersky Endpoint Security analiza los objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema.

## Comprobación de integridad

Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en busca de datos corruptos o modificaciones.

## Análisis del equipo

Un análisis antivirus es fundamental para la seguridad del equipo. Realice análisis antivirus de forma periódica para ayudar a descartar la posibilidad de que se extienda el software malicioso (malware) que los componentes de protección no han detectado debido a una configuración de nivel de seguridad baja o a otros motivos. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

Kaspersky Endpoint Security tiene tareas estándar *Análisis completo*, *Análisis de áreas críticas*, *Análisis personalizado* predefinidas. Si su organización tiene el sistema de administración de Kaspersky Security Center desplegado, puede [crear una tarea de Análisis antivirus](#) y configurar el análisis. La tarea de [Análisis en segundo plano](#) también está disponible en Kaspersky Security Center. No se puede configurar el análisis en segundo plano.

[Cómo ejecutar un análisis antivirus en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Tareas**.
4. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.  
Si es necesario, [cree una tarea de Análisis antivirus](#).
5. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
6. Configure la tarea de análisis (consulte la tabla a continuación).  
Si necesario, [configure la programación de la tarea de análisis](#).
7. Guarde los cambios.
8. Ejecutar la tarea de análisis.


Kaspersky Endpoint Security comenzará a escanear el equipo. Si el usuario ha interrumpido la ejecución de la tarea (por ejemplo, al apagar el equipo), Kaspersky Endpoint Security ejecuta automáticamente la tarea, continuando desde el punto donde se interrumpió el análisis.

### [Cómo ejecutar un análisis antivirus en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea de análisis.  
Se abre la ventana propiedades de la tarea.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Configure la tarea de análisis (consulte la tabla a continuación).  
Si necesario, [configure la programación de la tarea de análisis](#).
5. Guarde los cambios.
6. Ejecutar la tarea de análisis.

Kaspersky Endpoint Security comenzará a escanear el equipo. Si el usuario ha interrumpido la ejecución de la tarea (por ejemplo, al apagar el equipo), Kaspersky Endpoint Security ejecuta automáticamente la tarea, continuando desde el punto donde se interrumpió el análisis.

### [Cómo ejecutar un análisis antivirus 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 (consulte la tabla a continuación).  
Si necesario, [configure la programación de la tarea de análisis](#).
4. Guarde los cambios.
5. Ejecutar la tarea de análisis.

Kaspersky Endpoint Security comenzará a escanear el equipo. La aplicación mostrará el progreso del análisis, la cantidad de archivos analizados y el tiempo de análisis restante. Puede detener la tarea en cualquier momento haciendo clic en el botón **Detener**. Si no se muestra la tarea de análisis, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

#### Configuración del análisis

Parámetro	Descripción
<b>Nivel de seguridad</b>	<p>Kaspersky Endpoint Security puede usar diferentes grupos de parámetros para ejecutar un análisis. Estos grupos de parámetros guardados en la aplicación se denominan <i>niveles de seguridad</i>.</p> <ul style="list-style-type: none"> <li>• <b>Máximo.</b> Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, Kaspersky Endpoint Security también analiza archivos en formato de correo electrónico.</li> <li>• <b>Recomendado.</b> Kaspersky Endpoint Security analiza únicamente los formatos de archivo especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo, así como objetos OLE incrustados. Kaspersky Endpoint Security no analiza archivos o paquetes de instalación.</li> <li>• <b>Mínimo.</b> Kaspersky Endpoint Security únicamente analiza archivos nuevos o modificados con las extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. Kaspersky Endpoint Security no analiza archivos compuestos.</li> </ul> <p>Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración recomendada del nivel de seguridad.</p>
<b>Acción al detectar una amenaza</b>	<p><b>Desinfectar; eliminar si la desinfección falla.</b> Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.</p> <p><b>Desinfectar; bloquear si falla la desinfección.</b> Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección no es posible, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.</p> <p><b>Notificar.</b> Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Antes de intentar desinfectar o eliminar un archivo infectado, Kaspersky Endpoint Security crea una copia de seguridad del archivo en caso de que necesite <a href="#">restaurarlo o que sea posible desinfectarlo en el futuro</a>.</p> </div>

	<p>Al detectar archivos infectados que son parte de la aplicación Windows Store, Kaspersky Endpoint Security intenta eliminar los archivos.</p>
<p><b>Ejecutar la desinfección avanzada de inmediato</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Se realiza una desinfección avanzada durante una tarea de análisis antivirus en un equipo solo si la <a href="#">característica Desinfección avanzada está activada</a> en las propiedades de la directiva aplicada a este equipo.</p> <p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security desinfecta la infección activa inmediatamente después de que se detecta durante la ejecución de la tarea de análisis antivirus. Una vez que se desinfecta la infección activa, Kaspersky Endpoint Security reinicia el equipo sin preguntarle al usuario.</p> <p>Si la casilla de verificación está desactivada, Kaspersky Endpoint Security no desinfecta la infección activa inmediatamente después de que se detecta durante la ejecución de la tarea de análisis antivirus. Kaspersky Endpoint Security genera eventos de infección activos en informes de aplicaciones locales y en el lado de Kaspersky Security Center. La infección activa se puede desinfectar cuando se vuelve a ejecutar la tarea de análisis antivirus con la función Desinfección avanzada activada. De esta forma, el administrador del sistema puede elegir el momento adecuado para realizar la Desinfección avanzada y, posteriormente, reiniciar los equipos automáticamente.</p>
<p><b>Cobertura del análisis</b></p>	<p>Lista de objetos que Kaspersky Endpoint Security analiza mientras realiza una tarea de análisis. Los objetos dentro de la cobertura del análisis pueden ser la memoria del núcleo, los procesos en ejecución, los sectores de arranque, el almacenamiento de respaldo del sistema, las bases de datos de correo, las unidades de disco duro, las extraíbles o las de red, una carpeta o un archivo.</p>
<p><b>Planificación de análisis</b></p>	<p><b>Manual.</b> Modo de ejecución en el que puede comenzar a analizar manualmente en el momento que sea conveniente para usted.</p> <p><b>Según programación.</b> En este modo de ejecución de la tarea de análisis, Kaspersky Endpoint Security comienza el análisis en función de la planificación especificada. Si está seleccionado este modo de ejecución de la tarea de análisis, también puede iniciar la tarea de análisis manualmente.</p>
<p><b>Posponer la ejecución después del inicio de la aplicación durante N minutos</b></p>	<p>Inicio pospuesto de la tarea de análisis después del inicio de la aplicación. Dado que se ejecutan varios procesos al iniciar el sistema operativo, es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después del inicio de Kaspersky Endpoint Security.</p>
<p><b>Ejecutar tareas ignoradas</b></p>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security inicia la tarea de análisis omitida lo antes posible. La tarea de análisis se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programa de la tarea de actualización. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no inicia las tareas de análisis omitidas. En lugar de ello, lleva a cabo la siguiente tarea de análisis de acuerdo con la planificación actual.</p>
<p><b>Ejecutar solo cuando el equipo está inactivo</b></p>	<p>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 si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió.</p>
<p><b>Ejecutar el análisis como</b></p>	<p>Por defecto, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. La cobertura de la protección puede incluir unidades de</p>

	red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que tenga los permisos adecuados en la configuración de Kaspersky Endpoint Security y realizar la tarea de análisis con esta cuenta de usuario.
<b>Tipos de archivos</b>	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security considera los archivos sin extensión como ejecutables. Kaspersky Endpoint Security siempre analiza los archivos ejecutables independientemente de los tipos de archivo que seleccione para analizar.</p> </div> <p><b>Todos los archivos.</b> Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones).</p> <p><b>Archivos analizados por formato.</b> Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.</p> <p><b>Archivos analizados por extensión.</b> Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . El formato de archivo se determina en función de su extensión.</p> <p>De forma predeterminada, Kaspersky Endpoint Security analiza archivos según su formato. El análisis de archivos por extensión es menos seguro porque un archivo malicioso puede tener una extensión que no está en la lista de potencialmente infectable (por ejemplo, .123).</p>
<b>Analizar solamente archivos nuevos y modificados</b>	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
<b>Omitir los objetos analizados durante más de N segundos</b>	Limita la duración del análisis de un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.
<b>Analizar archivos</b>	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo.
<b>Analizar paquetes de distribución</b>	Use esta casilla para activar o desactivar el análisis de paquetes de distribución de terceros.
<b>Analizar archivos en formatos de Microsoft Office</b>	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.
<b>Analizar formatos de correo</b>	Análisis de archivos en formato de correo electrónico y la base de datos de correo electrónico. La aplicación analiza los archivos PST y OST utilizados por los clientes de correo MS Outlook y Windows Mail/Outlook Express, así como los archivos EML.

	<p>Kaspersky Endpoint Security no es compatible con la versión de 64 bits del cliente de correo electrónico MS Outlook. ThEsto significa que Kaspersky Endpoint Security no analiza los archivos de 64 bits de MS Outlook (archivos PST y OST) si hay una versión de 64 bits de MS Outlook instalada en el equipo, aunque <a href="#">el correo esté incluido en la cobertura del análisis</a>.</p> <p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security fracciona el archivo de formato de correo en sus componentes (encabezado, cuerpo y archivos adjuntos) y los analiza en busca de amenazas.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza el archivo de formato de correo como un único archivo.</p>
<b>Analizar archivos protegidos por contraseña</b>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analiza los archivos protegidos mediante contraseña. Antes de que se puedan analizar los archivos de un archivador, se le solicitará que introduzca la contraseña.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security omite el análisis de los archivos protegidos mediante contraseña.</p>
<b>No descomprimir archivos compuestos grandes</b>	<p>Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security no escanea archivos compuestos cuyo tamaño exceda el valor especificado.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.</p> <p>Kaspersky Endpoint Security analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.</p>
<b>Aprendizaje automático y análisis de firmas</b>	<p>El método de aprendizaje automático y análisis de firmas utiliza la base de datos de Kaspersky Endpoint Security, que contiene descripciones de las amenazas conocidas y métodos para erradicarlas. La protección que utiliza este método proporciona el nivel de seguridad mínimo aceptable.</p> <p>Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.</p>
<b>Análisis heurístico</b>	<p>La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.</p> <p>Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.</p>
<b>Tecnología iSwift</b>  <i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i>	<p>Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.</p>
<b>Tecnología</b>	<p>Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos</p>

## iChecker

*(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)*

archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

## Análisis de unidades extraíbles cuando se conectan al equipo

Kaspersky Endpoint Security analiza todos los archivos que ejecuta o copia, inclusive si el archivo está ubicado en una unidad extraíble (componente Protección frente a amenazas en archivos). A fin de evitar la propagación de virus u otro malware, puede configurar análisis automáticos de unidades extraíbles cuando estén conectadas al equipo. Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos. El componente mantiene seguro el equipo mediante la ejecución de análisis que implementan aprendizaje automático, análisis heurístico (nivel alto) y análisis de firma. Kaspersky Endpoint Security también utiliza las tecnologías de optimización de análisis iSwift e iChecker. Estas tecnologías están siempre activas y no se pueden desactivar.


### [Cómo configurar la ejecución del Análisis de unidades extraíbles en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Tareas locales** → **Análisis de unidades extraíbles**.
6. En la lista desplegable **Acción al conectar una unidad extraíble**, seleccione **Análisis detallado** o **Análisis rápido**.
7. Configure las opciones avanzadas para el análisis de unidades extraíbles (consulte la tabla a continuación).
8. Guarde los cambios.

### [Cómo configurar la ejecución del Análisis de unidades extraíbles en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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. Ir a **Tareas locales** → **Análisis de unidades extraíbles**.
5. En la lista desplegable **Acción al conectar una unidad extraíble**, seleccione **Análisis detallado** o **Análisis rápido**.
6. Configure las opciones avanzadas para el análisis de unidades extraíbles (consulte la tabla a continuación).
7. Guarde los cambios.

### Cómo configurar la ejecución del Análisis de unidades extraíbles en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en .
3. Utilice interruptor **Análisis de unidades extraíbles** para activar o desactivar el análisis de unidades extraíbles al conectarse al equipo.
4. Configure las opciones avanzadas para el análisis de unidades extraíbles (consulte la tabla a continuación).
5. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security ejecuta un análisis de unidades extraíbles para unidades extraíbles que no superen el tamaño máximo especificado. Si la tarea de *Análisis de unidades extraíbles* no se muestra, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

Configuración de los parámetros de análisis de unidades extraíbles

Parámetro	Descripción
<b>Acción al conectar una unidad extraíble</b>	<p><b>Análisis detallado.</b> Si se selecciona este elemento, después de que se conecta una unidad extraíble, Kaspersky Endpoint Security analiza todos los archivos en la unidad extraíble, incluidos los archivos dentro de objetos compuestos, archivos, paquetes de distribución y archivos en formatos de Office. Kaspersky Endpoint Security no analiza archivos en formatos de correo ni archivos protegidos con contraseña.</p> <p><b>Análisis rápido.</b> Si se selecciona esta opción, cuando se conecte una unidad extraíble, Kaspersky Endpoint Security analizará solo los <a href="#">archivos que sean de algunos formatos específicos</a>, por ser los más propensos a estar infectados. Los objetos compuestos no se desempaquetarán.</p>
<b>Tamaño máximo de la unidad extraíble</b>	<p>Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security lleva a cabo la acción seleccionada en la lista desplegable <b>Acción al conectar una unidad extraíble</b> sobre las unidades extraíbles con un tamaño no superior al tamaño máximo especificado para la unidad.</p> <p>Si la casilla de verificación está desactivada, Kaspersky Endpoint Security lleva a cabo la acción seleccionada en la lista desplegable <b>Acción al conectar una unidad extraíble</b> sobre unidades de cualquier tamaño.</p>



<b>Mostrar progreso del análisis</b>	<p>Si la casilla está seleccionada, Kaspersky Endpoint Security mostrará el progreso de los análisis de unidades extraíbles en la sección <b>Tareas</b> y en una ventana separada.</p> <p>Si la casilla no está seleccionada, Kaspersky Endpoint Security analizará las unidades extraíbles en segundo plano.</p>
<b>No permitir que se detenga la tarea de análisis</b>	<p>Si esta casilla está seleccionada, para la tarea de análisis de unidades extraíbles en la interfaz local de Kaspersky Endpoint Security, ni el botón <b>Detener</b> en la sección <b>Tareas</b> ni el botón <b>Detener</b> en la ventana de análisis de unidades extraíbles estarán disponibles.</p>

## Análisis en segundo plano

El *análisis en segundo plano* es uno de los modos de análisis disponibles en Kaspersky Endpoint Security. Cuando se realiza un análisis de este tipo, la aplicación no le muestra ninguna notificación al usuario. En comparación con otros tipos de análisis, como el análisis completo, un análisis en segundo plano tiene menos impacto en los recursos del equipo. En este modo, Kaspersky Endpoint Security analiza los objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema. La aplicación inicia un análisis en segundo plano en los siguientes casos:

- Las bases de datos antivirus se han actualizado hace poco.
- Kaspersky Endpoint Security se ha estado ejecutando por 30 minutos.
- Cada seis horas.
- Cuando el equipo está inactivo durante cinco minutos o más (el equipo está bloqueado o el protector de pantalla está encendido).

El análisis en segundo plano cuando el equipo está inactivo se interrumpe cuando se cumple alguna de las siguientes condiciones:

- El equipo entró en modo activo.

Si el análisis en segundo plano no se ha ejecutado desde hace más de diez días, el análisis no se interrumpe.

- El equipo (portátil) ha cambiado al modo batería.

Cuando se realiza un análisis en segundo plano, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.


[Cómo activar el análisis en segundo plano en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Tareas locales** → **Análisis en segundo plano**.
6. Utilice la casilla de verificación **Activar análisis en segundo plano** para activar o desactivar los análisis en segundo plano.
7. Guarde los cambios.

### [Cómo activar los análisis en segundo plano en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Tareas locales** → **Análisis en segundo plano**.
5. Utilice la casilla de verificación **Activar análisis en segundo plano** para activar o desactivar los análisis en segundo plano.
6. Guarde los cambios.

### [Cómo activar los análisis en segundo plano en la interfaz de la aplicación](#)

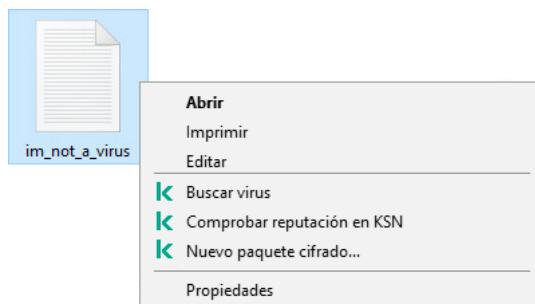
1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en .
3. Utilice el interruptor **Análisis en segundo plano** para activar o desactivar los análisis en segundo plano.
4. Guarde los cambios.

Si el *Análisis en segundo plano* no se muestra, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

## Analizar desde el menú contextual

Kaspersky Endpoint Security permite analizar archivos individuales en busca de virus y otras clases de malware desde el menú contextual (vea la siguiente imagen).

Cuando se realiza un análisis desde el menú contextual, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.



Analizar desde el menú contextual


### [Cómo configurar Analizar desde el menú contextual en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Tareas locales** → **Analizar desde el menú contextual**.
6. Configure Analizar desde el menú contextual (consulte la tabla a continuación).
7. Guarde los cambios.

### [Cómo configurar Analizar desde el menú contextual en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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. Ir a **Tareas locales** → **Analizar desde el menú contextual**.
5. Configure Analizar desde el menú contextual (consulte la tabla a continuación).
6. Guarde los cambios.



## Cómo configurar Analizar desde el menú contextual en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en .
3. Configure Analizar desde el menú contextual (consulte la tabla a continuación).
4. Guarde los cambios.

Si la tarea *Analizar desde el menú contextual* no se muestra, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

### Configuración de la tarea Analizar desde el menú contextual

Parámetro	Descripción
<b>Nivel de seguridad</b>	<p>Kaspersky Endpoint Security puede usar diferentes grupos de parámetros para ejecutar un análisis. Estos grupos de parámetros guardados en la aplicación se denominan <i>niveles de seguridad</i>.</p> <ul style="list-style-type: none"><li>• <b>Máximo.</b> Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, Kaspersky Endpoint Security también analiza archivos en formato de correo electrónico.</li><li>• <b>Recomendado.</b> Kaspersky Endpoint Security analiza únicamente los formatos de archivo especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo, así como objetos OLE incrustados. Kaspersky Endpoint Security no analiza archivos o paquetes de instalación.</li><li>• <b>Mínimo.</b> Kaspersky Endpoint Security únicamente analiza archivos nuevos o modificados con las extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. Kaspersky Endpoint Security no analiza archivos compuestos.</li></ul>
<b>Acción al detectar una amenaza</b>	<p><b>Desinfectar; eliminar si la desinfección falla.</b> Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.</p> <p><b>Desinfectar; bloquear si falla la desinfección.</b> Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección no es posible, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.</p> <p><b>Notificar.</b> Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.</p>
<b>Tipos de archivos</b>	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"><p>Kaspersky Endpoint Security considera los archivos sin extensión como ejecutables. Kaspersky Endpoint Security siempre analiza los archivos ejecutables independientemente de los tipos de archivo que seleccione para analizar.</p></div> <p><b>Todos los archivos.</b> Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones).</p>

	<p><b>Archivos analizados por formato.</b> Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.</p> <p><b>Archivos analizados por extensión.</b> Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . El formato de archivo se determina en función de su extensión.</p> <p>De forma predeterminada, Kaspersky Endpoint Security analiza archivos según su formato. El análisis de archivos por extensión es menos seguro porque un archivo malicioso puede tener una extensión que no está en la lista de potencialmente infectable (por ejemplo, .123).</p>
<b>Analizar solamente archivos nuevos y modificados</b>	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
<b>Omitir los objetos analizados durante más de N segundos</b>	Limita la duración del análisis de un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.
<b>Analizar archivos</b>	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo.
<b>Analizar paquetes de distribución</b>	La casilla de verificación activa o desactiva el análisis de los paquetes de distribución.
<b>Analizar archivos en formatos de Microsoft Office</b>	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.
<b>Analizar formatos de correo</b>	<p>Esta casilla de verificación activa o desactiva la opción para que Kaspersky Endpoint Security analice archivos con formato de correo electrónico y bases de datos de correo.</p> <p>La aplicación analiza completamente solo los formatos de archivo de correo de MS Outlook, Windows Mail/Outlook Express y EML, y solo si el equipo tiene el cliente de correo MS Outlook x86.</p> <p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security fracciona el archivo de formato de correo en sus componentes (encabezado, cuerpo y archivos adjuntos) y los analiza en busca de amenazas.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza el archivo de formato de correo como un único archivo.</p>
<b>Analizar archivos protegidos por contraseña</b>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analiza los archivos protegidos mediante contraseña. Antes de que se puedan analizar los archivos de un archivador, se le solicitará que introduzca la contraseña.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security omite el análisis de los archivos protegidos mediante contraseña.</p>
<b>No descomprimir archivos</b>	Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security no escanea archivos compuestos cuyo tamaño exceda el valor especificado.

<b>compuestos grandes</b>	<p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.</p> <p>Kaspersky Endpoint Security analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.</p>
<b>Aprendizaje automático y análisis de firmas</b>	<p>El método de aprendizaje automático y análisis de firmas utiliza la base de datos de Kaspersky Endpoint Security, que contiene descripciones de las amenazas conocidas y métodos para erradicarlas. La protección que utiliza este método proporciona el nivel de seguridad mínimo aceptable.</p> <p>Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.</p>
<b>Análisis heurístico</b>	<p>La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.</p> <p>Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.</p>
<b>Tecnología iSwift</b>	<p>Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.</p>
<b>Tecnología iChecker</b>	<p>Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).</p>

## Control de integridad de la aplicación

Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en busca de datos corruptos o modificaciones. Si detecta, por ejemplo, que una de las bibliotecas no tiene la firma digital correcta, considera que la biblioteca está dañada. Los archivos de la aplicación se analizan a través de la tarea *Comprobación de integridad*. Recomendamos que ejecute la tarea *Comprobación de integridad* si observa que Kaspersky Endpoint Security detecta, pero no neutraliza, un objeto malicioso.

Puede crear la tarea *Comprobación de integridad* en Kaspersky Security Center Web Console y en la Consola de administración. No se puede crear una tarea en Kaspersky Security Center Cloud Console.

Las siguientes situaciones pueden comprometer la integridad de la aplicación:

- Un objeto malicioso modifica los archivos de Kaspersky Endpoint Security. Ante esta situación, siga el procedimiento para restaurar Kaspersky Endpoint Security con las herramientas del sistema operativo. Cuando concluya la restauración, realice un análisis completo del equipo y ejecute nuevamente la comprobación de integridad.

- La firma digital llega a su fecha de caducidad. Ante esta situación, actualice Kaspersky Endpoint Security.

## [Cómo ejecutar una comprobación de integridad de aplicación mediante la Consola de administración \(MMC\)](#)

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)** → **Comprobación de integridad**.

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

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

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

### Paso 3. Configurar una planificación de inicio de tarea

Configure una planificación para iniciar una tarea, por ejemplo, manualmente o cuando se detecte un brote de virus.

### Paso 4. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Comprobación de integridad después de que se haya infectado el equipo*.

### Paso 5. Conclusión de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea. Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique de forma programada (consulte la tabla a continuación).

## [Cómo ejecutar una comprobación de integridad de aplicación mediante Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en el botón **Añadir**.  
El Asistente de tareas comienza.
3. Configure los parámetros de la tarea:
  - a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.
  - b. En la lista desplegable **Tipo de tarea**, seleccione **Comprobación de integridad**.
  - 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 la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.
5. Salga del Asistente.  
La nueva tarea aparecerá en la lista de tareas.
6. Active la casilla ubicada junto a la tarea.

Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique de forma programada (consulte la tabla a continuación).

### [Cómo ejecutar una comprobación de integridad en la interfaz de la aplicación](#) ?

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. Esto abre la lista de tareas; seleccione la tarea *Comprobación de integridad* y haga clic en **Ejecutar análisis**.

Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique de forma programada (consulte la tabla a continuación). Si la *Comprobación de integridad* no se muestra, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

Configuración de la tarea de Comprobación de integridad

Parámetro	Descripción
<b>Programación de análisis</b>	<p><b>Manual.</b> Modo de ejecución en el que puede comenzar a analizar manualmente en el momento que sea conveniente para usted.</p> <p><b>Según programación.</b> En este modo de ejecución de la tarea de análisis, Kaspersky Endpoint Security comienza el análisis en función de la planificación especificada. Si está seleccionado este modo de ejecución de la tarea de análisis, también puede iniciar la tarea de análisis manualmente.</p>
<b>Ejecutar las</b>	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security inicia la tarea de



<b>tareas omitidas</b>	análisis omitida lo antes posible. La tarea de análisis se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programa de la tarea de actualización. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no inicia las tareas de análisis omitidas. En lugar de ello, lleva a cabo la siguiente tarea de análisis de acuerdo con la planificación actual.
<b>Ejecutar solo cuando el equipo está inactivo</b>	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 si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió.

## Edición de la cobertura del análisis

La *Cobertura del análisis* es una lista de rutas a carpetas y rutas que Kaspersky Endpoint Security analiza al ejecutar la tarea. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.

Para editar la cobertura del análisis, recomendamos usar la tarea de *Análisis personalizado*. Los expertos de Kaspersky recomiendan que no cambie la cobertura del análisis de las tareas de *Análisis completo* y *Análisis de áreas críticas*.

Kaspersky Endpoint Security tiene los siguientes objetos predefinidos como parte de la cobertura del análisis:

- **Mi correo.**  
Archivos relevantes para el cliente de correo de Outlook: archivos de datos (PST), archivos de datos desconectados (OST).
- **Memoria del sistema.**
- **Objetos de arranque.**  
Memoria ocupada por procesos y archivos ejecutables de aplicaciones que se ejecutan al iniciar el sistema.
- **Sectores de arranque del disco.**  
Sectores de arranque del disco duro y del disco extraíble.
- **Copia de seguridad del sistema.**  
Contenido de la carpeta System Volume Information.
- **Todos los dispositivos externos.**
- **Todos los discos duros.**
- **Todas las unidades de red.**

Para excluir carpetas o archivos de la cobertura del análisis, [añada la carpeta o el archivo a la zona de confianza](#).

[Cómo editar una cobertura del análisis en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Tareas**.
4. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.  
Si es necesario, [cree una tarea de Análisis antivirus](#).
5. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
6. En la sección **Cobertura del análisis**, haga clic en **Configuración**.
7. En la ventana abierta, seleccione los objetos que desea añadir o excluir de la cobertura del análisis.
8. Si desea añadir un nuevo objeto a la cobertura del análisis:

- a. Haga clic en el botón **Añadir**.

- b. En el campo **Objeto**, introduzca la ruta a la carpeta o archivo.

Usar máscaras:

- El carácter **\*** (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\\*\\*.txt** incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
- Dos caracteres **\*\*** consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\Carpeta\\*\*\\*.txt** incluirá todas las rutas a archivos con la extensión TXT que se encuentren en la carpeta llamada **Carpeta** y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara **C:\\*\*\\*.txt** no es válida.
- El carácter **?** (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\Carpeta\???.txt** incluirá las rutas a todos los archivos de la carpeta llamada **Carpeta** que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura del análisis. Para hacerlo, desactive la casilla de verificación junto al objeto.

9. Guarde los cambios.

[Cómo editar una cobertura del análisis en Web Console y Cloud Console](#) 

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

Se abre la lista de tareas.

2. Haga clic en la tarea de análisis.

Se abre la ventana propiedades de la tarea. Si es necesario, [cree una tarea de Análisis antivirus](#).

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

4. En la sección **Cobertura del análisis**, seleccione los objetos que desea añadir o excluir de la cobertura del análisis.

5. Si desea añadir un nuevo objeto a la cobertura del análisis:

a. Haga clic en el botón **Añadir**.

b. En el campo **Ruta**, introduzca la ruta a la carpeta o archivo.

Usar máscaras:

- El carácter **\*** (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\\*\\*.txt** incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
- Dos caracteres **\*\*** consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\Carpeta\\*\*\\*.txt** incluirá todas las rutas a archivos con la extensión TXT que se encuentren en la carpeta llamada **Carpeta** y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara **C:\\*\*\\*.txt** no es válida.
- El carácter **?** (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\Carpeta\???.txt** incluirá las rutas a todos los archivos de la carpeta llamada **Carpeta** que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura del análisis. Para hacerlo, coloque el interruptor junto a él en la posición de apagado.

6. Guarde los cambios.

## [Cómo editar una cobertura del análisis en la interfaz de la aplicación](#)

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

2. En la lista de tareas, seleccione la tarea de *Análisis personalizado* y haga clic en **Seleccionar**.

También puede editar la cobertura del análisis para otras tareas. Los expertos de Kaspersky recomiendan que no cambie la cobertura del análisis de las tareas de *Análisis completo* y *Análisis de áreas críticas*.

3. En la ventana abierta, seleccione los objetos que desea añadir a la cobertura del análisis.

4. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

## Análisis programado en ejecución

El análisis completo del equipo requiere algo de tiempo y recursos del equipo. Debe elegir el momento óptimo para ejecutar un análisis de equipo para evitar afectar negativamente el rendimiento de otro software. Kaspersky Endpoint Security le permite configurar una planificación normal para analizar el equipo. Esto es conveniente si su organización tiene una planificación de trabajo. Puede configurar un análisis del equipo para que se ejecute por la noche o los fines de semana. Si no es posible iniciar la tarea de análisis por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se inicie automáticamente lo antes posible.

Si no es posible configurar una programación de análisis óptima, Kaspersky Endpoint Security le permite ejecutar un análisis del equipo cuando se cumplen las siguientes condiciones especiales:

- Después de una actualización de las bases de datos.

Kaspersky Endpoint Security ejecuta el análisis del equipo con las bases de datos de firmas actualizadas.

- Después de iniciar la aplicación.

Kaspersky Endpoint Security ejecuta un análisis del equipo cuando transcurre un período específico después de iniciar la aplicación. Dado que se ejecutan varios procesos al iniciar el sistema operativo, es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después del inicio de Kaspersky Endpoint Security.

- Wake-on-LAN.

Kaspersky Endpoint Security ejecuta un análisis del equipo según lo programado, incluso si el equipo está apagado. Para hacerlo, la aplicación utiliza la función Wake-on-LAN del sistema operativo. La función Wake-on-LAN permite encender el equipo de forma remota mediante el envío de una señal especial a través de la red local. Para utilizar esta función, debe activar Wake-on-LAN en la configuración del BIOS.

Puede configurar la ejecución del análisis mediante Wake-on-LAN solo para la tarea de *Análisis antivirus* en Kaspersky Security Center. No puede activar Wake-on-LAN para analizar el equipo en la interfaz de la aplicación.

- Cuando el equipo está inactivo.

Kaspersky Endpoint Security ejecuta un análisis del equipo según lo programado cuando el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security suspende el análisis. Esto significa que la aplicación puede tardar varios días en completar un análisis total del equipo.

## [Cómo configurar la programación del análisis en la Consola de administración \(MMC\)](#)


1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Tareas**.
4. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.  
Si es necesario, [cree una tarea de Análisis antivirus](#).
5. En la ventana de propiedades de la tarea, seleccione la sección **Programación**.
6. Configure la programación de la tarea de análisis.
7. Según la frecuencia seleccionada, ajuste la configuración avanzada que especifica la planificación de la ejecución de la tarea (ver la tabla a continuación).
8. Guarde los cambios.

## [Cómo configurar la programación del análisis en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea de análisis.  
Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Planificación**.
4. Configure la programación de la tarea de análisis.
5. Según la frecuencia seleccionada, ajuste la configuración avanzada que especifica la planificación de la ejecución de la tarea (ver la tabla a continuación).
6. Guarde los cambios.

## [Cómo configurar la programación del análisis en la interfaz de la aplicación](#)

Puede configurar la programación del análisis solo si no se aplica una directiva al equipo. Para equipos con una directiva, puede configurar la programación de la tarea de *Análisis antivirus* 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 el botón **Programación de análisis**.
4. En la ventana abierta, configure el programa de ejecución de la tarea de análisis.
5. Según la frecuencia seleccionada, ajuste la configuración avanzada que especifica la planificación de la ejecución de la tarea (ver la tabla a continuación).
6. Guarde los cambios.

Configuración de la programación del análisis

Parámetro	Descripción
<b>Programación de análisis</b>	<p><b>Manual.</b> Modo de ejecución en el que puede comenzar a analizar manualmente en el momento que sea conveniente para usted.</p> <p><b>Según programación.</b> En este modo de ejecución de la tarea de análisis, Kaspersky Endpoint Security comienza el análisis en función de la planificación especificada. Si está seleccionado este modo de ejecución de la tarea de análisis, también puede iniciar la tarea de análisis manualmente.</p>
<b>Posponer la ejecución después del inicio de la aplicación durante N minutos</b>	Inicio pospuesto de la tarea de análisis después del inicio de la aplicación. Dado que se ejecutan varios procesos al iniciar el sistema operativo, es conveniente posponer la ejecución de la tarea de análisis en lugar de ejecutarla inmediatamente después del inicio de Kaspersky Endpoint Security.
<b>Ejecutar las tareas omitidas</b>	Si se selecciona la casilla de verificación, Kaspersky Endpoint Security inicia la tarea de análisis omitida lo antes posible. La tarea de análisis se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio programa de la tarea de actualización. Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no inicia las tareas de análisis omitidas. En lugar de ello, lleva a cabo la siguiente tarea de análisis de acuerdo con la planificación actual.
<b>Ejecutar solo cuando el equipo está inactivo</b>	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 si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió.
<b>Usar el retraso aleatorio automáticamente para el inicio de tareas</b>	Si se selecciona la casilla de verificación, la tarea no se ejecuta estrictamente según lo programado, sino aleatoriamente dentro de un intervalo determinado, es decir, se distribuyen las horas de inicio de la tarea. Las horas de inicio aleatorias ayudan a evitar que una gran cantidad de equipos accedan simultáneamente al Servidor de administración cuando la tarea se ejecuta según lo programado.

<p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>El intervalo de horas de inicio aleatorias se calcula automáticamente cuando se crea la tarea, según la cantidad de equipos que tienen la tarea asignada. Posteriormente, la tarea siempre se ejecuta a la hora de inicio calculada. Sin embargo, siempre que se modifique la configuración de la tarea o la tarea se ejecute manualmente, la hora de inicio calculada cambia.</p> <p>Si la casilla de verificación está desactivada, la tarea se ejecuta exactamente a la hora programada.</p>
<p><b>Detenga la tarea si se ha estado ejecutando durante más de N (min)</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Al limitar el tiempo de ejecución de la tarea Después del período de tiempo especificado, Kaspersky Endpoint Security detiene la tarea. La tarea no está marcada como completada. La próxima vez que Kaspersky Endpoint Security ejecute la tarea, se ejecutará desde el principio y según lo programado.</p> <p>Para reducir el tiempo de ejecución de la tarea, puede, por ejemplo, <a href="#">configurar el alcance del análisis</a> u <a href="#">optimizar el análisis</a>.</p>
<p><b>Activar el dispositivo con la función Wake-on-LAN antes de que se inicie la tarea (min)</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Si se selecciona la casilla de verificación, el sistema operativo del equipo recibe un tiempo de espera especificado para completar el inicio antes de que se ejecute la tarea. El tiempo de espera predeterminado es de 5 minutos.</p> <p>Seleccione la casilla de verificación si desea ejecutar la tarea en todos los equipos, incluidos los que están apagados.</p>

## Ejecutar un análisis como un usuario diferente

Por defecto, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. La cobertura de protección puede incluir unidades de red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que tenga los permisos adecuados en la configuración de Kaspersky Endpoint Security y realizar la tarea de análisis con esta cuenta de usuario.

Puede ejecutar los siguientes análisis como un usuario diferente:

- Análisis de áreas críticas.
- Análisis completo.
- Análisis personalizado.
- [Analizar desde el menú contextual](#).

No puede configurar los derechos de usuario para ejecutar un [Análisis de unidades extraíbles](#), un [Análisis en segundo plano](#) ni una [Comprobación de integridad](#).


[Cómo ejecutar un análisis como un usuario diferente en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Tareas**.
4. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.
5. En la ventana de propiedades de la tarea, seleccione la sección **Cuenta**.
6. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar una tarea de análisis.
7. Guarde los cambios.

### Cómo ejecutar un análisis como un usuario diferente en Web Console o Cloud Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea de análisis.  
Se abre la ventana propiedades de la tarea.
3. Seleccione la pestaña **Configuración**.
4. Debajo de **Cuenta**, haga clic en **Configuración**.
5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar una tarea de análisis.
6. Guarde los cambios.

### Cómo ejecutar un análisis como un usuario diferente en la interfaz de la aplicación

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en .
3. En las propiedades de la tarea, seleccione **Configuraciones avanzadas** → **Ejecutar el análisis como**.
4. En la ventana abierta, introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar una tarea de análisis.
5. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).



## Optimización del análisis

Puede optimizar el análisis de archivos: reduzca el tiempo de análisis y aumente la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede conseguir si analiza solamente los archivos nuevos y los que se hayan modificado desde el último análisis. Este modo se aplica tanto a archivos simples como a compuestos. También puede establecer un límite para la duración del análisis de un único archivo. Cuando se supera el intervalo de tiempo especificado, Kaspersky Endpoint Security excluye el archivo del análisis actual (excepto los archivos y objetos que incluyen varios archivos).

Una técnica común para ocultar virus y otro tipo de software malicioso (malware) consiste en implantarlos en archivos compuestos, como archivos comprimidos o bases de datos. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

También puede activar las tecnologías iChecker e iSwift. Las tecnologías iChecker e iSwift optimizan la velocidad del análisis de archivos ya que excluyen archivos que no han sido modificados desde el análisis más reciente.

[Cómo optimizar el análisis en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Tareas**.
4. Seleccione la tarea de análisis y haga doble clic para abrir las propiedades de la tarea.  
Si es necesario, [cree una tarea de Análisis antivirus](#).
5. En la ventana de propiedades de la tarea, seleccione la sección **Configuración**.
6. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.  
Esto abre la ventana de configuración de la tarea de análisis.
7. En el bloque **Optimización del análisis**, establezca la configuración del análisis:
  - **Analizar solamente archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.  
También puede configurar el análisis de archivos nuevos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo archivos comprimidos nuevos y archivos de formato Office.
  - **Omitir archivos cuyo análisis dure más de N segundos**. Esto establece un límite de tiempo para analizar un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.
8. Haga clic en el botón **Avanzado**.  
Esto abre la ventana de configuración de análisis de archivos compuestos.
9. En la sección **Límite de tamaño**, seleccione la casilla **No descomprimir archivos compuestos de gran tamaño**. Esto establece un límite de tiempo para analizar un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.

Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.
10. Haga clic en **Aceptar**.
11. Seleccione la pestaña **Adicional**.
12. En el bloque **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar durante un análisis:
  - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

- **Tecnología iChecker.** Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

13. Guarde los cambios.

### [Cómo optimizar el análisis en Web Console y Cloud Console](#)

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

Se abre la lista de tareas.

2. Haga clic en la tarea de análisis.

Se abre la ventana propiedades de la tarea. Si es necesario, [cree una tarea de Análisis antivirus](#).

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

4. En la sección **Acción al detectar una amenaza**, seleccione la casilla de verificación **Analizar solamente archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.

También puede configurar el análisis de archivos nuevos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo archivos comprimidos nuevos y archivos de formato Office.


5. Seleccione la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**. Esto establece un límite de tiempo para analizar un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.

Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

6. Debajo de **Configuraciones avanzadas**, seleccione la casilla de verificación **Omitir archivos cuyo análisis dure más de N segundos**. Esto establece un límite de tiempo para analizar un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.

7. Guarde los cambios.

### [Cómo optimizar el análisis en la interfaz de la aplicación](#)

1. En la ventana principal de la aplicación, vaya a la sección **Tareas**.
2. En la lista de tareas, seleccione la tarea de análisis y haga clic en .
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Optimización del análisis**, establezca la configuración del análisis:
  - **Analizar solamente archivos nuevos y modificados.** Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.  
También puede configurar el análisis de archivos nuevos por tipo. Por ejemplo, puede analizar todos los paquetes de distribución y analizar solo archivos comprimidos nuevos y archivos de formato Office.
  - **Omitir los objetos analizados durante más de N segundos.** Esto establece un límite de tiempo para analizar un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.
5. En la sección **Límite de tamaño**, seleccione la casilla **No descomprimir archivos compuestos de gran tamaño**. Esto establece un límite de tiempo para analizar un solo objeto. Tras la cantidad de tiempo especificada, Kaspersky Endpoint Security detiene el análisis del archivo. Esto ayuda a reducir la duración del análisis.

Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

6. En el bloque **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar durante un análisis:
  - **Tecnología iSwift.** Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
  - **Tecnología iChecker.** Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).
7. Guarde los cambios.

Si no se muestra la tarea de análisis, significa que el administrador [ha prohibido el uso de tareas locales en la directiva](#).

## Actualización de las bases de datos y módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

Las actualizaciones regulares requieren una licencia efectiva. Si no hay ninguna licencia actual, solamente podrá realizar una actualización una vez.

El origen principal de actualizaciones para Kaspersky Endpoint Security son los servidores de actualizaciones de Kaspersky.

Su equipo debe estar conectado a Internet para descargar satisfactoriamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. De forma predeterminada, los parámetros de conexión a Internet se determinan automáticamente. Si utiliza un servidor proxy, debe ajustar la configuración del servidor proxy.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTP.

Mientras se lleva a cabo la actualización, se descargan e instalan los siguientes objetos en su equipo:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se proporciona por medio de bases de datos que contienen firmas de virus y otras amenazas, así como información sobre la forma de neutralizarlas. Los componentes de protección emplean esta información a la hora de buscar y neutralizar archivos infectados en el equipo. Las bases de datos se actualizan constantemente con registros de nuevas amenazas y métodos para combatirlas. Por tanto, es recomendable que actualice la base de datos con regularidad.  
Además de las bases de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de protección interceptar el tráfico de la red.
- Módulos de la aplicación. Aparte de las bases de datos de Kaspersky Endpoint Security, también puede actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación sirve para solucionar vulnerabilidades en Kaspersky Endpoint Security, añade nuevas funciones o mejora las existentes.

Durante una actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con los de la versión actualizada en el origen de actualizaciones. Si los módulos de la aplicación y las bases de datos actuales son diferentes de sus respectivas versiones actualizadas, la parte de las actualizaciones que falte se instala en su equipo.

Los archivos de ayuda contextual se pueden actualizar junto con las actualizaciones de los módulos de la aplicación.

Si las bases de datos no están actualizadas, puede que el tamaño del paquete de actualización sea considerable, lo que provocaría un tráfico de Internet adicional (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en la ventana principal de la aplicación o en la información sobre herramientas que ve cuando pasa el cursor sobre el icono de la aplicación en el área de notificación.

La información sobre los resultados de la actualización y sobre todos los eventos se producen durante la ejecución de la tarea de actualización se registra en el [informe de Kaspersky Endpoint Security](#).

## Escenarios de actualización de las bases de datos y los módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

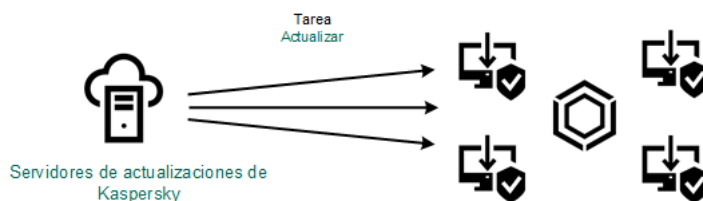
Los objetos que se actualizan en los equipos de los usuarios son los siguientes:

- Bases de datos antivirus. Las bases de datos antivirus contienen bases de datos con firmas de malware, descripciones de ataques de red, bases de datos de direcciones web fraudulentas y maliciosas, bases de datos de banners, bases de datos de spam y otras clases de información.
- Módulos de la aplicación. Las actualizaciones de módulos están diseñadas para eliminar vulnerabilidades de la aplicación y mejorar los métodos con los que se protegen los equipos. Cuando se actualizan los módulos, la aplicación puede sumar nuevas funciones y modificar el comportamiento de sus componentes.

Las bases de datos y los módulos de Kaspersky Endpoint Security pueden actualizarse de las siguientes maneras:

- Actualización con los servidores de Kaspersky.

Los servidores de actualización de Kaspersky están ubicados en varios países del mundo. Gracias a ello, el proceso de actualización es altamente fiable. Cuando Kaspersky Endpoint Security no puede descargar las actualizaciones de un servidor, cambia a uno distinto.



Actualización con los servidores de Kaspersky

- Actualización centralizada.

La actualización centralizada reduce el tráfico de Internet externo y facilita el control del proceso.

La actualización centralizada consta de los siguientes pasos:

1. Descargar el paquete de actualización a un repositorio ubicado en la red de la organización.

Para descargar el paquete de actualización, se utiliza la tarea del Servidor de administración llamada *Descargar actualizaciones en el repositorio del Servidor de administración*.

2. Descargar el paquete de actualización a una carpeta compartida (opcional).

Para descargar el paquete de actualización a una carpeta compartida, puede usar los siguientes métodos:

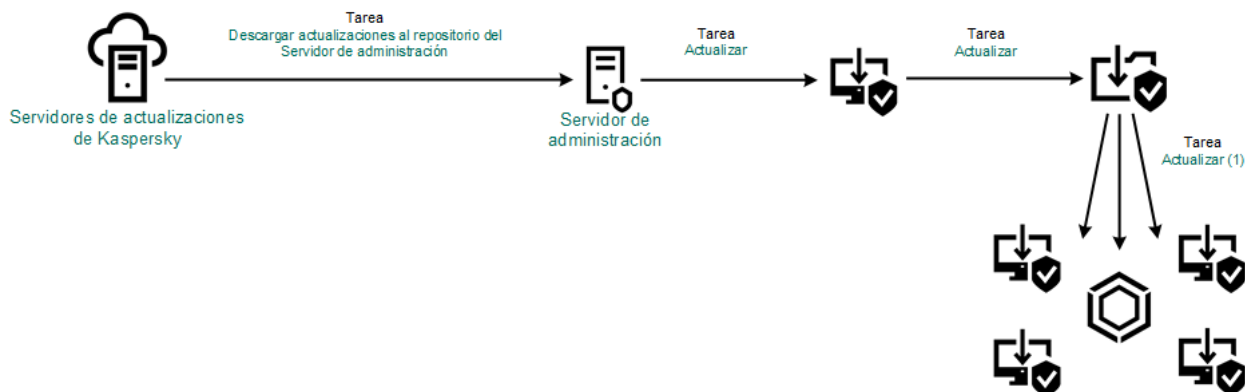
- Uso de la tarea *Actualización* de Kaspersky Endpoint Security. Esta tarea está destinada a uno de los equipos en la red de la compañía local.
- Usar la herramienta Kaspersky Update Utility. Para obtener información detallada sobre el uso de Kaspersky Update Utility, consulte la [Base de conocimientos de Kaspersky](#).

3. Distribuir el paquete de actualización a los equipos cliente.

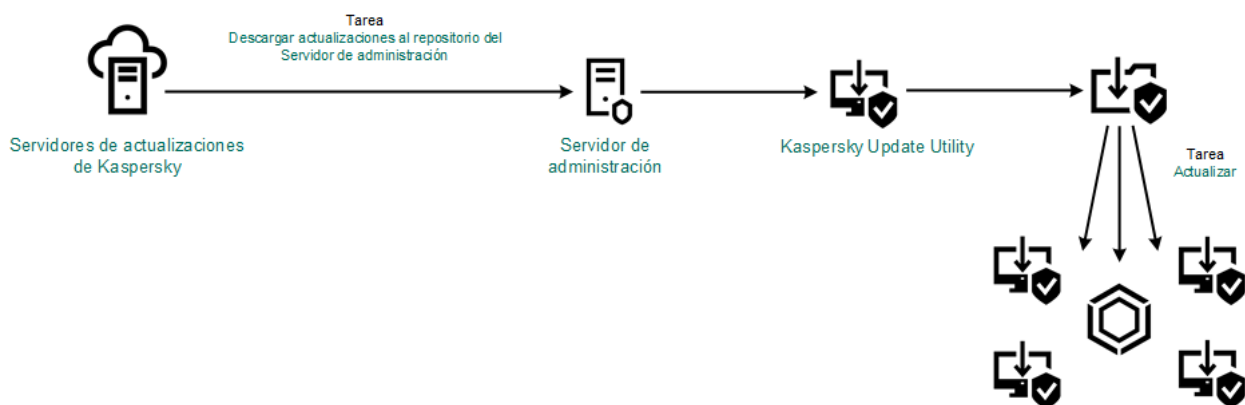
Para distribuir el paquete a los equipos cliente, utilice la tarea *Actualización* de Kaspersky Endpoint Security. Podrá crear cuantas tareas de actualización necesite para cada grupo de administración.



Actualización con un repositorio de servidor



Actualización con una carpeta compartida



Actualización con Kaspersky Update Utility

Para Web Console, la lista predeterminada de orígenes de actualizaciones contiene los servidores de actualización del Servidor de administración de Kaspersky Security Center y de Kaspersky. Para Kaspersky Security Center Cloud Console, la lista predeterminada de orígenes de actualizaciones contiene los servidores de actualización de Kaspersky y los puntos de distribución. Para obtener más información sobre puntos de distribución, consulte la [Ayuda de Kaspersky Security Center Cloud Console](#). Puede añadir a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones. Cuando Kaspersky Endpoint Security no puede descargar las actualizaciones de un origen, cambia a uno distinto.

Las actualizaciones se descargan de los servidores de actualizaciones de Kaspersky, o de otros servidores FTP o HTTP, usando protocolos de red estándar. Si la conexión al origen de actualizaciones debe establecerse a través de un servidor proxy, [especifique los parámetros de conexión pertinentes en los ajustes de directiva de Kaspersky Endpoint Security](#).

## Actualización con un repositorio de servidor

Para reducir el tráfico de Internet, los equipos conectados a la LAN de la organización pueden obtener las actualizaciones de las bases de datos y de los módulos de la aplicación de un repositorio de servidor. En esta modalidad, Kaspersky Security Center descarga un paquete de actualización de los servidores de actualizaciones de Kaspersky y lo guarda en un repositorio (un servidor FTP o HTTP, una carpeta de red o una carpeta local). Los demás equipos conectados a la LAN obtienen de allí el paquete de actualización.

Si desea utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. Configurar la descarga del paquete de actualización a un repositorio del Servidor de administración (tarea *Descargar actualizaciones en el repositorio del Servidor de administración*).
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*).



Para configurar la descarga de un paquete de actualización al repositorio del servidor:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Seleccione la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** del Servidor de administración.  
Se abre la ventana propiedades de la tarea.  
La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* del Servidor de administración se crea automáticamente al usar el Asistente de inicio rápido de Kaspersky Security Center Web Console. Solo puede existir un ejemplar de esta tarea.
3. Seleccione la ficha **Configuración de la aplicación**.
4. En la sección **Otros parámetros**, haga clic en **Configurar**.
5. En el campo **Carpeta para almacenar actualizaciones**, escriba la dirección del servidor FTP/HTTP, carpeta local o carpeta de red en donde Kaspersky Security Center copia el paquete de actualización que reciba de los servidores de actualización de Kaspersky.

Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

- Para un servidor FTP o HTTP, introduzca su dirección web o su dirección IP.  
Por ejemplo, `http://dn1-01.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://<nombre de usuario>:<contraseña>@<nodo>:<puerto>`.
- Para una carpeta de red, introduzca la ruta UNC.  
Por ejemplo, `\\ Server\Share\Update distribution`.
- En el caso de una carpeta local, introduzca la ruta completa de esa carpeta.



Por ejemplo, C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

6. Guarde los cambios.

*Para configurar la actualización de Kaspersky Endpoint Security desde el almacenamiento del servidor especificado:*

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

Se abre la lista de tareas.

2. Haga clic en la tarea **Actualización** correspondiente a Kaspersky Endpoint Security.

Se abre la ventana propiedades de la tarea.

La tarea *Actualización* se crea automáticamente al usar el Asistente de inicio rápido de Kaspersky Security Center. Para crear la tarea *Actualización*, instale el complemento web de Kaspersky Endpoint Security para Windows mientras esté 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 **Añadir**.

5. En el campo **Origen**, escriba la dirección del servidor FTP/HTTP, carpeta local o carpeta de red en donde Kaspersky Security Center guardará el paquete de actualización que reciba de los servidores de Kaspersky.

La dirección de la fuente de actualización debe coincidir con la dirección que especificó en el campo **Carpeta para almacenar actualizaciones** cuando configuró la descarga de actualizaciones en el almacenamiento del servidor (consulte *las instrucciones anteriores*).

6. En la sección **Estado**, seleccione **Activado**.

7. Haga clic en **Aceptar**.

8. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.

9. Guarde los cambios.

Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

## Actualización con una carpeta compartida

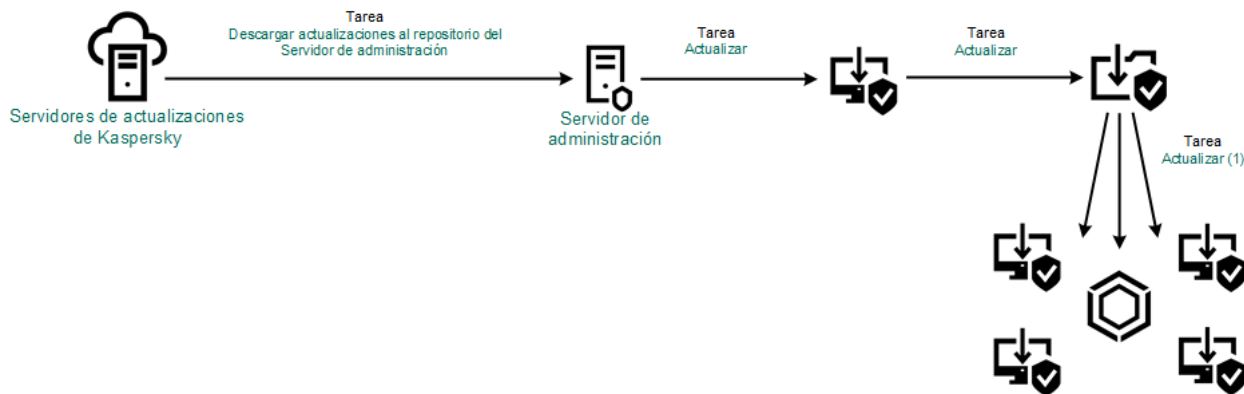
Para reducir el tráfico de Internet, los equipos conectados a la LAN de la organización pueden obtener las actualizaciones de las bases de datos y de los módulos de la aplicación de una carpeta compartida. En esta modalidad, uno de los equipos de la LAN se encarga de recibir los paquetes de actualización 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.

Si desea utilizar una carpeta compartida para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. [Utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación.](#)

2. Activar la copia de un paquete de actualización en una carpeta compartida en uno de los equipos de la LAN empresarial (ver las instrucciones a continuación).
3. Configuración del proceso de actualización para que los demás equipos de la LAN de la organización obtengan las bases de datos y los módulos de la aplicación más recientes de la carpeta compartida (vea las instrucciones a continuación).

La versión y localización de la aplicación Kaspersky Endpoint Security que copia el paquete de actualización a una carpeta compartida debe coincidir con la versión y localización de la aplicación que actualiza las bases de datos desde la carpeta compartida. Si las versiones o localizaciones de las aplicaciones no coinciden, la actualización de la base de datos puede terminar con un error.



Actualización con una carpeta compartida

Para activar la copia del paquete de actualización en la carpeta compartida:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea **Actualización** correspondiente a Kaspersky Endpoint Security.  
Se abre la ventana propiedades de la tarea.  
La tarea *Actualización* se crea automáticamente al usar el Asistente de inicio rápido de Kaspersky Security Center. Para crear la tarea *Actualización*, instale el complemento web de Kaspersky Endpoint Security para Windows mientras esté 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. Active la casilla **Copiar las actualizaciones en la carpeta**.
6. En el campo **Ruta**, introduzca la ruta UNC a la carpeta compartida (por ejemplo, \\Server\Share\Update distribution).  
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\AVP11\Update distribution\.
7. Guarde los cambios.

La tarea *Actualización* debe asignarse al equipo que actuará como origen de actualizaciones.

Para que la actualización se realice usando una carpeta compartida:

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

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

c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Actualización desde una carpeta compartida*).

d. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

La tarea *Actualización* debe asignarse a los equipos conectados a la LAN de la organización, salvo al que actúa como origen de actualizaciones.

4. Seleccione dispositivos de acuerdo con la opción de cobertura de la tarea que haya elegido y vaya al paso siguiente.

5. Salga del Asistente.

La nueva tarea aparecerá en la tabla de tareas.

6. Haga clic en la tarea *Update* recién creada.

Se abre la ventana propiedades de la tarea.

7. Vaya a la sección **Configuración de la aplicación**.

8. Seleccione la ficha **Modo local**.

9. En el bloque **Origen de actualizaciones**, haga clic en **Añadir**.

10. En el campo **Origen**, escriba la ruta de la carpeta compartida.

La dirección del origen debe ser la misma que haya especificado en el campo **Ruta** al configurar la copia del paquete de actualización a la carpeta compartida (consulte las instrucciones de más arriba).

11. Haga clic en **Aceptar**.

12. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.

13. Guarde los cambios.

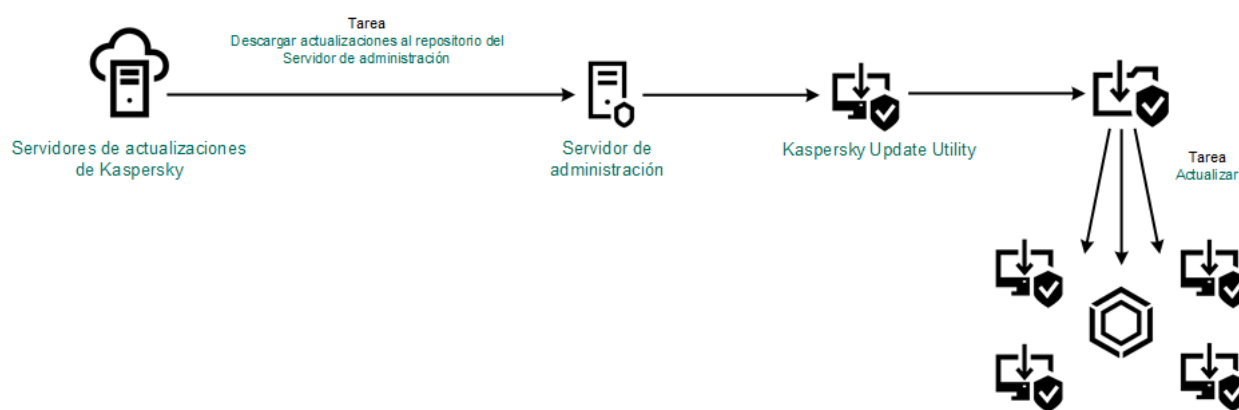
## Actualización con Kaspersky Update Utility

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.

Si desea utilizar una carpeta compartida para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. [Utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación.](#)
2. Instale Kaspersky Update Utility en uno de los equipos conectados a la LAN de su organización.
3. Configure Kaspersky Update Utility para que el paquete de actualización se copie a la carpeta compartida.
4. Configuración del proceso de actualización para que los demás equipos de la LAN de la organización obtengan las bases de datos y los módulos de la aplicación más recientes de la carpeta compartida.

La versión y localización de la aplicación Kaspersky Endpoint Security que copia el paquete de actualización a una carpeta compartida debe coincidir con la versión y localización de la aplicación que actualiza las bases de datos desde la carpeta compartida. Si las versiones o localizaciones de las aplicaciones no coinciden, la actualización de la base de datos puede terminar con un error.



Actualización con Kaspersky Update Utility

Para descargar el paquete de distribución de Kaspersky Update Utility, visite el [sitio web de soporte técnico de Kaspersky](#). Después de instalar la utilidad, seleccione el origen de las actualizaciones (por ejemplo, el repositorio del Servidor de administración) y la carpeta compartida a la que Kaspersky Update Utility copiará los paquetes de actualización. Para obtener información detallada sobre el uso de Kaspersky Update Utility, consulte la [Base de conocimientos de Kaspersky](#).

Para que la actualización se realice usando una carpeta compartida:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**. Se abre la lista de tareas.
2. Haga clic en la tarea **Actualización** correspondiente a Kaspersky Endpoint Security.

Se abre la ventana propiedades de la tarea.

La tarea *Actualización* se crea automáticamente al usar el Asistente de inicio rápido de Kaspersky Security Center. Para crear la tarea *Actualización*, instale el complemento web de Kaspersky Endpoint Security para Windows mientras esté 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 **Añadir**.
5. En el campo **Origen**, introduzca la ruta UNC a la carpeta compartida (por ejemplo, \\Server\Share\Update distribution).

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 **Arriba** y **Abajo**.
8. Guarde los cambios.

## Actualización en modo móvil

Se denomina *modo móvil* al modo en que Kaspersky Endpoint Security funciona cuando un equipo sale de la red de la organización (*equipo sin conexión*). Para más información sobre cómo trabajar con los equipos sin conexión y los usuarios que están fuera de la oficina, consulte la [Ayuda de Kaspersky Security Center](#).

Los equipos sin conexión a la red de la organización no pueden acceder al Servidor de administración para actualizar las bases de datos y los módulos de la aplicación. De forma predeterminada en el modo móvil, solo los servidores de actualización de Kaspersky se utilizan como fuente de actualización para actualizar bases de datos y módulos de aplicaciones. El uso de un servidor proxy para acceder a Internet se rige por una directiva especial, llamada [directiva fuera de la oficina](#). Esta directiva debe crearse por separado. Cuando Kaspersky Endpoint Security cambia al modo móvil, la tarea de actualización se ejecuta cada dos horas.

*Para configurar los parámetros de actualización en modo móvil:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea **Actualización** correspondiente a Kaspersky Endpoint Security.  
Se abre la ventana propiedades de la tarea.  
La tarea *Actualización* se crea automáticamente al usar el Asistente de inicio rápido de Kaspersky Security Center. Para crear la tarea *Actualización*, instale el complemento web de Kaspersky Endpoint Security para Windows mientras esté utilizando el Asistente.  
Seleccione la pestaña **Configuración de la aplicación** → **Modo móvil**.
3. 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.
4. Guarde los cambios.

Como resultado, las bases de datos y los módulos de aplicación se actualizarán en los equipos de los usuarios cuando cambien al modo móvil.

## Inicio y parada de una tarea de actualización

Independientemente del modo de ejecución de la tarea de actualización seleccionado, puede iniciar o parar una tarea de actualización de Kaspersky Endpoint Security en cualquier momento.

*Para iniciar o parar una tarea de actualización:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. En el mosaico **Actualización de las bases de datos y módulos de la aplicación**, haga clic en el botón **Actualizar** si desea iniciar la tarea de actualización.

Kaspersky Endpoint Security comenzará a actualizar los módulos y las bases de datos de la aplicación. La aplicación mostrará el progreso de la tarea, el tamaño de los archivos descargados y el origen de actualizaciones. Puede detener la tarea en cualquier momento haciendo clic en **Detener actualización**.


*Para iniciar o detener la tarea de actualización cuando se muestra la [interfaz simplificada de la aplicación](#):*

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En la lista desplegable **Tareas** del menú contextual, lleve a cabo una de las siguientes acciones:
  - seleccione una tarea de actualización que no esté en ejecución para iniciarla
  - seleccione una tarea de actualización en ejecución para detenerla
  - seleccione una tarea de actualización suspendida para reanudarla o reiniciarla

## Inicio de una tarea de actualización con los permisos de una cuenta de usuario distinta

De forma predeterminada, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta se ha utilizado para iniciar la sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security se podría actualizar desde un origen de actualizaciones al que el usuario no pueda acceder debido a la falta de los permisos necesarios (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o un origen de actualizaciones para el que no se haya configurado la autenticación del servidor proxy. En la configuración de Kaspersky Endpoint Security, puede especificar un usuario que tenga esos permisos e iniciar la tarea de actualización de Kaspersky Endpoint Security con la cuenta de ese usuario.

*Para iniciar una tarea de actualización con una cuenta de usuario distinta:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. Esto abre la lista de tareas. Seleccione la tarea de actualización y haga clic en .
3. Haga clic en **Ejecutar actualizaciones de bases de datos como**.


4. Esto abre una ventana donde debe seleccionar **Otro usuario**.
5. Introduzca las credenciales de la cuenta de un usuario con los permisos necesarios para acceder al origen de actualizaciones.
6. Guarde los cambios.

## Selección del modo de ejecución de la tarea de actualización

Si no es posible iniciar la tarea de actualización por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se inicie automáticamente lo antes posible.

Puede retrasar la ejecución de la tarea de actualización después de que se inicie la aplicación si selecciona el modo de ejecución de la tarea de ejecución **Según programación** y si el momento del inicio de Kaspersky Endpoint Security coincide con la planificación del inicio de la tarea de actualización. La tarea de actualización solamente puede ejecutarse después de que transcurra la cantidad de tiempo especificada una vez que se inicia Kaspersky Endpoint Security.

*Para seleccionar el modo de ejecución de la tarea de actualización:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. Esto abre la lista de tareas. Seleccione la tarea de actualización y haga clic en .
3. Haga clic en **Programación de la actualización de bases de datos**.
4. En la ventana abierta, seleccione el modo de ejecución de la tarea de actualización:
  - Si quiere que Kaspersky Endpoint Security ejecute la tarea de actualización en función de si hay o no disponible un paquete de actualización en el origen de actualizaciones, seleccione **Automático**. La frecuencia de las comprobaciones que realiza Kaspersky Endpoint Security para ver si hay paquetes de actualización aumenta durante los brotes de virus y disminuye en otros momentos.
  - Si quiere iniciar una tarea de actualización manualmente, seleccione **Manual**.
  - Si quiere configurar una planificación para ejecutar la tarea de actualización, seleccione otras opciones. Establezca la configuración avanzada para iniciar la tarea de actualización:
    - En el campo **Posponer la ejecución después del inicio de la aplicación durante N minutos**, introduzca el intervalo de tiempo durante el que desea posponer el inicio de la tarea de actualización después del inicio de Kaspersky Endpoint Security.
    - Seleccione la opción **Ejecutar análisis planificado 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.
5. Guarde los cambios.

## Adición de un origen de actualizaciones

Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security.


Las fuentes de las actualizaciones incluyen el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky y carpetas locales y en red.

La lista predeterminada de orígenes de actualizaciones incluye los servidores de actualizaciones de Kaspersky Security Center y Kaspersky. Puede agregar a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones.

Kaspersky Endpoint Security no es compatible con las actualizaciones de los servidores HTTPS a menos que sean servidores de actualizaciones de Kaspersky.

Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno después de otro, empieza desde el inicio de la lista y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible.

*Para agregar un origen de actualizaciones:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. Esto abre la lista de tareas. Seleccione la tarea de actualización y haga clic en .
3. Haga clic en el botón **Seleccionar origen de actualizaciones**.
4. En la ventana abierta, haga clic en el botón **Añadir**.
5. En la ventana que se abre, especifique la dirección del servidor FTP o HTTP, la carpeta de red o la carpeta local que contiene el paquete de actualización.

Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

- Para un servidor FTP o HTTP, introduzca su dirección web o su dirección IP.  
Por ejemplo, `http://dn1-01.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://<nombre de usuario>:<contraseña>@<nodo>:<puerto>`.
- Para una carpeta de red, introduzca la ruta UNC.  
Por ejemplo, `\\ Server\Share\Update distribution`.
- En el caso de una carpeta local, introduzca la ruta completa de esa carpeta.  
Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Haga clic en el botón **Seleccionar**.
7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.
8. Guarde los cambios.

## Configuración de actualización desde 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.


Si desea utilizar una carpeta compartida para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. Activar la copia de un paquete de actualización en una carpeta compartida en uno de los equipos de la red de área local.
2. Configuración del proceso de actualización para que los demás equipos de la LAN de la organización obtengan las bases de datos y los módulos de la aplicación más recientes de la carpeta compartida.

*Para activar la copia del paquete de actualización en la carpeta compartida:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. Esto abre la lista de tareas. Seleccione la tarea de actualización y haga clic en .
3. En el bloque **Distribuyendo actualizaciones**, seleccione la casilla de verificación **Copiar las actualizaciones a la carpeta**.
4. Introduzca la ruta UNC a la carpeta compartida (por ejemplo, \\Server\Share\Update distribution).
5. Guarde los cambios.

*Para que la actualización se realice usando una carpeta compartida:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. Esto abre la lista de tareas. Seleccione la tarea de actualización y haga clic en .
3. Haga clic en el botón **Seleccionar origen de actualizaciones**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. En la ventana que se abre, introduzca la ruta de la carpeta compartida.

La dirección del origen debe ser la misma que haya especificado al configurar la copia del paquete de actualización a la carpeta compartida (consulte las *instrucciones de más arriba*).

6. Haga clic en el botón **Seleccionar**.
7. Configure la prioridad de los orígenes de actualizaciones con los botones **Arriba** y **Abajo**.
8. Guarde los cambios.

## Actualización de los módulos de la aplicación

Las actualizaciones del módulo de la aplicación corrigen errores, mejoran el rendimiento y añaden nuevas funciones. Cuando esté disponible una nueva actualización del módulo de la aplicación, debe confirmar la instalación de la actualización. Puede confirmar la instalación de una actualización del módulo de la aplicación en la interfaz de la aplicación o en Kaspersky Security Center. Cuando haya una actualización disponible, la aplicación mostrará una de las siguientes notificaciones en la ventana principal de Kaspersky Endpoint Security: actualización importante (🔔) o actualización crítica (🔴). Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia de usuario final, la aplicación instala las actualizaciones después de que se hayan aceptado dichos términos. Para obtener detalles sobre cómo realizar un seguimiento de las actualizaciones del módulo de la aplicación y confirmar una actualización en Kaspersky Security Center, consulte la [Ayuda de Kaspersky Security Center](#).

Después de instalar una actualización de la aplicación, es posible que deba reiniciar su equipo.

*Para configurar las actualizaciones de los módulos de la aplicación:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. Esto abre la lista de tareas. Seleccione la tarea de actualización y haga clic en ⚙️.
3. En el bloque **Descargando e instalando las actualizaciones de los módulos de la aplicación**, seleccione la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación**.
4. Seleccione las actualizaciones del módulo de la aplicación que desea instalar.
  - **Instalar actualizaciones críticas y aprobadas.** Si se selecciona esta opción, cuando las actualizaciones de los módulos de la aplicación están disponibles, Kaspersky Endpoint Security instala automáticamente las actualizaciones críticas y todas las demás únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center.
  - **Instalar solo actualizaciones aprobadas.** Si se selecciona esta opción, cuando están disponibles las actualizaciones de los módulos de la aplicación, Kaspersky Endpoint Security las instala únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.
5. Guarde los cambios.

## Actualización mediante un servidor proxy

Para que las bases de datos y los módulos de la aplicación más recientes puedan descargarse de un origen de actualizaciones, puede ser necesario especificar los parámetros de conexión de un servidor proxy. Estos parámetros se utilizan para todos los orígenes de actualizaciones. Si el servidor proxy no se necesita para un origen en particular, su uso puede deshabilitarse en las propiedades de la directiva. Kaspersky Endpoint Security también usará un servidor proxy para acceder a Kaspersky Security Network y a los servidores de activación.

*Para conectarse a los orígenes de actualizaciones a través de un servidor proxy:*


1. En la ventana principal de Web Console, haga clic en ⚙️.  
Se abre la ventana de propiedades del Servidor de administración.
2. Vaya a la sección **Configuración del acceso a Internet**.
3. Active la casilla **Usar servidor proxy**.

4. Defina los parámetros para conectarse con el servidor proxy: la dirección del servidor proxy, el número de puerto y los valores de autenticación (nombre de usuario y contraseña).
5. Guarde los cambios.

*Para desactivar el uso de un servidor proxy para un grupo de administración específico:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 la sección **Configuración del servidor proxy**, seleccione **No usar servidor proxy para direcciones locales**.
6. Guarde los cambios.

*Para establecer la configuración del servidor proxy en la interfaz de la aplicación:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Servidor proxy**, haga clic en el enlace **Configuración del servidor proxy**.
4. En la ventana abierta, seleccione una de las siguientes opciones para determinar la dirección del servidor proxy:
  - **Detectar automáticamente la configuración del servidor proxy.**  
Esta opción está seleccionada de forma predeterminada. Kaspersky Endpoint Security utiliza la configuración del servidor proxy que se define en la configuración del sistema operativo.
  - **Usar configuración especificada del servidor proxy.**  
Si seleccionó esta opción, establezca la configuración para conectarse al servidor proxy: dirección y puerto del servidor proxy.
5. Si desea activar la autenticación en el servidor proxy, seleccione la casilla de verificación **Usar autenticación de servidor proxy** y proporcione las credenciales de su cuenta de usuario.
6. Si desea desactivar el uso del servidor proxy al [actualizar las bases de datos y los módulos de aplicaciones](#) desde una carpeta compartida, seleccione la casilla **No usar servidor proxy para direcciones locales**.
7. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security utilizará el servidor proxy para descargar actualizaciones de los módulos de la aplicación y de la base de datos. Kaspersky Endpoint Security también usará un servidor proxy para acceder a servidores KSN y a los servidores de activación de Kaspersky. Si se requiere autenticación en el servidor proxy, pero las credenciales de la cuenta de usuario no se proporcionaron o son incorrectas, Kaspersky Endpoint Security le solicitará el nombre de usuario y la contraseña.

## Reversión de la última actualización

Una vez actualizados las bases de datos y los módulos de la aplicación por primera vez, la función de deshacer la actualización de las bases de datos y los módulos de la aplicación a sus versiones anteriores pasa a estar disponible.

Cada vez que un usuario inicia el proceso de actualización, Kaspersky Endpoint Security crea una copia de seguridad de las bases de datos y de los módulos de la aplicación actuales. Esto permite deshacer la actualización de las bases de datos y de los módulos de la aplicación y restablecer sus versiones anteriores cuando sea necesario. Anular la última actualización es útil, por ejemplo, si la nueva versión de la base de datos contiene una firma no válida que provoca que Kaspersky Endpoint Security bloquee una aplicación segura.

*Para anular la última actualización:*

1. En la ventana principal de la aplicación, vaya a la sección **Actualizar**.
2. En el mosaico **Restauración de las bases de datos a su versión anterior**, haga clic en el botón **Revertir**.

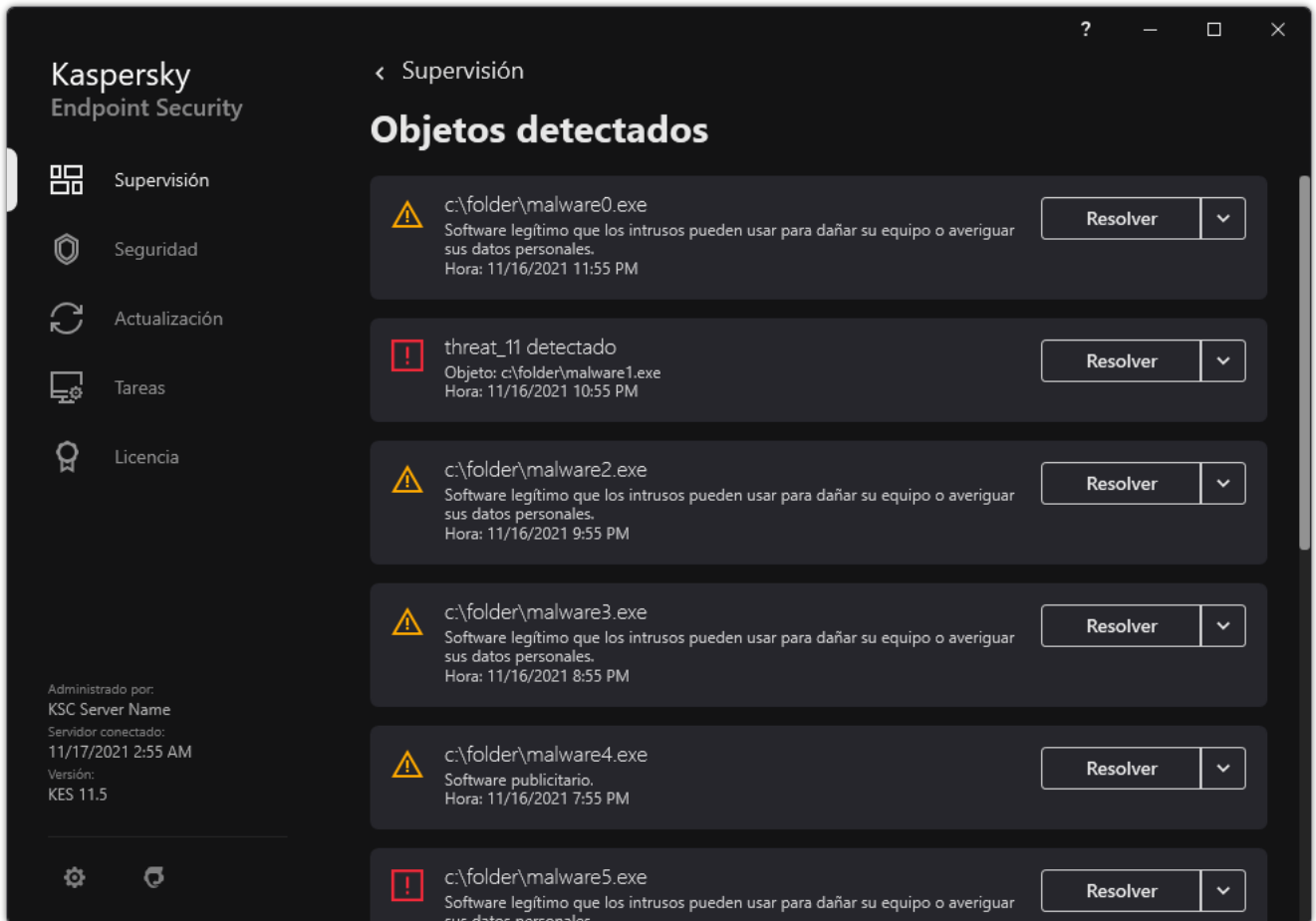
Kaspersky Endpoint Security comenzará a revertir la última actualización de la base de datos. La aplicación mostrará el progreso de la reversión, el tamaño de los archivos descargados y el origen de actualizaciones. Puede detener la tarea en cualquier momento haciendo clic en **Detener actualización**.

*Para iniciar o detener una tarea de anulación cuando se muestra la [interfaz simplificada de la aplicación](#):*

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En la lista desplegable **Tareas** del menú contextual, lleve a cabo una de las siguientes acciones:
  - Seleccione una tarea de anulación que no esté en ejecución para iniciarla.
  - Seleccione una tarea de anulación en ejecución para detenerla.
  - Seleccione una tarea de anulación suspendida para reanudarla o reiniciarla.

## Trabajar con amenazas activas

Kaspersky Endpoint Security registra información sobre los archivos que no ha procesado por alguna razón. Esta información se recoge como eventos en la lista de amenazas activas (consulte la figura siguiente). Para trabajar con amenazas activas, Kaspersky Endpoint Security utiliza la [tecnología de Desinfección avanzada](#). La Desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Puede configurar la desinfección avanzada en la configuración de la tarea [Análisis antivirus](#) y en la [configuración de la aplicación](#).

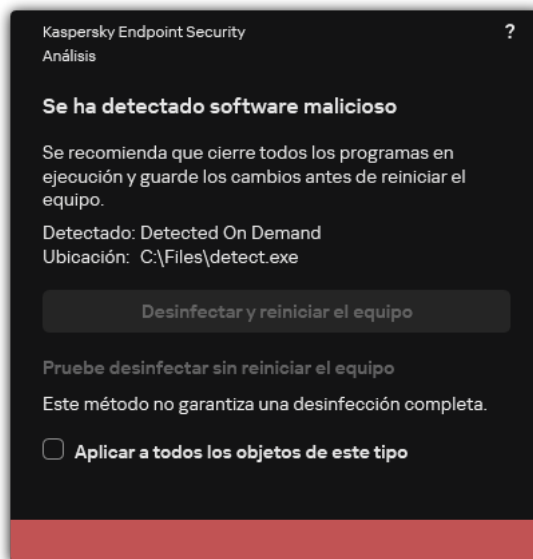


Una lista de amenazas activas

## Desinfección de amenazas activas en estaciones de trabajo

Para trabajar con amenazas activas en estaciones de trabajo, [active la tecnología de Desinfección avanzada](#) en la configuración de aplicaciones. A continuación, configure la experiencia del usuario en las propiedades de la tarea [Análisis antivirus](#). Hay una casilla de verificación **Ejecutar la desinfección avanzada de inmediato** en las propiedades de la tarea. Si se establece una marca, Kaspersky Endpoint Security realizará una desinfección sin notificarle al usuario. Cuando la desinfección esté completa, se reiniciará el equipo. Si no se establece la marca, Kaspersky Endpoint Security mostrará una notificación sobre amenazas activas (consulte la figura a continuación). No puede cerrar esta notificación sin procesar el archivo.

Se realiza una desinfección avanzada durante una tarea de análisis antivirus en un equipo solo si la [característica Desinfección avanzada está activada](#) en las propiedades de la directiva aplicada a este equipo.



Notificación sobre amenazas activas

## Desinfección de amenazas activas en servidores

Para trabajar con amenazas activas en servidores, debe hacer lo siguiente:

- [activar la tecnología de Desinfección avanzada](#) en la configuración de aplicaciones;
- [active Desinfección avanzada inmediata](#) en las propiedades de la tarea Análisis antivirus.

Si Kaspersky Endpoint Security se instala en un equipo en el que se ejecuta Windows para servidores, Kaspersky Endpoint Security no muestra la notificación. Por lo tanto, el usuario no puede seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe [activar la tecnología de Desinfección avanzada](#) en la configuración de la aplicación y [activar la Desinfección avanzada de inmediato](#) en la configuración de la tarea *Análisis antivirus*. Luego, debe iniciar la tarea *Análisis antivirus*.

## Activación o desactivación de la tecnología de desinfección avanzada

Si Kaspersky Endpoint Security no puede detener la ejecución de malware, puede usar la tecnología de desinfección avanzada. La opción Desinfección avanzada está desactivada de manera predeterminada porque esta tecnología usa una cantidad significativa de recursos informáticos. Por lo tanto, puede activar Desinfección avanzada solo cuando [trabaje con amenazas activas](#).

La Desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Para usar la tecnología en servidores, debe [activar la desinfección avanzada inmediata](#) en las propiedades de la tarea *Análisis antivirus*. Este requisito previo no es necesario para usar la tecnología en estaciones de trabajo.


[Cómo activar o desactivar la tecnología de desinfección avanzada en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de la aplicación**.
6. En la sección **Modo de funcionamiento**, seleccione o desactive la casilla de verificación **Activar tecnología de desinfección avanzada** para activar o desactivar la tecnología de desinfección avanzada.
7. Guarde los cambios.

### [Cómo activar o desactivar la tecnología de desinfección avanzada en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 la aplicación**.
5. En la sección **Modo de funcionamiento**, seleccione o desactive la casilla de verificación **Activar tecnología de desinfección avanzada** para activar o desactivar la tecnología de desinfección avanzada.
6. Guarde los cambios.

### [Cómo activar o desactivar la tecnología de desinfección avanzada en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. En la sección **Modo de funcionamiento**, seleccione o desactive la casilla **Usar tecnología de Desinfección avanzada (requiere varios recursos informáticos)** para activar o desactivar la tecnología de desinfección avanzada.
4. Guarde los cambios.

Como resultado, el usuario no puede usar la mayoría de las características del sistema operativo mientras la desinfección activa está en curso. Cuando la desinfección esté completa, se reinicia el equipo.



## Procesamiento de amenazas activas

Se considera un archivo infectado como *procesado* si Kaspersky Endpoint Security desinfectó el archivo o eliminó la amenaza como parte del análisis del equipo en busca de virus y otro malware.

Kaspersky Endpoint Security mueve el archivo a la lista de amenazas activas si, por cualquier motivo, Kaspersky Endpoint Security no lleva a cabo una acción en este archivo de acuerdo con la configuración especificada de la aplicación al analizar el equipo en busca de virus y otras amenazas.

Esta situación puede darse en los siguientes casos:

- El archivo analizado no está disponible (por ejemplo, se encuentra en una unidad de red o en una unidad extraíble sin derechos de escritura).
- En la configuración de la tarea [Análisis antivirus](#), la acción sobre la detección de amenazas se establece como **Notificar**. Después, 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 icono a . En la ventana principal de la aplicación, aparece la notificación de amenaza (consulte la figura siguiente). En la consola de Kaspersky Security Center, el estado del equipo cambia a *Crítico* - .

### [Cómo procesar una directiva en la Consola de administración \(MMC\)](#)

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Adicional** → **Repositorios remota** → **Amenazas activas**.

Se abre la lista de amenazas activas.

2. Seleccione el objeto que desea procesar.

3. Elija de qué manera quiere manejar la amenaza:

- **Desinfectar**. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
- **Eliminar**.

### [Cómo procesar una directiva en Web Console y Cloud Console](#)



1. En la ventana principal de Web Console, seleccione **Operaciones** → **Repositorios** → **Amenazas activas**.

Se abre la lista de amenazas activas.

2. Seleccione el objeto que desea procesar.

3. Elija de qué manera quiere manejar la amenaza:

- **Desinfectar.** Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
- **Eliminar.**

### Cómo procesar una amenaza en la interfaz de la aplicación

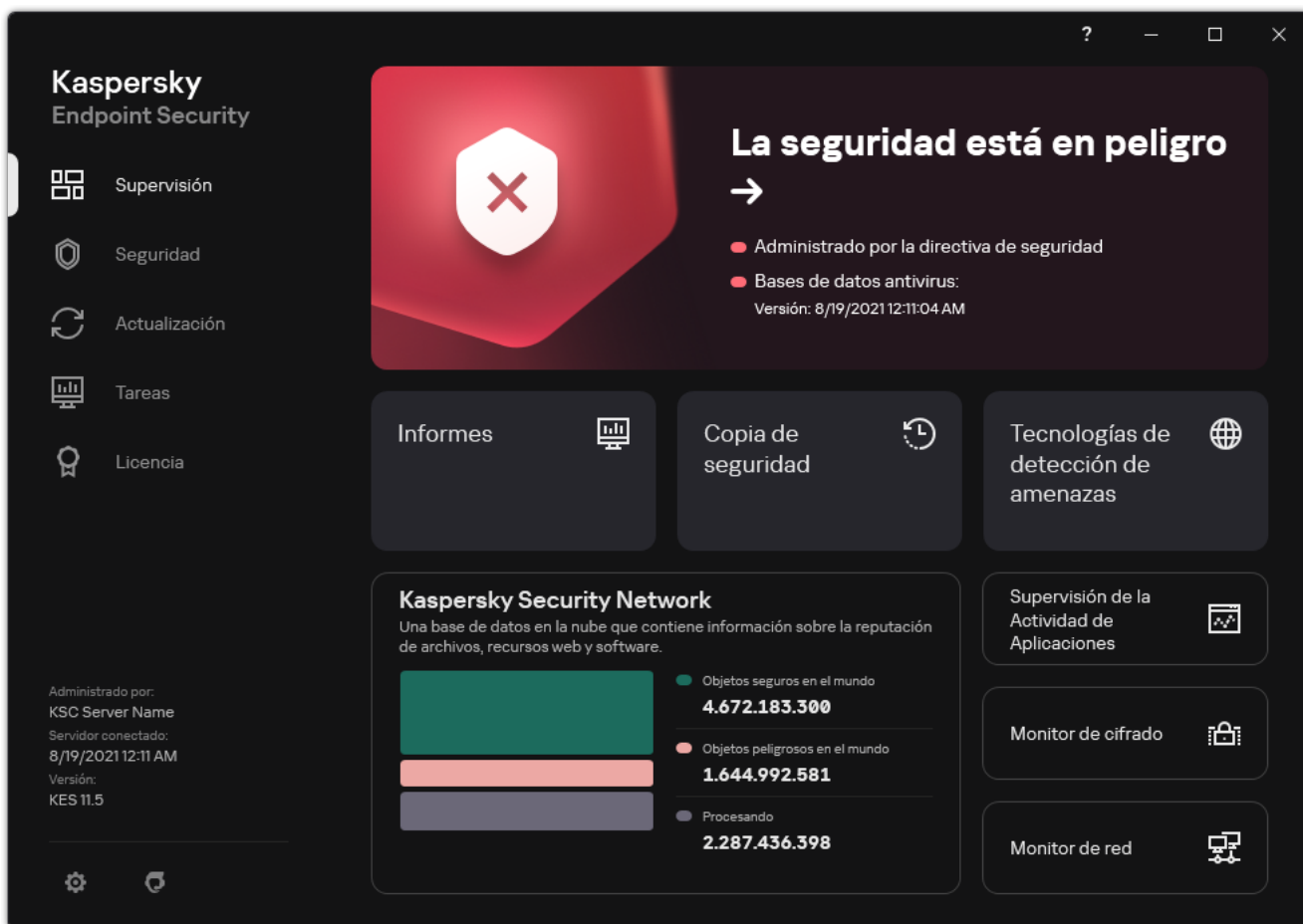
1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **La protección está en peligro**.

Se abre la lista de amenazas activas.

2. Seleccione el objeto que desea procesar.

3. Elija de qué manera quiere manejar la amenaza:

- **Resolver.** Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
- **Añadir a las exclusiones.** Si se selecciona esta acción, Kaspersky Endpoint Security sugiere [añadir el archivo a la lista de exclusiones del análisis](#). Los ajustes de la exclusión se configuran automáticamente. Si no está disponible la opción para añadir una exclusión, significa que el administrador ha desactivado la adición de exclusiones en la configuración de la directiva.
- **Ignorar.** Si se selecciona esta opción, Kaspersky Endpoint Security elimina la entrada de la lista de amenazas activas. Si no quedan amenazas activas en la lista, el estado del equipo se modificará a *Sin inconvenientes*. Si el objeto se vuelve a detectar, Kaspersky Endpoint Security añadirá una nueva entrada a la lista de amenazas activas.
- **Abrir la carpeta donde se encuentra.** Si se selecciona esta opción, Kaspersky Endpoint Security abre la carpeta que contiene el objeto en el administrador de archivos. A continuación, puede eliminar manualmente el objeto o mover el objeto a una carpeta que no está dentro de la cobertura de protección.
- **Más información.** Si se selecciona esta opción, Kaspersky Endpoint Security abre el [sitio web Kaspersky Virus Encyclopedia](#) .



Ventana principal de la aplicación cuando se detecta una amenaza

# Protección del equipo

## Protección frente a amenazas en archivos

El componente Protección frente a amenazas en archivos le permite evitar la infección del sistema de archivos del equipo. De forma predeterminada, el componente Protección frente a amenazas en archivos permanece todo el tiempo en la RAM del equipo. El componente analiza los archivos en todas las unidades del equipo, así como en las unidades conectadas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.


El componente analiza los archivos a los que accede el usuario o la aplicación. Si se detecta un archivo malicioso, Kaspersky Endpoint Security bloquea la operación del archivo. A continuación, la aplicación desinfecta o elimina el archivo malicioso, en función de la configuración del componente Protección frente a amenazas en archivos.

Cuando se intenta acceder a un archivo cuyo contenido está almacenado en la nube de OneDrive, Kaspersky Endpoint Security descarga el contenido y lo analiza.

## Activación y desactivación de Protección frente a amenazas en archivos

De forma predeterminada, el componente Protección frente a amenazas en archivos está configurado en el modo recomendado por los expertos de Kaspersky. Para Protección frente a amenazas en archivos, Kaspersky Endpoint Security puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros que se almacenan en la aplicación se denominan *niveles de seguridad*: **Máximo**, **Recomendado**, **Mínimo**. Se considera que la configuración del nivel de seguridad **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky (vea la tabla abajo). Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración recomendada del nivel de seguridad.

*Para activar o desactivar el componente Protección frente a amenazas en archivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Utilice el interruptor **Protección frente a amenazas en archivos** para activar o desactivar el componente.
4. Si lo activó, realice una de las siguientes acciones en la sección **Nivel de seguridad**:
  - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
    - **Alta**. Si se selecciona este nivel de seguridad de archivos, el componente Protección frente a amenazas en archivos realiza el control más estricto de todos los archivos abiertos, guardados y ejecutados. El componente Protección frente a amenazas en archivos analiza todos los tipos de archivos en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. También analiza archivos comprimidos, paquetes de instalación y objetos OLE incrustados.
    - **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección frente a amenazas en archivos solo analiza los formatos de archivos especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo y en

los objetos de OLE incrustados. El componente Protección frente a amenazas en archivos no analiza los archivos ni los paquetes de instalación. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.

- **Baja.** La configuración de este nivel de seguridad de archivo garantiza la máxima velocidad de análisis. El componente Protección frente a amenazas en archivos solo analiza los archivos con extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. El componente Protección frente a amenazas en archivos no analiza los archivos compuestos.
  - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina su propia configuración del componente.
- Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Restaurar nivel de seguridad recomendado** en la parte superior de la ventana.

## 5. Guarde los cambios.

Configuración de Protección frente a amenazas en archivos recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

Parámetro	Valor	Descripción
<b>Tipos de archivos</b>	<b>Analizar archivos por formato</b>	Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.
<b>Análisis heurístico</b>	<b>Análisis superficial</b>	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.  Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
<b>Analizar solamente archivos nuevos y modificados</b>	<b>Activa</b>	Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.
<b>Tecnología iSwift</b>	<b>Activa</b>	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.
<b>Tecnología iChecker</b>	<b>Activa</b>	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).


<b>Analizar archivos en formatos de Microsoft Office</b>	<b>Activa</b>	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.
<b>Modo de análisis</b>	<b>Modo inteligente</b>	En este modo, Protección frente a amenazas en archivos analiza un objeto en función de un análisis de las acciones aplicadas al objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.
<b>Acción al detectar una amenaza</b>	<b>Desinfectar; eliminar si la desinfección falla</b>	Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.

## Suspensión automática de Protección frente a amenazas en archivos

Puede configurar la Protección frente a amenazas en archivos para que se suspenda de forma automática a una hora concreta o cuando utilice determinados programas.

La Protección frente a amenazas en archivos se debería suspender solo como último recurso cuando entra en conflicto con algunas aplicaciones. Si surge algún conflicto mientras se ejecuta un componente, se recomienda que se comunique con el [Soporte técnico de Kaspersky](#). Los expertos de soporte le ayudarán a configurar el componente de Protección frente a amenazas en archivos para que se ejecute simultáneamente con otras aplicaciones en su equipo.


*Para configurar la suspensión automática de la Protección frente a amenazas en archivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Pausar la Protección frente a amenazas en archivos**, haga clic en el enlace **Pausar la Protección frente a amenazas en archivos**.
5. En la ventana abierta, establezca la configuración para pausar la Protección frente a amenazas en archivos:
  - a. Configure una programación para pausar la Protección frente a amenazas en archivos automáticamente.
  - b. Cree una lista de aplicaciones cuyo funcionamiento debería hacer que la Protección frente a amenazas en archivos detenga sus actividades.
6. Guarde los cambios.

## Modificación de las acciones tomadas en archivos infectados por parte del componente Protección frente a amenazas en archivos

De forma predeterminada, el componente Protección frente a amenazas en archivos automáticamente intenta desinfectar todos los archivos infectados que se detecten. Si la desinfección falla, el componente Protección frente a amenazas en archivos elimina estos archivos.


*Para cambiar la acción realizada a los archivos infectados por el componente de Protección frente a amenazas en archivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. En el bloque **Acción al detectar una amenaza**, seleccione la opción correspondiente:
  - **Desinfectar; eliminar si la desinfección falla.** Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
  - **Desinfectar; bloquear si la desinfección falla.** Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección no es posible, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.
  - **Bloquear.** Si se selecciona esta opción, el componente Protección frente a amenazas en archivos automáticamente bloquea todos los archivos infectados sin intentar desinfectarlos.

Antes de intentar desinfectar o eliminar un archivo infectado, Kaspersky Endpoint Security crea una copia de seguridad del archivo en caso de que necesite [restaurarlo o que sea posible desinfectarlo en el futuro](#).

4. Guarde los cambios.

## Formación la cobertura de protección del componente Protección frente a amenazas en archivos

La cobertura de protección hace referencia a los objetos que analiza el componente cuando está activado. Las coberturas de protección de los distintos componentes tienen distintas propiedades. La ubicación y el tipo de archivos que se van a analizar son propiedades de la cobertura de protección del componente Protección frente a amenazas en archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza solo los [archivos potencialmente infectables](#)  ejecutados desde discos duros, unidades extraíbles y unidades de red.




Al seleccionar el tipo de archivos que vayan a analizarse, tenga en cuenta lo siguiente:

1. Hay una probabilidad baja de introducir código malicioso en archivos de determinados formatos y su posterior activación (por ejemplo, formato TXT). De igual modo, otros formatos de archivos contienen código ejecutable

(por ejemplo, .exe o .dll). El código ejecutable también puede estar contenido en formatos de archivo que no están destinados para este fin (por ejemplo, el formato DOC). Es elevado el riesgo de penetración y activación de código malicioso en estos archivos.

2. Un intruso puede enviar un virus u otra aplicación maliciosa a su equipo en un archivo ejecutable al que se ha cambiado el nombre con la extensión .txt. Si selecciona el análisis de archivos por extensión, la aplicación omitirá el archivo durante el análisis. Si se selecciona el análisis de archivos por formato, Kaspersky Endpoint Security analiza el encabezado del archivo sin importar su extensión. Si se determina que el archivo es de un formato ejecutable (por ejemplo, EXE), se lo somete a análisis.

*Para crear la Cobertura de protección:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Tipos de archivos**, especifique el tipo de archivo que desea que el componente Protección frente a amenazas en archivos analice:
  - **Todos los archivos**. Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones).
  - **Archivos analizados por formato**. Si se activa este parámetro, Kaspersky Endpoint Security analiza [únicamente los archivos infectables](#) . Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.
  - **Archivos analizados por extensión**. Si se activa este parámetro, Kaspersky Endpoint Security analiza [únicamente los archivos infectables](#) . El formato de archivo se determina en función de su extensión.
5. Haga clic en el enlace **Editar cobertura de protección**.
6. En la ventana abierta, seleccione los objetos que desea añadir a la cobertura de protección o excluir de ella.

No puede eliminar ni editar objetos que se incluyan en la cobertura de protección predeterminada.

7. Si desea añadir un nuevo objeto a la cobertura de protección:

- a. Haga clic en el botón **Añadir**.

Se abre el árbol de carpetas.

- b. Seleccione un objeto para añadir a la cobertura de protección.

Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en la cobertura del análisis. Para hacerlo, desactive la casilla de verificación junto al objeto.


8. Guarde los cambios.

## Uso de métodos de análisis

Kaspersky Endpoint Security usa una técnica de análisis llamada Aprendizaje automático y análisis de firmas. Durante el análisis de firmas, Kaspersky Endpoint Security equipara el objeto detectado con los registros en su base de datos. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.


Para aumentar la eficacia de la protección, puede usar el análisis heurístico. Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.

*Para configurar el uso del análisis heurístico en el funcionamiento del componente Protección frente a amenazas en archivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en el botón **Configuración avanzada**.
4. Si desea que la aplicación utilice un análisis heurístico para la protección frente a amenazas en archivos, seleccione la casilla **Análisis heurístico** en el bloque **Métodos de análisis**. A continuación, utilice el control deslizante para definir el análisis de nivel heurístico: **Análisis superficial**, **Análisis medio** o **Análisis avanzado**.
5. Guarde los cambios.

## Utilización de las tecnologías de análisis en el funcionamiento del componente Protección frente a amenazas en archivos

*Para configurar el uso de tecnologías de análisis en el funcionamiento del componente Protección frente a amenazas en archivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar para la protección frente a amenazas en archivos:
  - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.



- **Tecnología iChecker.** Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).


5. Guarde los cambios.

## Optimización del análisis de archivos

Puede optimizar el análisis de archivos realizado por el componente Protección frente a amenazas en archivos, lo que reduce el tiempo de análisis y aumenta la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede conseguir si analiza solamente los archivos nuevos y los que se hayan modificado desde el último análisis. Este modo se aplica tanto a archivos simples como a compuestos.

También puede [activar el uso de las tecnologías iChecker e iSwift](#), que optimizan la velocidad del análisis de archivos mediante la exclusión de archivos que no se han modificado desde el análisis más reciente.

*Para optimizar el análisis de archivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Optimización del análisis**, seleccione la casilla de verificación **Analizar solamente archivos nuevos y modificados**.
5. Guarde los cambios.


## Análisis de archivos compuestos

Una técnica común para ocultar virus y otro tipo de software malicioso (malware) consiste en implantarlos en archivos compuestos, como archivos comprimidos o bases de datos. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

El método empleado para procesar un archivo compuesto infectado (desinfección o eliminación) depende del tipo de este.

El componente Protección frente a amenazas en archivos desinfecta archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR y ICE, y elimina archivos con otros formatos (excepto bases de datos de correo).

*Para configurar el análisis de archivos compuestos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiera analizar: archivos de almacenamiento, paquete de distribución o archivos en formatos de Office.
5. Si el [análisis de solo archivos nuevos y modificados está desactivado](#), establezca la configuración para analizar cada tipo de archivo compuesto: analice todos los archivos de este tipo o solo los archivos nuevos.  
Si está activado el análisis de solo archivos nuevos y modificados, Kaspersky Endpoint Security analiza solo archivos nuevos y modificados de todos los tipos de archivos compuestos.
6. Establezca la configuración avanzada para el análisis de archivos compuestos.

- **No descomprimir archivos compuestos de gran tamaño.**

Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security no escanea archivos compuestos cuyo tamaño exceda el valor especificado.

Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.

Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

- **Extraer archivos compuestos en segundo plano.**

Si la casilla de verificación está seleccionada, Kaspersky Endpoint Security proporciona acceso a archivos compuestos cuyo tamaño sea superior al valor especificado antes de analizar estos archivos. En este caso, Kaspersky Endpoint Security extrae y analiza los archivos compuestos en segundo plano.

Kaspersky Endpoint Security proporciona acceso a archivos compuestos cuyo tamaño sea inferior a este valor solo después de extraer y analizar estos archivos.

Si la casilla de verificación no está seleccionada, Kaspersky Endpoint Security proporciona acceso a archivos compuestos solo después de extraer y analizar archivos de cualquier tamaño.

7. Guarde los cambios.

## Modificación del modo de análisis

*Modo de análisis* remite a la condición que activa el análisis de archivos por parte del componente Protección frente a amenazas en archivos. De forma predeterminada, Kaspersky Endpoint Security analiza archivos en modo inteligente. En este modo de análisis, el componente Protección frente a amenazas en archivos analiza las operaciones que el usuario o una aplicación en nombre del usuario (con la cuenta actual activa o una cuenta de usuario diferente) o el sistema operativo han realizado con un archivo. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office Word la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.

*Para modificar el modo de análisis de archivos:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en archivos**.

3. Haga clic en el botón **Configuración avanzada**.

4. En la sección **Modo de análisis**, seleccione el modo requerido:

- **Modo inteligente.** En este modo, Protección frente a amenazas en archivos analiza un objeto en función de un análisis de las acciones aplicadas al objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.
- **Durante el acceso y modificación.** En este modo, Protección frente a amenazas en archivos analiza objetos cuando se intenta abrirlos o modificarlos.
- **Durante el acceso.** En este modo, Protección frente a amenazas en archivos analiza objetos solo tras intentar abrirlos.
- **Durante la ejecución.** En este modo, Protección frente a amenazas en archivos solo analiza objetos tras intentar ejecutarlos.

5. Guarde los cambios.

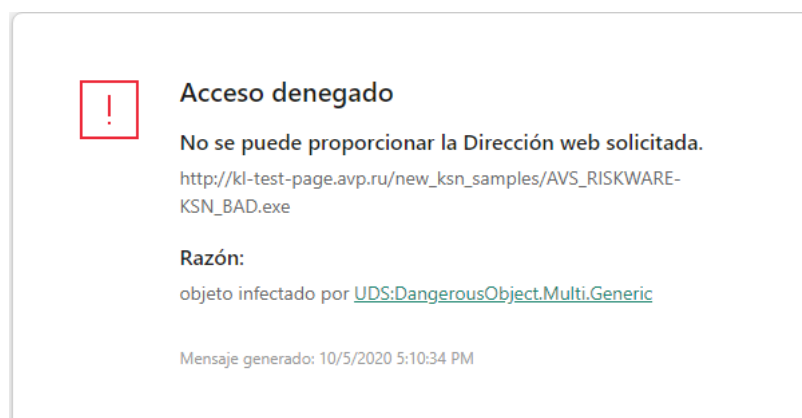
## Protección frente a amenazas web

El componente Protección frente a amenazas web evita la descarga de archivos maliciosos de Internet y también bloquea los sitios web maliciosos y de phishing. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

Kaspersky Endpoint Security analiza tráfico HTTP, HTTPS y FTP. Kaspersky Endpoint Security analiza direcciones IP y URLs. Puede [especificar los puertos que Kaspersky Endpoint Security supervisará](#) o seleccionar todos los puertos.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario [activar el análisis de conexiones cifradas](#).

Cuando un usuario intenta abrir un sitio web malicioso o de phishing, Kaspersky Endpoint Security bloqueará el acceso y le mostrará una advertencia (vea la imagen más abajo).




Mensaje de acceso al sitio web denegado

## Activación y desactivación de Protección frente a amenazas web

De forma predeterminada, el componente Protección frente a amenazas web está activado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para la Protección frente a amenazas web, Kaspersky Endpoint Security puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros que se almacenan en la aplicación se denominan *niveles de seguridad*: **Máximo**, **Recomendado**, **Mínimo**. Se considera que la configuración del nivel de seguridad para el tráfico web **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky (vea la tabla más abajo). Puede seleccionar uno de los niveles de seguridad preinstalados para el tráfico web que se recibe o se transmite a través de los protocolos HTTP y FTP, o configurar un nivel de seguridad del tráfico web personalizado. Si cambia la configuración del nivel de seguridad del tráfico web, siempre podrá volver a la configuración del nivel de seguridad recomendada del tráfico web.

*Para activar o desactivar el componente Protección frente a amenazas web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas web**.
3. Utilice el interruptor **Protección frente a amenazas web** para activar o desactivar el componente.
4. Si lo activó, realice una de las siguientes acciones en la sección **Nivel de seguridad**:
  - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
    - **Alta**. El nivel de seguridad en el que componente Protección frente a amenazas web realiza el máximo análisis del tráfico web que el equipo recibe a través de los protocolos HTTP y FTP. Protección frente a amenazas web analiza en detalle todos los objetos del tráfico web mediante todo el conjunto de bases de datos de la aplicación, y realiza el [análisis heurístico](#) más exhaustivo posible.
    - **Recomendado**. El nivel de seguridad que ofrece el equilibrio perfecto entre el rendimiento de Kaspersky Endpoint Security y la seguridad del tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.
    - **Baja**. La configuración de este nivel de seguridad de tráfico web garantiza el análisis más rápido de tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio.
  - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina su propia configuración del componente.

Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Restaurar nivel de seguridad recomendado** en la parte superior de la ventana.

5. Guarde los cambios.

Configuración de Protección frente a amenazas web recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)


Parámetro	Valor	Descripción
<b>Contrastar la dirección web con la base de datos de</b>	<b>Activa</b>	Al analizar los enlaces para determinar si están incluidos en la base de datos de direcciones web maliciosas, se le permite rastrear sitios web que hayan sido incluidos en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web maliciosas, que se incluye en el paquete

<b>direcciones web maliciosas</b>		de instalación de la aplicación y que se actualiza con las actualizaciones de la base de datos de Kaspersky Endpoint Security.
<b>Contrastar la dirección web con la base de datos de direcciones web de phishing</b>	<b>Activa</b>	La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.
<b>Usar análisis heurístico</b> (Protección frente a amenazas web)	<b>Análisis medio</b>	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.  Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.
<b>Usar análisis heurístico</b> (Anti-Phishing)	<b>Activa</b>	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.
<b>Acción al detectar una amenaza</b>	<b>Bloquear descarga</b>	Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.

## Modificación de las acciones que se van a realizar en objetos maliciosos del tráfico web

De forma predeterminada, al detectar un objeto infectado en el tráfico web, el componente Protección frente a amenazas web bloquea el acceso al objeto y muestra una notificación sobre la acción.

*Para cambiar la acción que se va a realizar en objetos maliciosos del tráfico web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas web**.
3. En la sección **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos del tráfico web:
  - **Bloquear descarga.** Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el

navegador.

- **Notificar.** Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, Kaspersky Endpoint Security permite que este objeto se descargue en el equipo, pero añade información sobre el objeto a la lista de amenazas activas.


4. Guarde los cambios.

## Análisis de URL contra bases de datos de phishing y direcciones web maliciosas

El análisis de enlaces para ver si están incluidos en la lista de direcciones web fraudulentas permite evitar *intentos de fraude*. Un intento de phishing se puede disfrazar, por ejemplo, como un mensaje de correo electrónico de su banco con un enlace al sitio web oficial del banco. Al hacer clic en el enlace, se abre una copia exacta del sitio web del banco e incluso puede ver la dirección real en el navegador, a pesar de que se trata de una imitación. A partir de este momento, todas sus acciones dentro del sitio son rastreadas y pueden servir para robarle su dinero.

Puesto que los enlaces a los sitios web phishing pueden recibirse no solo por correo electrónico, sino también por otros medios, como mensajes ICQ, el componente Protección frente a amenazas web supervisa los intentos de acceder a un sitio web phishing en el nivel de análisis del tráfico web y bloquea el acceso a esos sitios web. Las listas de direcciones fraudulentas se incluyen en el kit de distribución de Kaspersky Endpoint Security.

*Para configurar el componente Protección frente a amenazas web a fin de comprobar los enlaces con las bases de datos de direcciones phishing y maliciosas, haga lo siguiente:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas web**.
3. Haga clic en el botón **Configuración avanzada**.
4. Haga lo siguiente:
  - Si desea que el componente Protección frente a amenazas web compruebe los enlaces con las bases de datos de direcciones web maliciosas, en la sección **Métodos de análisis**, seleccione la casilla de verificación **Contrastar la dirección web con la base de datos de direcciones web maliciosas**. Al analizar los enlaces para determinar si están incluidos en la base de datos de direcciones web maliciosas, se le permite rastrear sitios web que hayan sido incluidos en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web maliciosas, que se incluye en el paquete de instalación de la aplicación y que se actualiza con las actualizaciones de la base de datos de Kaspersky Endpoint Security.

Kaspersky Endpoint analiza todos los enlaces para determinar si están incluidos en bases de datos de direcciones web maliciosas. La configuración del análisis de conexión segura de la aplicación no afecta la funcionalidad de análisis de enlaces. En otras palabras, si [el análisis de conexiones cifradas está desactivado](#), Kaspersky Endpoint Security verifica los enlaces con bases de datos de direcciones web maliciosas, aunque el tráfico de red se transmita a través de una conexión cifrada.

- Si desea que el componente Protección frente a amenazas web compruebe los enlaces con las bases de datos de direcciones web de phishing, seleccione la casilla de verificación **Contrastar la dirección web con la base de datos de direcciones web de phishing** en el bloque **Anti-Phishing**. La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean

para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.


También puede comprobar enlaces comparándolos con las bases de datos de reputación de [Kaspersky Security Network](#).

5. Guarde los cambios.

## Utilización del análisis heurístico en el funcionamiento del componente Protección frente a amenazas web

Para aumentar la eficacia de la protección, puede usar el análisis heurístico. Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones en el sistema operativo. El análisis heurístico puede detectar amenazas para las que no existen registros actualmente en las bases de datos de Kaspersky Endpoint Security.

*Para configurar el uso del análisis heurístico:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas web**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Métodos de análisis**, seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar el tráfico web en busca de virus y otros tipos de software malicioso. A continuación, utilice el control deslizante para definir el análisis de nivel heurístico: **Análisis superficial**, **Análisis medio** o **Análisis avanzado**.
5. En el bloque **Anti-Phishing**, seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al escanear páginas web en busca de enlaces de phishing.
6. Guarde los cambios.

## Creación de la lista de direcciones web de confianza

Puede crear una lista de direcciones URL en cuyo contenido confía. El componente Protección frente a amenazas web no analiza la información desde direcciones web de confianza en busca de virus u otras amenazas. Esta opción es útil, por ejemplo, cuando el componente Protección frente a amenazas web interfiere en la descarga de un archivo de un sitio web conocido.

Una dirección URL puede ser la dirección de una página web concreta o de la dirección de un sitio web.

*Para crear una lista de direcciones web de confianza:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas web**.
3. Haga clic en el botón **Configuración avanzada**.
4. Seleccione la casilla **No analizar tráfico web de URL de confianza**.  
Si se selecciona la casilla de verificación, el componente Protección frente a amenazas web no analiza el contenido de páginas o sitios web cuyas direcciones estén incluidas en la lista de direcciones web de confianza. Puede añadir a esta lista de direcciones web de confianza tanto direcciones específicas como máscaras de páginas o sitios web.
5. Cree una lista de direcciones URL/páginas web en cuyo contenido confíe.
6. Guarde los cambios.

## Exportación e importación de la lista de direcciones web de confianza

Puede exportar la lista de direcciones web de confianza a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir gran cantidad de direcciones web del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de direcciones web de confianza o para migrar la lista a un servidor diferente.

[Cómo exportar e importar una lista de direcciones web de confianza en la Consola de administración \(MMC\)](#) 



1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas web**.
6. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
7. En la ventana que se abre, seleccione la pestaña **Direcciones web de confianza**.
8. Para exportar la lista de direcciones web de confianza:
  - a. Seleccione las direcciones web de confianza que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.  
Si no seleccionó ninguna dirección web de confianza, Kaspersky Endpoint Security exportará todas las direcciones web.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de direcciones web de confianza y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de direcciones web de confianza al archivo XML.
9. Para importar la lista de direcciones de confianza:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que importar la lista de direcciones de confianza.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de direcciones de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
10. Guarde los cambios.

[Cómo exportar e importar una lista de direcciones web de confianza en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas básicas** → **Protección frente a amenazas web**.
5. Para exportar la lista de exclusiones en el bloque **Direcciones web de confianza**:
  - a. Seleccione las direcciones web de confianza que desea exportar.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de direcciones web de confianza y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de direcciones web de confianza al archivo XML.
6. Para importar una lista de exclusiones en el bloque **Direcciones web de confianza**:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que importar la lista de direcciones de confianza.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de direcciones de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
7. Guarde los cambios.

## Protección frente a amenazas en el correo

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

Protección frente a amenazas en el correo puede analizar tanto los mensajes entrantes como los salientes. La aplicación es compatible con POP3, SMTP, IMAP y NNTP en los siguientes clientes de correo:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Microsoft Outlook Express
- Windows Mail

Protección frente a amenazas en el correo no es compatible con otros protocolos y clientes de correo.

Es posible que Protección frente a amenazas en el correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, Protección frente a amenazas en el correo incluye una [extensión para Microsoft Office Outlook](#). La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección frente a amenazas en el correo es compatible con operaciones con Outlook 2010, 2013, 2016 y 2019.


El componente Protección frente a amenazas en el correo no analiza los mensajes si el programa de correo se abre en un navegador.

Cuando se detecta un archivo malicioso en un adjunto, Kaspersky Endpoint Security modifica el nombre del asunto del mensaje a: [El mensaje necesita su participación en el procesamiento] <asunto del mensaje> o [Se ha procesado el mensaje] <asunto del mensaje>.

## Activación y desactivación de Protección frente a amenazas en el correo

De forma predeterminada, el componente Protección frente a amenazas en el correo está activado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para Protección frente a amenazas en el correo, Kaspersky Endpoint Security aplica diferentes grupos de ajustes. Estos grupos de parámetros que se almacenan en la aplicación se denominan *niveles de seguridad*: **Máximo**, **Recomendado**, **Mínimo**. Se considera que la configuración del nivel de seguridad de correo **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky (vea la tabla más abajo). Puede seleccionar uno de los niveles de seguridad del correo electrónico preinstalados o configurar un nivel de seguridad del correo electrónico personalizado. Si ha cambiado la configuración del nivel de seguridad del correo, siempre puede volver a la configuración recomendada del nivel de seguridad del correo.

*Para activar o desactivar el componente Protección frente a amenazas en el correo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
3. Utilice el interruptor **Protección frente a amenazas en el correo** para activar o desactivar el componente.
4. Si lo activó, realice una de las siguientes acciones en el bloque **Nivel de seguridad**:
  - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
    - **Máximo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo analiza los mensajes más exhaustivamente. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico avanzado. El nivel de seguridad de correo Máximo se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo electrónico gratuito desde una red doméstica sin protección centralizada del correo electrónico.
    - **Recomendado**. El nivel de seguridad de correo electrónico que proporciona el equilibrio perfecto entre el rendimiento de Kaspersky Endpoint Security y la seguridad del correo electrónico. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico de correo. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.

- **Mínimo.** Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo solamente analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza archivos adjuntos en mensajes de correo electrónico. Con este nivel de seguridad, el componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico a una velocidad máxima y con un uso mínimo de recursos del sistema operativo. Se recomienda el nivel de seguridad de correo Mínimo para su uso en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una LAN empresarial con protección centralizada del correo electrónico.
- Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y defina su propia configuración del componente.

Puede restaurar los valores de los niveles de seguridad preestablecidos haciendo clic en el botón **Restaurar nivel de seguridad recomendado** en la parte superior de la ventana.

## 5. Guarde los cambios.

Configuración de Protección frente a amenazas en el correo recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)


Parámetro	Valor	Descripción
<b>Cobertura de protección</b>	<b>Mensajes entrantes y salientes</b>	<p>La <i>Cobertura de protección</i> incluye objetos que el componente comprueba cuando se ejecuta: Mensajes entrantes y salientes o Solo mensajes entrantes.</p> <p>Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar que los archivos infectados se envíen en archivos. También puede activar el análisis de mensajes salientes si desea evitar que se envíen archivos en formatos particulares, como archivos de audio y vídeo, por ejemplo.</p>
<b>Conectar el complemento de Microsoft Outlook</b>	<b>Activa</b>	<p>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.</p> <p>Si el correo se analiza usando la extensión para Microsoft Outlook, se recomienda usar el modo caché de Exchange. Para información más detallada sobre el Modo caché de Exchange y recomendaciones sobre su uso, consulte la <a href="#">Base de conocimientos de Microsoft</a>.</p>
<b>Analizar archivos adjuntos</b>	<b>Activa</b>	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo.
<b>Analizar archivos adjuntos con formatos de Microsoft Office</b>	<b>Activa</b>	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.
<b>Filtrado de adjuntos</b>	<b>Renombrar los adjuntos de los tipos seleccionados</b>	Si se selecciona esta opción, el componente Protección frente a amenazas en el correo cambia el último carácter de la extensión en archivos adjuntos de los tipos especificados con el símbolo de barra baja (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.
<b>Análisis heurístico</b>	<b>Análisis medio</b>	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.

		<p>Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.</p>
<p><b>Acción al detectar una amenaza</b></p>	<p><b>Desinfectar; eliminar si la desinfección falla</b></p>	<p>Cuando se detecta un objeto infectado en un mensaje entrante o saliente, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security eliminará el objeto infectado. Kaspersky Endpoint Security añade información sobre la acción realizada al asunto del mensaje: [Se ha procesado el mensaje] &lt;asunto del mensaje&gt;.</p>

## Modificación de las acciones que se van a realizar en mensajes de correo electrónico infectados

De forma predeterminada, el componente Protección frente a amenazas en el correo automáticamente intenta desinfectar todos los mensajes de correo electrónico infectados que se detecten. Si la desinfección falla, el componente Protección frente a amenazas en el correo elimina los mensajes de correo infectados.

*Para cambiar la acción que se debe realizar con los mensajes de correo electrónico infectados:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
3. En el bloque **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security cuando se detecta un mensaje infectado.
  - **Desinfectar; eliminar si la desinfección falla.** Cuando se detecta un objeto infectado en un mensaje entrante o saliente, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security eliminará el objeto infectado. Kaspersky Endpoint Security añade información sobre la acción realizada al asunto del mensaje: [Se ha procesado el mensaje] <asunto del mensaje>.
  - **Desinfectar; bloquear si falla la desinfección.** Cuando se detecta un objeto infectado en un mensaje entrante, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security añade una advertencia al asunto del mensaje: [El mensaje necesita su participación en el procesamiento] <asunto del mensaje>. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, Kaspersky Endpoint Security intenta desinfectar el objeto. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.
  - **Bloquear.** Si se detecta un objeto infectado en un mensaje entrante, Kaspersky Endpoint Security añade una advertencia al asunto del mensaje: [El mensaje necesita su participación en el procesamiento] <asunto del mensaje>. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, Kaspersky Endpoint Security bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.

4. Guarde los cambios.

## Formación la cobertura de protección del componente de Protección frente a amenazas en el correo

La *cobertura de protección* hace referencia a los objetos que son analizados por el componente cuando este está activo. Las coberturas de protección de los distintos componentes tienen distintas propiedades. Las propiedades de la cobertura de protección del componente Protección frente a amenazas en el correo incluyen los parámetros para integrarlo en clientes de correo, así como el tipo de mensajes de correo electrónico y los protocolos de correo electrónico cuyo tráfico analiza este componente. De forma predeterminada, Kaspersky Endpoint Security analiza los mensajes de correo entrante y saliente, así como el tráfico, a través de los protocolos POP3, SMTP, NNTP e IMAP, y se integra en los clientes de correo electrónico Microsoft Office Outlook.

*Para formar la cobertura de protección del componente de Protección frente a amenazas en el correo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Cobertura del análisis**, 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 que los archivos infectados se envíen en archivos. También puede activar el análisis de mensajes salientes si desea evitar que se envíen archivos en formatos particulares, como archivos de audio y vídeo, por ejemplo.

Si elige analizar solo los mensajes entrantes, recomendamos que lleve a cabo un único análisis de todos los mensajes salientes, ya que existe la posibilidad de que su equipo tenga gusanos del correo electrónico que se distribuyan por correo. Esto ayuda a evitar problemas provocados por un envío masivo e incontrolado por correo electrónico de mensajes infectados desde su equipo.

5. En la sección **Conectividad**, haga lo siguiente:
  - Si quiere que el componente Protección frente a amenazas en el correo analice los mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que el equipo del usuario los reciba, active la casilla de verificación **Analizar tráfico POP3, SMTP, NNTP e IMAP**.
  - Si no quiere que el componente Protección frente a amenazas en el correo analice los mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen al equipo del usuario, desactive la casilla de verificación **Analizar tráfico POP3, SMTP, NNTP e IMAP**. En este caso, los mensajes son analizados por la extensión de la Protección frente a amenazas en el correo incorporada al cliente de correo de Microsoft Office Outlook después de que llegan al equipo del usuario si se selecciona la casilla de verificación **Conectar el complemento de Microsoft Outlook**.

Si utiliza un cliente de correo que no sea Microsoft Office Outlook, el componente Protección frente a amenazas en el correo no analiza los mensajes que se transmiten a través de los protocolos POP3, SMTP, NNTP e IMAP cuando la casilla de verificación **Analizar tráfico POP3, SMTP, NNTP e IMAP** está desactivada.

- Si desea permitir el acceso a la configuración del componente Protección frente a amenazas en el correo desde Microsoft Office Outlook y activar el análisis de los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que llegan al equipo utilizando la extensión incorporada a Microsoft Office Outlook, seleccione la casilla de verificación **Conectar el complemento de Microsoft Outlook**.

Si desea bloquear el acceso a la configuración del componente Protección frente a amenazas de correo desde Microsoft Office Outlook y no desea que los mensajes transmitidos por POP3, SMTP, NNTP, IMAP y MAPI se analicen con la extensión para Microsoft Office Outlook una vez que estén en el equipo, desactive la casilla de verificación **Conectar el complemento de Microsoft Outlook**.

La extensión Protección frente a amenazas en el correo se integra en el programa de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

6. Guarde los cambios.

## Analizar archivos compuestos adjuntos a mensajes de correo electrónico

Puede activar o desactivar el análisis de adjuntos del mensaje, limitar el tamaño máximo de los adjuntos de los mensajes para su análisis y limitar la duración máxima del análisis del adjunto del mensaje.

*Para configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Análisis de archivos compuestos**, establezca la configuración del análisis:
  - **Analizar archivos adjuntos de formatos Microsoft Office**. Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.
  - **Analizar archivos adjuntos**. Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo.

Si durante el análisis, Kaspersky Endpoint Security detecta la contraseña de un archivo comprimido en el cuerpo del mensaje, la utilizará para buscar aplicaciones maliciosas en el contenido del archivo. La contraseña no se guarda. El archivo comprimido se descomprime antes del análisis. Si se produce un error de la aplicación al descomprimir, puede eliminar de forma manual los archivos descomprimidos, que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tendrán el prefijo PR.

- **No analizar archivos comprimidos mayores de N MB.** Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en el correo excluye del análisis los archivos adjuntos de los mensajes de correo electrónico si su tamaño supera el valor especificado. Si se desactiva la casilla de verificación, el componente Protección frente a amenazas en el correo analiza archivos adjuntos de cualquier tamaño.
- **Limitar el tiempo de comprobación de archivos a N segundos.** Si se selecciona la casilla de verificación, el tiempo asignado para analizar los archivos adjuntos a los mensajes de correo electrónico se limita al período especificado.


5. Guarde los cambios.

## Filtro de archivos adjuntos de mensajes de correo electrónico

El filtro de archivos adjuntos no se aplica a los mensajes de correo electrónico salientes.

Las aplicaciones maliciosas se pueden distribuir en forma de adjuntos del correo electrónico. Puede configurar el filtrado según el tipo de adjuntos del mensaje de modo que los archivos de los tipos especificados se renombran o eliminan automáticamente. Al volver a asignar un nombre a un tipo determinado de adjunto, Kaspersky Endpoint Security es capaz de proteger su equipo contra la ejecución automática de una aplicación maliciosa.

*Para configurar el filtrado de archivos adjuntos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Filtrado de adjuntos**, lleve a cabo una de las siguientes acciones:
  - **Desactivar el filtrado.** Si se selecciona esta opción, el componente Protección frente a amenazas en el correo no filtra archivos que están adjuntos a mensajes de correo electrónico.
  - **Renombrar los adjuntos de los tipos seleccionados.** Si se selecciona esta opción, el componente Protección frente a amenazas en el correo cambia el último carácter de la extensión en archivos adjuntos de los tipos especificados con el símbolo de barra baja (por ejemplo, adjunto.doc\_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.
  - **Eliminar los adjuntos de los tipos seleccionados.** Si se selecciona esta opción, el componente Protección frente a amenazas en el correo elimina los archivos adjuntos de los tipos especificados.
5. Si seleccionó la opción **Renombrar los adjuntos de los tipos seleccionados** o **Eliminar los adjuntos de los tipos seleccionados** durante el paso anterior, seleccione las casillas situadas junto a los tipos de archivos pertinentes.
6. Guarde los cambios.



## Exportación e importación de extensiones para filtrado de adjuntos

Puede exportar la lista de extensiones de filtro de archivos adjuntos a un archivo XML. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de extensiones o para migrar la lista a un servidor diferente.

### [Cómo exportar e importar una lista de extensiones de filtro de archivos adjuntos en la Consola de administración \(MMC\)](#)<sup>2</sup>

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
6. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
7. En la ventana que se abre, seleccione la pestaña **Filtrado de adjuntos**.
8. Para exportar la lista de extensiones:
  - a. Seleccione las extensiones que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de extensiones y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de extensiones al archivo XML.
9. Para importar la lista de extensiones:
  - a. Haga clic en el enlace **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de extensiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de extensiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
10. Guarde los cambios.



1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
5. Para exportar la lista de extensiones en el bloque de **Filtrado de adjuntos**:
  - a. Seleccione las extensiones que desea exportar.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de extensiones y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de extensiones al archivo XML.
6. Para importar la lista de extensiones en el bloque de **Filtrado de adjuntos**:
  - a. Haga clic en el enlace **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de extensiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de extensiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
7. Guarde los cambios.

## Análisis de correos electrónicos en Microsoft Office Outlook

Durante la instalación de Kaspersky Endpoint Security, la extensión Protección frente a amenazas en el correo se incrusta en Microsoft Office Outlook (en adelante, también denominado Outlook). Le permite abrir la configuración del componente Protección frente a amenazas en el correo desde Outlook y especificar en qué momento desea que se analicen los mensajes de correo electrónico en busca de virus y otras amenazas. La extensión Protección frente a amenazas en el correo para Outlook puede analizar los mensajes entrantes y salientes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI. Kaspersky Endpoint Security también admite trabajar con otros clientes de correo electrónico (incluidos Microsoft Outlook Express®, Windows Mail y Mozilla™ Thunderbird™).

La extensión Protección frente a amenazas en el correo es compatible con operaciones con Outlook 2010, 2013, 2016 y 2019.

Al trabajar con el cliente de correo electrónico Mozilla Thunderbird, si se utilizan filtros para mover mensajes fuera de la carpeta Bandeja de entrada, el componente Protección frente a amenazas en el correo no analiza en busca de virus y otras amenazas los mensajes de correo electrónico transmitidos mediante el protocolo IMAP.

En Outlook, los mensajes entrantes de correo electrónico se analizan primero con el componente Protección frente a amenazas en el correo (seleccionando la casilla de verificación [Analizar tráfico POP3, SMTP, NNTP e IMAP](#) en la interfaz de Kaspersky Endpoint Security) y, a continuación, con la extensión Protección frente a amenazas en el correo para Outlook. Si el componente Protección frente a amenazas en el correo detecta un objeto malicioso en un mensaje, le alerta sobre ello.

La configuración del componente Protección frente a amenazas en el correo se puede definir directamente en Outlook si la [extensión para Microsoft Office Outlook está conectada](#) en la interfaz de Kaspersky Endpoint Security.

Los mensajes salientes son analizados primero por la extensión Protección frente a amenazas en el correo para Outlook y, a continuación, los analiza el componente Protección frente a amenazas en el correo.

Si el correo se mediante la extensión Protección frente a amenazas en el correo para Outlook, se recomienda utilizar el modo caché de Exchange. 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 Protección frente a amenazas en el correo para Outlook con Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en el correo**.
6. En el bloque **Nivel de seguridad**, haga clic en el botón **Configuración**.
7. En la sección **Conectividad**, haga clic en **Configuración**.
8. En la ventana **Protección del correo**, haga lo siguiente:
  - Seleccione la casilla de verificación **Analizar al recibir** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes entrantes cuando lleguen al buzón de correo.
  - Seleccione la casilla de verificación **Analizar al abrir** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes entrantes cuando el usuario los abra.
  - Seleccione la casilla de verificación **Analizar al enviar** si desea que la extensión de Protección frente a amenazas en el correo para Outlook analice los mensajes salientes cuando se envían.
9. Guarde los cambios.


## Protección frente a amenazas en la red

El componente Protección frente a amenazas en la red analiza el tráfico de red entrante en busca de actividad habitual en los ataques de red. Cuando Kaspersky Endpoint Security detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante. Las bases de datos de Kaspersky Endpoint Security ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos. La lista de ataques de red que detecta el componente Protección frente a amenazas en la red se actualiza durante [las actualizaciones de módulos de aplicaciones y bases de datos](#).

## Activación y desactivación de Protección frente a amenazas en la red

De forma predeterminada, Protección frente a amenazas en la red está activado y funcionando en modo óptimo. Puede desactivar Protección frente a amenazas en la red si fuera necesario.


*Para activar o desactivar Protección frente a amenazas en la red:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en la red**.
3. Utilice el interruptor **Protección frente a amenazas en la red** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si la Protección frente a amenazas en la red está activada, Kaspersky Endpoint Security analiza el tráfico de red entrante en busca de actividad típica de los ataques de red. Cuando Kaspersky Endpoint Security detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante.

## Bloquear un equipo atacante

*Para bloquear un equipo atacante:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en la red**.
3. Seleccione la casilla **Añadir un equipo atacante a la lista de equipos bloqueados durante N minutos**.

Si se selecciona la casilla de verificación, el componente Protección frente a amenazas en la red añade al equipo atacante a la lista de bloqueados. Esto quiere decir que el componente Protección frente a amenazas en la red bloquea la conexión de red del equipo atacante después del primer intento de ataque de red durante el período de tiempo especificado. Este bloqueo protege automáticamente al equipo del usuario frente a posibles ataques de red desde la misma dirección en el futuro.

El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 32 768 minutos.

Puede ver la lista de rechazados en la ventana de la [herramienta Monitor de red](#).

Kaspersky Endpoint Security borra la lista de rechazados al reiniciar la aplicación y cuando se cambian los ajustes de Protección frente a amenazas en la red.


1. Establezca una duración de bloqueo diferente para un equipo atacante en el campo a la derecha de la casilla **Añadir un equipo atacante a la lista de equipos bloqueados durante N minutos**.
2. Guarde los cambios.

Como resultado, cuando Kaspersky Endpoint Security detecta un intento de ataque de red contra el equipo del usuario, bloqueará todas las conexiones de red con el equipo atacante.

## Configurar direcciones de exclusiones de bloqueo

Kaspersky Endpoint Security puede reconocer un ataque de red y bloquear una conexión de red no segura que transmita una gran cantidad de paquetes (por ejemplo, desde cámaras de vigilancia). Para trabajar con dispositivos de confianza, puede añadir las direcciones IP de estos dispositivos a la lista de exclusiones.

*Para configurar direcciones de exclusiones de bloqueo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en la red**.
3. Haga clic en el enlace **Administrar exclusiones**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. Introduzca la dirección IP del equipo desde el que no se deben bloquear los ataques de red.
6. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security no rastrea la actividad de los dispositivos en la lista de exclusiones.

## Exportación e importación de la lista de exclusiones de bloqueo

Puede exportar la lista de exclusiones a un archivo XML. Luego puede modificar el archivo para, por ejemplo, añadir una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

[Cómo exportar e importar una lista de exclusiones en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en la red**.
6. En el bloque **Parámetros de Protección frente a amenazas en la red**, haga clic en el botón **Exclusiones**.
7. 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 enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
8. Para importar la lista de exclusiones:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
9. 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 **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas básicas** → **Protección frente a amenazas en la red**.
5. En el bloque **Parámetros de Protección frente a amenazas en la red**, haga clic en el enlace **Exclusiones**.  
Se abre la lista de exclusiones.
6. Para exportar la lista de reglas:
  - a. Seleccione las exclusiones que desea exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las exclusiones seleccionadas o exportar la lista completa de exclusiones.
  - d. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - e. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
7. Para importar la lista de exclusiones:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.

## Configurar la protección contra ataques a la red por tipo

Kaspersky Endpoint Security le permite administrar la protección contra los siguientes tipos de ataques a la red:

- *Inundación de redes* es un ataque a los recursos de red de una organización (como servidores web). Este ataque consiste en enviar una gran cantidad de solicitudes para sobrecargar el ancho de banda de los recursos de la red. Cuando esto sucede, los usuarios no pueden acceder a los recursos de red de la organización.
- Un ataque de tipo *"Port scan"* consiste en el escaneo de puertos UDP, TCP, puertos y servicios de red en el equipo. Este ataque permite al atacante identificar el grado de vulnerabilidad del equipo antes de realizar tipos


de ataques de red más peligrosos. Los ataques de tipo "Port scan" también permiten al atacante identificar el sistema operativo en el equipo y seleccionar los ataques de red apropiados para este sistema operativo.

- Los *ataques de spoofing de MAC* consisten en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Como resultado, un atacante puede redirigir los datos enviados a un dispositivo a otro dispositivo y obtener acceso a esos datos. Kaspersky Endpoint Security le permite saber si se detecta uno de estos ataques y bloquearlo.

Puede activar la detección de este tipo de ataques en caso de que algunas de sus aplicaciones permitidas realicen operaciones típicas de este tipo de ataques. Esto ayudará a evitar falsas alarmas.

De forma predeterminada, Kaspersky Endpoint Security no supervisa los ataques de inundación de red, ataques de tipo "Port scan" y spoofing de MAC.

*Para configurar la protección contra ataques a la red por tipo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección frente a amenazas en la red**.
3. Utilice el interruptor **Tratar el análisis de puerto y el desbordamiento de red como ataques** para activar o desactivar la detección de estos ataques.
4. Utilice el interruptor **Protección contra spoofing de MAC**.
5. En el bloque **Al detectar un ataque de spoofing de MAC**, seleccione una de las siguientes opciones:
  - **Solo notificar.**
  - **Notificar y bloquear.**
6. Guarde los cambios.

## Firewall

Firewall bloquea las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local. Firewall también controla la actividad de red de las aplicaciones en el equipo. Esto le permite proteger su red de área local corporativa del robo de identidad y otros ataques. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. De forma automática, el firewall crea las reglas de red necesarias para que funcionen la aplicación y el Agente de red. Como resultado, el firewall abre varios puertos en el ordenador. Los puertos se abren según la función del ordenador (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en el ordenador, consulte la [Ayuda de Kaspersky Security Center](#).

## Reglas de red

Puede configurar las reglas de la red en los siguientes niveles:



- *Reglas de paquetes de red.* Las reglas de paquetes de red imponen restricciones a los paquetes de red, con independencia de la aplicación. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security tiene reglas de paquetes de red predefinidas con permisos recomendados por los expertos de Kaspersky.
- *Reglas de red de la aplicación.* Las reglas de red de la aplicación imponen restricciones sobre la actividad de red de una aplicación concreta. No solo influyen en las características del paquete de red, sino también en la aplicación concreta a la que va dirigida la aplicación concreta o que emitió este paquete de red.

El componente [Prevención de intrusiones en el host](#) proporciona el acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de *derechos de aplicación*.

Durante el primer inicio de la aplicación, Firewall realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

Se le recomienda [participar en Kaspersky Security Network](#) para ayudar a Firewall a trabajar con más eficacia.

3. Coloca la aplicación en uno de los *grupos de confianza*: De confianza/Restricción mínima/Restricción máxima/No confiable.

Los [grupos de confianza definen los derechos](#) que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la [configuración del componente Prevención de intrusiones en el host](#). Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea la actividad de red de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega el uso de cualquier conexión de red.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

## Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más alta sea la posición de una regla en la lista, mayor prioridad tendrá. Si se añade actividad de red a varias reglas, Firewall regula la actividad de red en función de la regla con la prioridad más alta.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si tanto las reglas de paquetes de red como las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se gestiona de acuerdo con las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan de la siguiente manera: una regla de red para aplicaciones incluye reglas de acceso basadas en el estado de la red: *publica*, *local* o *de confianza*. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega cualquier actividad de red en redes de cualquier estado de forma predeterminada. Si se especifica una regla de red para una aplicación individual (aplicación principal), los subprocesos de otras aplicaciones se ejecutarán de acuerdo con la regla de red de la aplicación principal. Si no hay una regla de red para la aplicación, los subprocesos se ejecutarán de acuerdo con la regla de acceso a la red del grupo de confianza de la aplicación.

Por ejemplo, ha prohibido cualquier actividad de red en redes de todos los estados para todas las aplicaciones, excepto el navegador X. Si inicia la instalación del navegador Y (subproceso) desde el navegador X (aplicación principal), el instalador del navegador Y accederá a la red y descargará los archivos necesarios. Después de la instalación, se negarán las conexiones de red al navegador Y de acuerdo con la configuración del Firewall. Para prohibir la actividad de red del instalador del navegador Y como un subproceso, debe asignar una regla de red para el instalador del navegador Y.

## Estados de conexión de red

Firewall le permite controlar la actividad de la red en función del estado de la conexión de red. Kaspersky Endpoint Security recibe el estado de conexión de red del sistema operativo del equipo. El estado de la conexión de red en el sistema operativo lo establece el usuario al configurar la conexión. Puede [cambiar el estado de la conexión de red en la configuración de Kaspersky Endpoint Security](#). Firewall supervisará la actividad de la red en función del estado de la red en la configuración de Kaspersky Endpoint Security, y no en del sistema operativo.

La conexión de red puede tener uno de los siguientes tipos de estado:

- **Red pública.** La red no está protegida por aplicaciones antivirus, firewalls ni filtros (como la red wifi de una cafetería). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos mediante carpetas compartidas y acceso remoto al escritorio de este equipo. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.


Firewall asigna el estado *Red pública* a Internet de forma predeterminada. No se puede cambiar el estado de Internet.

- **Red local.** Red para usuarios con acceso restringido a archivos e impresoras en este equipo (como una red de área local corporativa o red doméstica).
- **Red de confianza.** Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.

## Activación y desactivación de Firewall

De forma predeterminada, Firewall está activado y las opciones en el modo óptimo.

*Para activar y desactivar el Firewall:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Utilice el interruptor **Firewall** para activar o desactivar el componente.
4. Guarde los cambios.


Como resultado, si se activa el Firewall, Kaspersky Endpoint Security controla la actividad de la red y bloquea las conexiones de red no autorizadas a su ordenador, y también bloquea la actividad de red no autorizada de las aplicaciones en su ordenador. El [componente Protección frente a amenazas en la red](#) también controla la actividad de red. El componente Protección frente a amenazas en la red analiza el tráfico de red entrante en busca de actividad habitual en los ataques de red.

Kaspersky Endpoint Security registra los eventos de ataques de red en sus informes, independientemente de la configuración del Firewall. Incluso si el Firewall bloquea la conexión de red utilizando reglas para así evitar un ataque de red, el componente Protección frente a amenazas en la red registra los eventos de ataque de red. Esto es necesario para generar información estadística acerca de los ataques de red en los ordenadores de su organización.

## Modificación del estado de la conexión de red

Firewall asigna el estado *Red pública* a Internet de forma predeterminada. No se puede cambiar el estado de Internet.

*Para cambiar el estado de la conexión de red:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Redes disponibles**.
4. Seleccione la conexión de red cuyo estado quiere cambiar.
5. En la columna **Tipo de red**, seleccione el estado de la conexión de red:
  - **Red pública.** La red no está protegida por aplicaciones antivirus, firewalls ni filtros (como la red wifi de una cafetería). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos mediante carpetas compartidas y acceso remoto al escritorio de este equipo. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.
  - **Red local.** Red para usuarios con acceso restringido a archivos e impresoras en este equipo (como una red de área local corporativa o red doméstica).
  - **Red de confianza.** Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.
6. Guarde los cambios.

## Gestión de las reglas de paquetes de red

Puede realizar las siguientes acciones mientras gestiona las reglas de paquetes de red:

- Crear una nueva regla de paquetes de red.

Puede crear una nueva regla de paquetes de red mediante la creación de un conjunto de condiciones y acciones que se aplican a los paquetes de red y los flujos de datos.

- Activar o desactivar una regla de paquetes de red.

Todas las reglas de paquetes de red creadas por Firewall tienen el estado *Activado* de forma predeterminada. Cuando una regla de paquetes de red está activada, Firewall aplica esta regla.

Puede desactivar cualquier regla de paquetes de red que esté seleccionada en la lista de reglas de paquetes de red. Cuando una regla de paquetes de red está desactivada, Firewall deja de aplicar temporalmente esta regla.

Con el estado *Activado*, se añade de forma predeterminada una nueva regla de paquetes de red personalizada a la lista de reglas de paquetes de red.

- Modificar los parámetros de una regla de paquetes de red ya existente.

Tras crear una nueva regla de paquetes de red, siempre puede volver a modificar sus parámetros y modificarlos si es necesario.

- Cambiar la acción de Firewall para una regla de paquetes de red.

En la lista de reglas de paquetes de red, puede modificar la acción que Firewall realiza para detectar la actividad de red que cumple con una regla de paquetes de red concreta.

- Cambiar la prioridad de una regla de paquetes de red.

Puede incrementar o reducir la prioridad de una regla de paquetes de red que esté seleccionada en la lista.

- Eliminar una regla de paquetes de red.

Puede eliminar una regla de paquetes de red para que Firewall deje de aplicar esta regla cuando detecte actividad de red y para que esta regla no se muestre en la lista de reglas de paquetes de red con el estado *Desactivado*.

## Crear una regla de paquetes de red

Puede crear una regla de paquetes de red de las siguientes maneras:

- Utilice la [herramienta Monitor de red](#).

*Monitor de red* es una herramienta diseñada para la visualización de información sobre la actividad de la red del equipo de un usuario en tiempo real. Esto es conveniente porque no es necesario configurar todos los parámetros de las reglas. Algunos parámetros del Firewall se insertarán automáticamente a partir de los datos del Monitor de red. El Monitor de red está disponible solo en la interfaz de la aplicación.

- Configure los parámetros del Firewall.

Esto le permite ajustar la configuración del Firewall. Puede crear reglas para cualquier actividad de la red, aunque no haya actividad de red en el momento dado.

Al crear reglas de paquetes de red, recuerde que estas tienen prioridad sobre las reglas para aplicaciones.

[Cómo utilizar la herramienta Monitor de red para crear una regla de paquete de red en la interfaz de la aplicación](#) 

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.
2. Seleccione la pestaña **Actividad de red**.

La pestaña **Actividad de red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes.
3. En el menú contextual de una conexión de red, seleccione **Cree una regla de paquete para la red**.


Se abren las propiedades de la regla de red.
4. Configure el estado **Activo** para la regla del paquete.
5. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
6. Configure los parámetros de la regla de red (consulte la tabla a continuación).

Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.


Toda la configuración de la regla de red se completará automáticamente.
7. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
8. Haga clic en el botón **Guardar**.

La nueva regla de red se añadirá a la lista.
9. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
10. Guarde los cambios.

[Cómo usar la configuración del Firewall para crear una regla de paquetes de red en la interfaz de la aplicación](#) 

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Reglas para paquetes**.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
4. Haga clic en el botón **Añadir**.  
Se abren las propiedades de la regla de red.
5. Configure el estado **Activo** para la regla del paquete.
6. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.
8. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
9. Haga clic en el botón **Guardar**.  
La nueva regla de red se añadirá a la lista.
10. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
11. Guarde los cambios.

[Cómo crear una regla de paquetes de red en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Firewall**.
6. En la sección **Configuración del Firewall**, haga clic en el botón **Configuración**.  
Se abre la lista de reglas de paquetes de red y la lista de reglas de red de la aplicación.
7. Seleccione la pestaña **Reglas de paquetes de red**.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
8. Haga clic en el botón **Añadir**.  
Esto abre las propiedades de la regla del paquete.
9. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
10. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el botón . Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.
11. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
12. Guarde la nueva regla de red.
13. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
14. Guarde los cambios.

El Firewall controlará los paquetes de red de acuerdo con la regla. Puede desactivar una regla de paquete de la operación del Firewall sin eliminarla de la lista. Para hacerlo, desactive la casilla de verificación junto al objeto.

[Cómo crear una regla de paquetes de red en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Protección frente a amenazas básicas** → **Firewall**.
5. En el bloque **Configuración del Firewall**, haga clic en el enlace **Reglas de paquetes de red**.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
6. Haga clic en el botón **Añadir**.  
Esto abre las propiedades de la regla del paquete.
7. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
8. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Seleccionar plantilla**. Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.
9. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
10. Guarde la nueva regla de red.  
La nueva regla de red se añadirá a la lista.
11. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
12. Guarde los cambios.

El Firewall controlará los paquetes de red de acuerdo con la regla. Puede desactivar una regla de paquete de la operación del Firewall sin eliminarla de la lista. Utilice el interruptor de la columna **Estado** para activar o desactivar la regla de paquetes.

Configuración de reglas de paquetes de red


Parámetro	Descripción
<b>Acción</b>	<p><b>Autorizar.</b></p> <p><b>Bloquear.</b></p> <p><b>Según reglas de la aplicación.</b> Si se selecciona esta opción, Firewall aplica las <a href="#">reglas de red de la aplicación</a> a la conexión de red.</p>
<b>Protocolo</b>	<p>Controle la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE.</p> <p>Si se seleccionan ICMP o ICMPv6 como el protocolo, puede definir el código y el tipo de paquete ICMP.</p> <p>Si se selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto delimitados por comas de los equipos local y remoto entre los que se debe supervisar la conexión:</p>



<b>Dirección</b>	<p><b>Entrante (paquete).</b> El Firewall aplica la regla de red a todos los paquetes de red entrantes.</p> <p><b>Entrante.</b> Firewall aplica la regla de red a todos los paquetes de red enviados por medio de una conexión iniciada por un equipo remoto.</p> <p><b>Entrante/Saliente.</b> Firewall aplica la regla de red a los paquetes de red tanto de entrada como de salida, independientemente de si la conexión de red se ha iniciado por el equipo del usuario o por un equipo remoto.</p> <p><b>Saliente (paquete).</b> El Firewall aplica la regla de red a todos los paquetes de red salientes.</p> <p><b>Saliente.</b> El Firewall aplica la regla de red a todos los paquetes de red enviados mediante una conexión de red iniciada por el equipo del usuario.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>El protocolo TCP establece una conexión. Para TCP, utilice las direcciones <b>Entrante, Saliente y Entrante/Saliente</b>. Todos los demás protocolos no establecen conexiones, pero envían paquetes. Para todos los demás protocolos, utilice las direcciones <b>Entrante (paquete), Saliente (paquete) y Entrante/Saliente</b>.</p> </div>
<b>Adaptadores de red</b>	<p>Adaptadores de red que pueden enviar o recibir paquetes de red. Especificar la configuración de los adaptadores de red permite distinguir entre los paquetes de red enviados o recibidos por los adaptadores de red con direcciones IP idénticas.</p>
<b>Período de vida (TTL)</b>	<p>Restrinja el control de los paquetes de red según su período de vida (TTL).</p>
<b>Dirección remota</b>	<p>Direcciones de red de los equipos remotos que puedan enviar y recibir paquetes de red. El Firewall aplica una regla de red al rango especificado de direcciones de la red remota. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP, especificar un rango de direcciones IP o seleccionar una subred (redes de confianza, redes locales, redes públicas). También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web.</p>
<b>Dirección local</b>	<p>Direcciones de red de los equipos que puedan enviar o recibir paquetes de red. Firewall aplica una regla de la red al rango especificado de direcciones de red local. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP o especificar un rango de direcciones IP. También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>En ocasiones, la dirección local no se puede obtener para las aplicaciones. Si este es el caso, este parámetro se ignora.</p> </div>

## Activación o desactivación de una regla de paquetes de red

*Para activar o desactivar una regla de paquetes de red:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.

3. Haga clic en el botón **Reglas para paquetes**.

Esto abre una lista de reglas de paquetes de red predeterminadas, definidas por el componente Firewall.

4. Seleccione la regla de los paquetes de red pertinente en la lista.

5. Utilice el interruptor en la columna **Estado** para activar o desactivar la regla.

6. Guarde los cambios.

## Modificación de la acción de Firewall para una regla de paquetes de red

*Para cambiar la acción de Firewall que se aplica a una regla de paquetes de red:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.

3. Haga clic en el botón **Reglas para paquetes**.

Esto abre una lista de reglas de paquetes de red predeterminadas, definidas por el componente Firewall.

4. Selecciónela en la lista de reglas de paquetes de red y haga clic en el botón **Editar**.

5. En la lista desplegable **Acción**, seleccione la acción que debe realizar Firewall cuando detecte este tipo de actividad de red:

- **Autorizar.**
- **Bloquear.**
- **Según reglas de la aplicación.** Si se selecciona esta opción, Firewall aplica las [reglas de red de la aplicación](#) a la conexión de red.

6. Guarde los cambios.


## Modificación de la prioridad de una regla de paquetes de red

La prioridad de una regla de paquetes de red viene determinada por su posición en la lista de reglas de paquetes de red. La regla de paquetes de red situada más arriba en la lista de reglas de paquetes de red tiene la máxima prioridad.

Cada una de las reglas de paquetes de red creadas manualmente se añade al final de la lista de reglas de paquetes de red y tienen la menor prioridad.

Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba abajo. En función de cada una de las reglas de paquetes de red procesadas que se aplican a una determinada conexión de red, Firewall permite o bloquea el acceso de red a la dirección y al puerto especificados en la configuración de esta conexión de red.

*Para modificar la prioridad de la regla de paquetes de red:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Reglas para paquetes**.  
Esto abre una lista de reglas de paquetes de red predeterminadas, definidas por el componente Firewall.
4. En la lista, seleccione la regla de paquetes de red cuya prioridad quiere cambiar.
5. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
6. Guarde los cambios.

## Exportación e importación de reglas de paquetes de red

Puede exportar la lista de reglas de paquetes de red a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de reglas del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de paquetes de red o para migrar la lista a un servidor diferente.

[Cómo exportar e importar una lista de reglas de paquetes de red en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Firewall**.
6. En la sección **Configuración del Firewall**, haga clic en el botón **Configuración**.  
Se abre la lista de reglas de paquetes de red y la lista de reglas de red de la aplicación.
7. Seleccione la pestaña **Reglas de paquetes de red**.
8. Para exportar la lista de reglas de paquetes de red:
  - a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.  
Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.
9. Para importar una lista de reglas de paquetes de red:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
10. 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 **Dispositivos** → **Directivas y perfiles**.
2. 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 **Protección frente a amenazas básicas** → **Firewall**.
5. Haga clic en el enlace **Reglas de paquetes de red**.
6. Para exportar la lista de reglas de paquetes de red:
  - a. Seleccione las reglas que quiera exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las reglas seleccionadas o exportar la lista completa.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas a un archivo XML en la carpeta de descargas predeterminada.
7. Para importar una lista de reglas de paquetes de red:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.

## Gestionar reglas de red de la aplicación

De forma predeterminada, Kaspersky Endpoint Security agrupa todas las aplicaciones que están instaladas en el equipo por el nombre del proveedor del software cuyo archivo o actividad de red monitoriza. Los grupos de aplicaciones, a su vez, se clasifican en [grupos de confianza](#). Todas las aplicaciones y grupos de aplicaciones heredan las propiedades de su grupo principal: reglas de control de aplicaciones, reglas de red de la aplicación y su prioridad de ejecución.

Al igual que el componente de [Prevención de intrusiones en el host](#), el componente Firewall aplica de forma predeterminada las reglas de red para un grupo de aplicaciones cuando filtra la actividad de red de todas las aplicaciones del grupo. El grupo de aplicaciones define los derechos de las aplicaciones dentro del grupo a acceder a diferentes conexiones de red.

De forma predeterminada, Firewall crea un conjunto de reglas de red para cada grupo de aplicaciones que Kaspersky Endpoint Security detecta en el equipo. Puede cambiar la acción que Firewall aplica a las reglas de red del grupo de aplicaciones que se crean de forma predeterminada. No puede modificar, eliminar, desactivar o cambiar la prioridad de las reglas de red del grupo de aplicaciones que se crean de forma predeterminada.

También puede crear una regla de red para una aplicación individual. Tal regla tendrá una prioridad más alta que la regla de red del grupo al cual la aplicación pertenece.

## Crear una regla de red de aplicaciones

De manera predeterminada, la actividad de las aplicaciones se controlada a través de reglas de red definidas para el [grupo de confianza](#) al que Kaspersky Endpoint Security asignó la aplicación en el primer inicio. Si es necesario, puede crear reglas de red para un grupo de confianza completo, para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza.

Las reglas de red definidas manualmente tienen una prioridad más alta que las reglas de red que se determinaron para un grupo de confianza. En otras palabras, si las reglas de aplicación definidas manualmente difieren de las reglas de aplicación determinadas para un grupo de confianza, el Firewall controla la actividad de la aplicación de acuerdo con las reglas definidas en forma manual para las aplicaciones.

De forma predeterminada, el Firewall crea las siguientes reglas de red para cada aplicación:

- Cualquier actividad de red en redes de confianza.
- Cualquier actividad de red en redes locales.
- Cualquier actividad de red en redes públicas.

Kaspersky Endpoint Security controla la actividad de red de las aplicaciones de acuerdo con las reglas de red predefinidas de la siguiente manera:

- Fiable y Restricción mínima: se permite toda la actividad de red.
- Restricción máxima y No fiable: toda la actividad de la red está bloqueada.

Las reglas de aplicación predefinidas no se pueden editar ni eliminar.

Puede crear una regla de red para aplicación de las siguientes formas:

- Utilice la [herramienta Monitor de red](#).

*Monitor de red* es una herramienta diseñada para la visualización de información sobre la actividad de la red del equipo de un usuario en tiempo real. Esto es conveniente porque no es necesario configurar todos los parámetros de las reglas. Algunos parámetros del Firewall se insertarán automáticamente a partir de los datos del Monitor de red. El Monitor de red está disponible solo en la interfaz de la aplicación.

- Configure los parámetros del Firewall.


Esto le permite ajustar la configuración del Firewall. Puede crear reglas para cualquier actividad de la red, aunque no haya actividad de red en el momento dado.

Al crear reglas de red para aplicaciones, recuerde que las reglas de paquetes de red tienen prioridad sobre las reglas de red de la aplicación.

## [Cómo utilizar la herramienta Monitor de red para crear una regla de red para aplicación en la interfaz de la aplicación](#)


1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.
2. Seleccione la pestaña **Actividad de red** o **Abrir puertos**.  
La pestaña **Actividad de red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes.  
La pestaña **Abrir puertos** muestra todos los puertos de red abiertos del equipo.
3. En el menú contextual de una conexión de red, seleccione **Crear una regla de red para la aplicación**.  
Se abre la ventana de propiedades y reglas de la aplicación.
4. Seleccione la pestaña **Reglas de red**.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
5. Haga clic en el botón **Añadir**.  
Se abren las propiedades de la regla de red.
6. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.
8. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
9. Haga clic en el botón **Guardar**.  
La nueva regla de red se añadirá a la lista.
10. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
11. Guarde los cambios.

## [Cómo utilizar la configuración del Firewall para crear una regla de red para aplicación en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Reglas para aplicaciones**.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere crear una regla de red.
5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.  
Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la pestaña **Reglas de red**.
7. Haga clic en el botón **Añadir**.  
Se abren las propiedades de la regla de red.
8. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
9. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.
10. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
11. Haga clic en el botón **Guardar**.  
La nueva regla de red se añadirá a la lista.
12. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
13. Guarde los cambios.

[Cómo crear una regla de red para aplicación en la Consola de administración \(MMC\)](#) 



1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas básicas** → **Firewall**.
6. En la sección **Configuración del Firewall**, haga clic en el botón **Configuración**.  
Se abre la lista de reglas de paquetes de red y la lista de reglas de red de la aplicación.
7. Seleccione la pestaña **Reglas de red de la aplicación**.
8. Haga clic en el botón **Añadir**.
9. En la ventana abierta, introduzca los criterios de búsqueda para la aplicación para la que quiera crear una regla de red.  
Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres \* y ? al introducir una máscara.
10. Haga clic en el botón **Actualizar**.  
Kaspersky Endpoint Security buscará la aplicación en la lista consolidada de aplicaciones instaladas en equipos administrados. Kaspersky Endpoint Security mostrará una lista de aplicaciones que coincidan con sus criterios de búsqueda.
11. Seleccione la aplicación pertinente.
12. En la lista desplegable **Añadir aplicaciones seleccionadas al grupo de confianza**, seleccione **Grupos predeterminados** y haga clic en **Aceptar**.  
La aplicación se añadirá al grupo predeterminado.
13. Seleccione la aplicación correspondiente y luego seleccione **Derechos de la aplicación** en el menú contextual de la aplicación.  
Se abre la ventana de propiedades y reglas de la aplicación.
14. Seleccione la pestaña **Reglas de red**.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
15. Haga clic en el botón **Añadir**.  
Se abren las propiedades de la regla de red.
16. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
17. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el botón . Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.

18. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
19. Guarde la nueva regla de red.
20. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
21. Guarde los cambios.

[Cómo crear una regla de red para aplicación en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Protección frente a amenazas básicas** → **Firewall**.
5. En el bloque **Configuración del Firewall**, haga clic en el enlace **Reglas de red de la aplicación**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
6. Seleccione la pestaña **Derechos de la aplicación**.  
Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.
7. Haga clic en el botón **Añadir**.  
Se inicia el Asistente para añadir una aplicación a un grupo de confianza.
8. Seleccione el grupo de confianza correspondiente para la aplicación.
9. Seleccione el tipo de **aplicación**. Haga clic en **Siguiente**.  
Si desea crear una regla de red para varias aplicaciones, seleccione el tipo **Grupo** y defina un nombre para el grupo de aplicaciones.
10. En la lista de aplicaciones abiertas, seleccione las aplicaciones para las que quiere crear una regla de red.  
Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres \* y ? al introducir una máscara.
11. Haga clic en **Aceptar** para finalizar el Asistente.  
La aplicación se añadirá al grupo de confianza.
12. En la parte izquierda de la ventana, seleccione la aplicación relevante.
13. En la parte derecha de la ventana, seleccione **Reglas de red** en la lista desplegable.  
Se abre una lista de reglas de red predeterminadas, definidas por el componente Firewall.
14. Haga clic en el botón **Añadir**.  
Se abren las propiedades de la regla de aplicaciones.
15. Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.
16. Configure los parámetros de la regla de red (consulte la tabla a continuación).  
Puede seleccionar una plantilla de regla predeterminada haciendo clic en el enlace **Seleccionar plantilla**.  
Las plantillas de reglas describen las conexiones de red más utilizadas.  
Toda la configuración de la regla de red se completará automáticamente.
17. Si desea que las acciones de la regla de red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
18. Guarde la nueva regla de red.

La nueva regla de red se añadirá a la lista.

19. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.


20. Guarde los cambios.

#### Configuración de la regla de red de aplicaciones

Parámetro	Descripción
<b>Acción</b>	<b>Autorizar.</b> <b>Bloquear.</b>
<b>Protocolo</b>	Controle la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE.  Si se seleccionan ICMP o ICMPv6 como el protocolo, puede definir el código y el tipo de paquete ICMP.  Si se selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto delimitados por comas de los equipos local y remoto entre los que se debe supervisar la conexión:
<b>Dirección</b>	<b>Entrante.</b> <b>Entrante/Saliente.</b> <b>Saliente.</b>
<b>Dirección remota</b>	Direcciones de red de los equipos remotos que puedan enviar y recibir paquetes de red. El Firewall aplica una regla de red al rango especificado de direcciones de la red remota. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP, especificar un rango de direcciones IP o seleccionar una subred (redes de confianza, redes locales, redes públicas). También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web.
<b>Dirección local</b>	Direcciones de red de los equipos que puedan enviar o recibir paquetes de red. Firewall aplica una regla de la red al rango especificado de direcciones de red local. Puede incluir todas las direcciones IP en una regla de red, crear una lista independiente de direcciones IP o especificar un rango de direcciones IP. También puede especificar un nombre DNS de un equipo en lugar de su dirección IP. Debe usar nombres DNS solo para equipos LAN o servicios internos. La interacción con los servicios de nube (como Microsoft Azure) y otros recursos de Internet debe ser manejada por el componente Control Web.  <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">En ocasiones, la dirección local no se puede obtener para las aplicaciones. Si este es el caso, este parámetro se ignora.</div>

## Activar y desactivar una regla de red de la aplicación

*Para activar o desactivar una regla de red de la aplicación:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.

3. Haga clic en el botón **Reglas para aplicaciones**.  
Esto abre la lista de reglas de la aplicación.
4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere crear o editar una regla de red.
5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.  
Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la pestaña **Reglas de red**.
7. En la lista de reglas de red para un grupo de aplicaciones, seleccione la regla de red pertinente.  
Se abre la ventana de propiedades de la regla de red.
8. Configure el estado **Activo** o **Inactivo** de la regla de red.  
No puede desactivar una regla de red del grupo de aplicaciones que Firewall haya creado de forma predeterminada.
9. Guarde los cambios.


## Modificación de la acción de Firewall para una regla de red de la aplicación

Puede cambiar la acción de Firewall que se aplica a las reglas de red para una aplicación o grupo de aplicaciones creado de forma predeterminada y cambiar la acción de Firewall por una única regla de red del grupo de aplicaciones personalizada.

*Para cambiar la acción del Firewall sobre todas las reglas de red para una aplicación o grupo de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Reglas para aplicaciones**.  
Esto abre la lista de reglas de la aplicación.
4. Si desea cambiar la acción del Firewall que se aplica a todas las reglas de red que se crean de forma predeterminada, seleccione una aplicación o grupo de aplicaciones de la lista. Las reglas de red creadas manualmente no se cambian.
5. Haga clic derecho para abrir el menú contextual, seleccione **Reglas de red** y luego seleccione la acción que desea asignar:
  - **Heredar.**
  - **Autorizar.**
  - **Bloquear.**
6. Guarde los cambios.

*Para cambiar la respuesta de Firewall para las reglas de red de una aplicación o un grupo de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Reglas para aplicaciones**.  
Esto abre la lista de reglas de la aplicación.
4. En la lista, seleccione la aplicación o el grupo de aplicaciones para las cuales desea cambiar la acción para una regla de red.
5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.  
Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la pestaña **Reglas de red**.
7. Seleccione la regla de red para la cual desea cambiar la acción del Firewall.
8. En la columna **Permiso**, haga clic con el botón derecho para acceder al menú contextual y seleccione la acción que quiere asignar:
  - **Heredar**.
  - **Autorizar**.
  - **Denegar**.
  - **Registrar eventos**.
9. Guarde los cambios.


## Modificación de la prioridad de una regla de red de la aplicación

La prioridad de una regla de red depende de su posición en la lista de reglas. Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de red, de arriba abajo. En función de cada una de las reglas de red aplicables a una determinada conexión de red, Firewall permite o bloquea el acceso a la red a la dirección y al puerto indicados en la configuración de esta conexión de red.

Las reglas de red creadas manualmente tienen una prioridad más alta que las reglas de red predeterminadas.

No puede cambiar la prioridad de las reglas de red del grupo de aplicaciones que se crean de forma predeterminada.

*Para cambiar la prioridad de una regla de red:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Firewall**.
3. Haga clic en el botón **Reglas para aplicaciones**.  
Esto abre la lista de reglas de la aplicación.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere cambiar la prioridad de una regla de red.
5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Detalles y reglas**.  
Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la pestaña **Reglas de red**.
7. Seleccione la conexión de red cuya prioridad quiera cambiar.
8. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de red.
9. Guarde los cambios.

## Monitor de red

*Monitor de red* es una herramienta diseñada para la visualización de información sobre la actividad de la red del equipo de un usuario en tiempo real.

*Para iniciar el Monitor de red:*

En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Monitor de red**.

Se abre la ventana Monitor de red. En esta ventana, se muestra información sobre la actividad de red del equipo en cuatro pestañas:

- La pestaña **Actividad de red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes. En esta pestaña, también puede [crear reglas de paquetes de red](#) para el funcionamiento del Firewall.
- La pestaña **Abrir puertos** muestra todos los puertos de red abiertos del equipo. En esta pestaña, también puede [crear reglas de paquetes de red](#) y [reglas de aplicación](#) para el funcionamiento del Firewall.
- La pestaña **Tráfico de red** muestra el volumen de tráfico de red entrante y saliente entre el equipo del usuario y otros equipos de la red a los que el usuario está conectado actualmente.
- La pestaña **Equipos bloqueados** incluye las direcciones IP de los equipos remotos cuya actividad de red ha bloqueado el componente Protección frente a amenazas en la red después de detectar intentos de ataques de red desde dichas direcciones IP.

## Prevención de ataques de BadUSB

Algunos virus modifican el firmware de los dispositivos USB para engañar al sistema operativo y que detecte el dispositivo USB y lo identifique como teclado. Como resultado, el virus puede ejecutar comandos en su cuenta de usuario para descargar software malicioso, por ejemplo.

El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.

Cuando un dispositivo USB se conecta al equipo y el sistema operativo lo identifica como un teclado, la aplicación solicita al usuario que introduzca desde este teclado un código numérico generado por la aplicación, o bien que utilice el [teclado en pantalla si está disponible](#) (vea la figura a continuación). Este procedimiento se conoce como autorización del teclado.

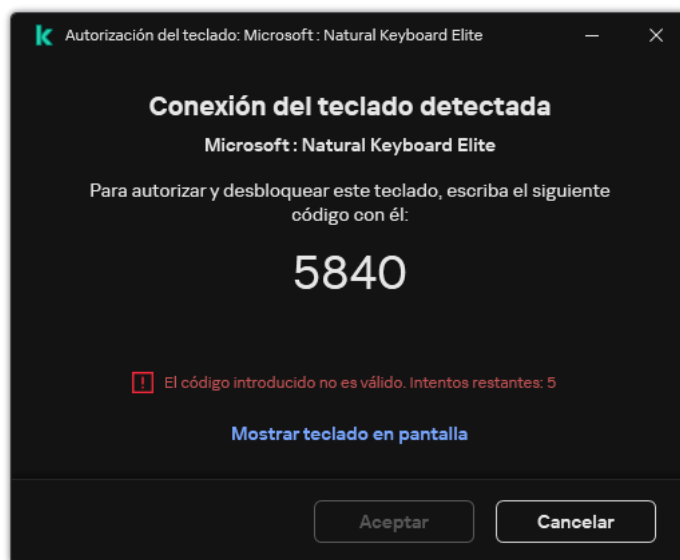
Si se ha introducido el código correctamente, la aplicación guarda los parámetros de identificación (los VID y PID del teclado y el número del puerto al cual se ha conectado) en la lista de teclados autorizados. No será necesario volver a realizar la autorización del teclado cuando se vuelva a conectar el teclado o después de que se reinicie el sistema operativo.

Si el teclado autorizado se conecta al equipo a través de un puerto USB diferente, la aplicación volverá a mostrar la solicitud de autorización.

Si se introduce el código numérico de forma incorrecta, la aplicación generará un nuevo código. Puede [configurar el número de intentos para introducir el código numérico](#). Si el código numérico se introduce de forma incorrecta muchas veces o si se cierra la ventana de autorización del teclado (ver la figura a continuación), la aplicación bloquea las acciones de ese teclado. Cuando se cumple el período de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación solicita al usuario que realice de nuevo el procedimiento de autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea los teclados que no se hayan autorizado.

El componente Prevención de ataques de BadUSB no se instala de forma predeterminada. Si necesita el componente Prevención de ataques de BadUSB, puede añadir el componente a las propiedades del [paquete de instalación](#) antes de instalar la aplicación o [cambiar sus componentes disponibles](#) después de instalarla.




*Autorización del teclado*

## Activación y desactivación de Prevención de ataques de BadUSB

Los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente Prevención de ataques de BadUSB se considerarán autorizados después de la instalación del componente.



*Para activar o desactivar Prevención de ataques de BadUSB:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Prevención de ataques de BadUSB**.
3. Utilice el interruptor **Prevención de ataques de BadUSB** para activar o desactivar el componente.
4. En **Autorización del teclado USB al conectarse**, ajuste la configuración de seguridad para introducir el código de autorización:
  - **Número máximo de intentos de autorización del dispositivo.** Bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite 5 intentos para introducir el código de autorización, el dispositivo USB se bloquea después del quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este período, puede tener 5 intentos para introducir el código de autorización.
  - **Tiempo de espera al alcanzar el número máximo de intentos.** Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos para introducir el código de autorización. Los valores válidos son de 1 a 180 (minutos).
5. Guarde los cambios.

Como resultado, si Prevención de ataques de BadUSB está activado, Kaspersky Endpoint Security requiere la autorización de un dispositivo USB conectado identificado como un teclado por el sistema operativo. El usuario no podrá usar un teclado no autorizado hasta que se autorice.

## Usar el teclado en pantalla para la autorización de dispositivos USB

El teclado en pantalla solo se debe utilizar para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (p.ej., escáneres de códigos de barras). No se recomienda usar el teclado en pantalla para la autorización de dispositivos USB desconocidos.

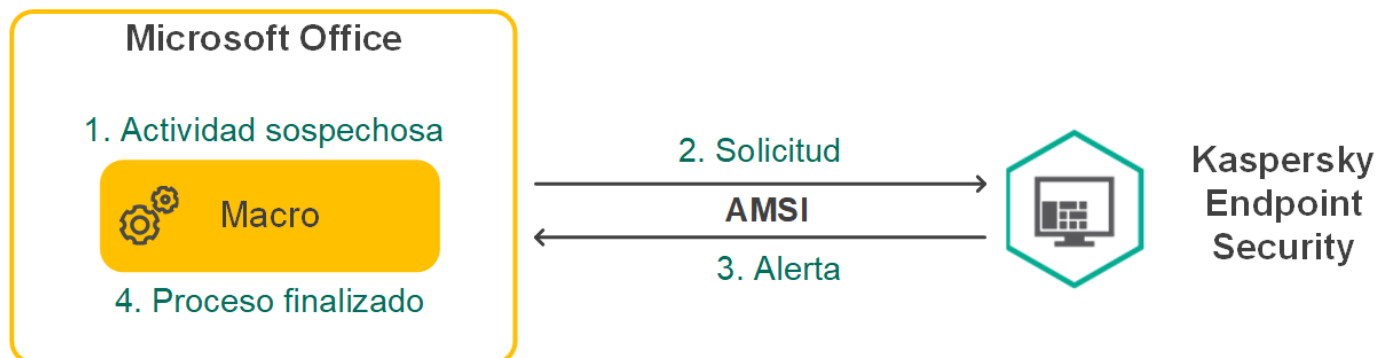
*Para permitir o prohibir el uso del teclado en pantalla para la autorización:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Prevención de ataques de BadUSB**.
3. Utilice la casilla de verificación **Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB** a fin de permitir o bloquear el uso del teclado en pantalla para la autorización.
4. Guarde los cambios.

## Protección AMSI

El componente de protección AMSI está diseñado para ser compatible con 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 más detalles sobre AMSI, consulte la [documentación de Microsoft](#).

La protección AMSI únicamente puede detectar una amenaza y notificar a una aplicación de terceros sobre dicha amenaza detectada. La aplicación de terceros, después de recibir una notificación de una amenaza, no permite realizar acciones maliciosas (por ejemplo, finaliza su proceso).



Ejemplo del funcionamiento de AMSI

El componente de protección AMSI puede rechazar una solicitud de una aplicación de terceros si, por ejemplo, esta aplicación sobrepasa el número máximo de solicitudes dentro de un intervalo específico. Cuando esto ocurre, Kaspersky Endpoint Security envía información al respecto al Servidor de administración. El componente Protección AMSI no rechaza las solicitudes de aquellas aplicaciones de terceros para las cuales la [integración continua con el componente de protección AMSI](#) está activada.


La protección AMSI está disponible para los siguientes sistemas operativos para estaciones de trabajo y servidores:

- Windows 10 Home/Pro/Pro for Workstations/Education/Enterprise;
- Windows 11;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter;
- Windows Server 2022.

## Activación y desactivación de la protección AMSI

De manera predeterminada, el componente de protección AMSI está activado.

*Para activar o desactivar la protección AMSI:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección AMSI**.


3. Utilice el interruptor **Protección AMSI** para activar o desactivar el componente.

4. Guarde los cambios.

## Uso de la protección AMSI para analizar archivos compuestos

Una técnica común para ocultar virus u otro malware es incorporarlo en archivos compuestos, como archivos de almacenamiento. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

*Para configurar el análisis de protección AMSI para archivos compuestos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas básicas** → **Protección AMSI**.
3. En la sección **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiera analizar: archivos de almacenamiento, paquete de distribución o archivos en formatos de Office.
4. En el bloque **Límite de tamaño**, lleve a cabo una de las siguientes acciones:
  - Para que el componente de protección AMSI no descomprima archivos compuestos de gran tamaño, active la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**, y especifique el valor que considere apropiado en el campo **Tamaño máximo de archivo**. El componente de protección AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.
  - Para permitir que el componente de protección AMSI descomprima archivos compuestos de gran tamaño, desactive la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

El componente de protección AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No descomprimir archivos compuestos de gran tamaño** está activada.

5. Guarde los cambios.


## Prevención de exploits

El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malicioso. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

## Activación y desactivación de Prevención de vulnerabilidades

De forma predeterminada, Prevención de exploits está activado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar Prevención de exploits.

*Para activar o desactivar la Prevención de exploits:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de exploits**.
3. Utilice el interruptor **Prevención de exploits** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si la Prevención de exploits está activada, Kaspersky Endpoint Security supervisará los archivos ejecutables ejecutados por aplicaciones vulnerables. Si Kaspersky Endpoint Security detecta que se ha ejecutado un archivo ejecutable desde una aplicación vulnerable por otra persona distinta del usuario, Kaspersky Endpoint Security realizará la acción seleccionada (por ejemplo, bloqueará la operación).

## Selección de la acción que se realizará al detectar una vulnerabilidad

De forma predeterminada, al detectar una vulnerabilidad, Kaspersky Endpoint Security bloquea el funcionamiento que intenta llevar a cabo la vulnerabilidad.


*Para elegir la acción que se realizará al detectarse una vulnerabilidad:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de exploits**.
3. Seleccione la acción correspondiente en el bloque **Al detectar vulnerabilidades**:
  - **Bloquear operación**. Si este elemento está seleccionado, al detectar una vulnerabilidad de seguridad, Kaspersky Endpoint Security bloquea el funcionamiento de la vulnerabilidad y crea una entrada de registro con información relevante.
  - **Notificar**. Si este elemento está seleccionado, cuando Kaspersky Endpoint Security detecte una vulnerabilidad registrará un evento que contenga información sobre la vulnerabilidad y añadirá información sobre esta vulnerabilidad a [la lista de amenazas activas](#).
4. Guarde los cambios.

## Protección de la memoria de los procesos del sistema

De forma predeterminada, la protección de la memoria de procesos del sistema está activada.

*Para activar o desactivar la protección de memoria de procesos del sistema:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de exploits**.
3. Utilice el interruptor **Activar protección de la memoria de los procesos del sistema** para activar o desactivar esta función.
4. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security bloqueará los procesos externos que intenten acceder a los procesos del sistema.

## Detección de comportamiento


El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones de su equipo y ofrece esta información a otros componentes de protección mejorar su rendimiento. El componente Detección de comportamientos utiliza firmas de patrones de actividad peligrosa (Behavior stream signatures, BSS) para aplicaciones. Si la actividad de la aplicación coincide con una BSS Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security basada en bases de datos de reglas heurísticas ofrece protección proactiva al equipo.

## Activar y desactivar Detección de comportamiento

De forma predeterminada, la Detección de comportamiento está activada y se ejecuta en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar la Detección de comportamiento.

No se recomienda desactivar la Detección de Comportamiento a menos que sea absolutamente necesario porque reduce la eficacia de los componentes de protección. Los componentes de protección pueden solicitar datos obtenidos por el componente Detección de comportamiento para detectar amenazas.


*Para activar o desactivar la Detección de comportamiento:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Detección de comportamiento**.
3. Utilice el interruptor **Detección de comportamiento** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si la Detección de comportamiento está activada, Kaspersky Endpoint Security utilizará firmas de flujo de comportamiento para analizar la actividad de las aplicaciones en el sistema operativo.

## Selección de la acción que se debe tomar al detectar actividad de malware

*A fin de elegir qué hacer si una aplicación participa en actividades maliciosas, realice los pasos siguientes:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Detección de comportamiento**.
3. Seleccione la acción correspondiente en el bloque **Al detectar actividad de software malicioso**:
  - **Eliminar el archivo**. Si este elemento está seleccionado, al detectar actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.
  - **Finalizar la aplicación**. Si se selecciona este elemento, al detectar una actividad maliciosa, Kaspersky Endpoint Security termina la aplicación.
  - **Notificar**. Si este elemento está seleccionado y se detecta actividad de malware, Kaspersky Endpoint Security añade información sobre la actividad maliciosa de la aplicación a la lista de amenazas activas.
4. Guarde los cambios.

## Protección de carpetas compartidas frente a cifrado externo

El componente solo supervisa operaciones con los archivos ubicados en dispositivos de almacenamiento con el sistema de archivos NTFS y que no están cifrados con el sistema EFS.

La función Protección de las carpetas compartidas frente a cifrado externo proporciona el análisis de actividad en carpetas compartidas. Si esta actividad coincide con un tipo de comportamiento típico del cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.


De forma predeterminada, la protección de carpetas compartidas contra el cifrado externo está desactivada.

Después de instalar Kaspersky Endpoint Security, la protección de carpetas compartidas contra el cifrado externo estará limitada hasta que el equipo se reinicie.

## Activación y desactivación de la protección de carpetas compartidas frente al cifrado externo

Después de instalar Kaspersky Endpoint Security, la protección de carpetas compartidas contra el cifrado externo estará limitada hasta que el equipo se reinicie.

*Para activar o desactivar la protección de carpetas compartidas contra el cifrado externo:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Detección de comportamiento**.

3. Utilice el interruptor **Activar protección de carpetas compartidas frente a cifrado externo** para activar o desactivar la detección de actividad típica del cifrado externo.

4. Guarde los cambios.

## Selección de la acción que se debe tomar al detectar el cifrado externo de carpetas compartidas

*Para seleccionar la acción que se debe tomar al detectar el cifrado externo de carpetas compartidas:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Detección de comportamiento**.
3. Seleccione la acción correspondiente en el bloque **Protección de carpetas compartidas frente a cifrado externo**:
  - **Bloquear conexión durante N minutos (de 1 a 43800)**. Si se selecciona esta opción, al detectar un intento de modificar los archivos de las carpetas compartidas, Kaspersky Endpoint Security realiza las siguientes acciones:
    - Bloquea el acceso a la modificación de archivos en la sesión que ha iniciado la actividad maliciosa (el archivo será de solo lectura).
    - Crea copias de seguridad de los archivos que se están modificando.
    - Añade una entrada en los [informes de la interfaz local de la aplicación](#).
    - Envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.

Además, si el componente Motor de reparación está activado, Kaspersky Endpoint Security restaura los archivos modificados desde las copias de seguridad.

- **Notificar**. Si se selecciona esta opción, al detectar un intento de modificar los archivos de las carpetas compartidas, Kaspersky Endpoint Security realiza las siguientes acciones:
    - Añade una entrada en los [informes de la interfaz local de la aplicación](#).
    - Añade una entrada a la lista de amenazas activas.
    - Envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.
4. Guarde los cambios.

## Creación de una exclusión para la protección de carpetas compartidas frente a cifrado externo

Excluir una carpeta puede reducir el número de falsos positivos si su organización usa cifrado de datos al intercambiar archivos mediante carpetas compartidas. Por ejemplo, la Detección de comportamiento puede arrojar falsos positivos si el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Esta actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, añade dicha carpeta a las exclusiones.

[Cómo crear una exclusión para proteger carpetas compartidas utilizando la Consola de administración \(MMC\)](#) 



1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones**.
6. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
7. En la ventana que se abre, seleccione la pestaña **Exclusiones del análisis**.  
Esto abre una ventana que incluye una lista de exclusiones.
8. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.
9. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.  
Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
10. Haga clic en **Añadir**.
11. En el bloque **Propiedades**, seleccione la casilla de verificación **Archivo o carpeta**.
12. Haga clic en el enlace **Seleccionar archivo o carpeta** del bloque **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para modificarlos)** para abrir la ventana **Nombre de archivo o carpeta**.
13. Haga clic en **Examinar** y seleccione la carpeta compartida.

También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres \* y ? al introducir una máscara:

- El carácter \* (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
- Dos caracteres \* consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\\*\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la Carpeta, salvo en la Carpeta misma. La máscara debe incluir al menos un nivel de anidación. La máscara C:\\*\*\\*.txt no es válida.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Carpeta` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

14. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

15. Haga clic en el enlace **Cualquiera** del bloque **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para modificarlos)** para activar el enlace **Seleccionar componentes**.

16. Haga clic en el enlace **seleccionar los componentes** para abrir la ventana **Componentes de protección**.

17. Seleccione la casilla que hay junto al componente **Detección de comportamiento**.


18. Guarde los cambios.

[Cómo crear una exclusión para proteger carpetas compartidas utilizando Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** → **Exclusiones**.
5. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el enlace **Exclusiones del análisis**.
6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.
7. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.  
  
Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
8. Haga clic en el botón **Añadir**.
9. Seleccione cómo desea añadir la exclusión **Archivo o carpeta**.
10. Haga clic en **Examinar** y seleccione la carpeta compartida.  
También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres \* y ? al introducir una máscara:
  - El carácter \* (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
  - Dos caracteres \* consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\\*\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la Carpeta, salvo en la Carpeta misma. La máscara debe incluir al menos un nivel de anidación. La máscara C:\\*\*\\*.txt no es válida.
  - El carácter ? (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\???.txt incluirá las rutas a todos los archivos de la carpeta llamada Carpeta que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
11. En el bloque **Componentes de protección**, seleccione el componente **Detección de comportamiento**.

12. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.
13. Seleccione el estado **Activo** para la exclusión.  
Puede usar el interruptor para [detener una exclusión](#) en cualquier momento.
14. Guarde los cambios.

## Cómo crear una exclusión para proteger carpetas compartidas en la interfaz de la aplicación


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.
4. Haga clic en **Añadir**.
5. Haga clic en **Examinar** y seleccione la carpeta compartida.  
También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres \* y ? al introducir una máscara:
  - El carácter \* (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
  - Dos caracteres \* consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\\*\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT que se encuentren en carpeta anidadas en la Carpeta, salvo en la Carpeta misma. La máscara debe incluir al menos un nivel de anidación. La máscara C:\\*\*\\*.txt no es válida.
  - El carácter ? (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\???.txt incluirá las rutas a todos los archivos de la carpeta llamada Carpeta que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
6. En el bloque **Componentes de protección**, seleccione el componente **Detección de comportamiento**.
7. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.
8. Seleccione el estado **Activo** para la exclusión.  
Puede usar el interruptor para [detener una exclusión](#) en cualquier momento.
9. Guarde los cambios.

## Configuración de exclusión de direcciones en Protección de carpetas compartidas frente a cifrado externo.

El servicio Auditar inicio de sesión debe estar habilitado para permitir que las exclusiones de direcciones protejan las carpetas compartidas del cifrado externo. De forma predeterminada, el servicio Auditar inicio de sesión está desactivado (para obtener información detallada sobre la activación del servicio Auditar inicio de sesión, visite el sitio web de Microsoft).

La funcionalidad para excluir direcciones de la protección de carpetas compartidas no funciona en un equipo remoto si este está encendido antes de que se inicie Kaspersky Endpoint Security. Puede reiniciar este equipo remoto después de que se inicie Kaspersky Endpoint Security para asegurarse de que la funcionalidad para excluir direcciones de la protección de carpetas compartidas funcione en este equipo remoto.

*Para excluir de la protección los equipos remotos que ejecutan el cifrado externo de carpetas compartidas:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Detección de comportamiento**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Configure direcciones de exclusiones**.
4. Haga clic en el botón **Añadir** si desea añadir una dirección IP o el nombre de un equipo a la lista de exclusiones.
5. Introduzca la dirección IP o el nombre del equipo desde el cual no se deben gestionar los intentos de cifrado externos.
6. Guarde los cambios.

## Exportar e importar una lista de exclusiones a la protección de carpetas compartidas frente a cifrado externo

Puede exportar la lista de exclusiones a un archivo XML. Luego puede modificar el archivo para, por ejemplo, añadir una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

[Cómo exportar e importar una lista de exclusiones en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Detección de comportamiento**.
6. En el bloque **Parámetros de Protección frente a amenazas en la red**, haga clic en el botón **Exclusiones**.
7. 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 enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
8. Para importar la lista de exclusiones:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
9. 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 **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Detección de comportamiento**.
5. Para exportar la lista de exclusiones en el bloque **Exclusiones**:
  - a. Seleccione las exclusiones que desea exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las exclusiones seleccionadas o exportar la lista completa de exclusiones.
  - d. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - e. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
6. Para importar la lista de exclusiones en el bloque **Exclusiones**:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
7. Guarde los cambios.

## Prevención de intrusiones en el host

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El componente Prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus y el servicio en la nube Kaspersky Security Network.

El componente controla el funcionamiento de las aplicaciones mediante el uso de *derechos de las aplicaciones*. Los derechos de las aplicaciones incluyen los siguientes parámetros de acceso:

- Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro)
- Acceso a datos personales (como archivos y aplicaciones)

La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.

Durante el primer inicio de la aplicación, el componente Prevención de intrusiones en el host realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

Se le recomienda [participar en Kaspersky Security Network](#) para ayudar al componente Prevención de intrusiones en el host a trabajar con más eficacia.

3. Coloca la aplicación en uno de los *grupos de confianza*: De confianza/Restricción mínima/Restricción máxima/No confiable.

Los [grupos de confianza definen los derechos](#) que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la [configuración del componente Prevención de intrusiones en el host](#). Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea las acciones de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega el acceso a los módulos del sistema operativo.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

## Activación y desactivación de Prevención de intrusiones en el host

De forma predeterminada, el componente Prevención de intrusiones en el host está configurado y se ejecuta en el modo recomendado por los expertos de Kaspersky.

[Cómo activar o desactivar el componente Prevención de intrusiones en el host en la Consola de administración \(MMC\)](#) <sup>2</sup>




1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. Utilice la casilla de verificación **Prevención de intrusiones en el host** para activar o desactivar el componente.
7. Guarde los cambios.

### [Cómo activar o desactivar el componente Prevención de intrusiones en el host en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. Utilice el interruptor **Prevención de intrusiones en el host** para activar o desactivar el componente.
6. Guarde los cambios.

### [Cómo activar o desactivar el componente Prevención de intrusiones en el host en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Utilice el interruptor **Prevención de intrusiones en el host** para activar o desactivar el componente.
4. Guarde los cambios.

Si el componente Prevención de intrusiones en el host está activado, Kaspersky Endpoint Security incluye una aplicación en un [grupo de confianza](#) en función del nivel de peligro que represente dicha aplicación para el equipo. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza.

## Gestionar grupos de confianza de aplicaciones

Cuando la aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host comprueba la seguridad de la aplicación y la coloca en uno de los [grupos de confianza](#).

En la primera etapa del análisis de aplicaciones, Kaspersky Endpoint Security busca en la base de datos interna de aplicaciones conocidas una entrada coincidente y, simultáneamente, envía una solicitud a la base de datos de Kaspersky Security Network (si hay alguna conexión a Internet disponible). Según los resultados de la búsqueda en la base de datos interna y la base de datos de Kaspersky Security Network, la aplicación se sitúa en un grupo de confianza. Cada vez que la aplicación se inicia posteriormente, Kaspersky Endpoint Security envía una nueva consulta a la base de datos de KSN y sitúa la aplicación en un grupo de confianza diferente si la reputación de la aplicación en la base de datos de KSN ha cambiado.

Puede seleccionar un grupo de confianza al que Kaspersky Endpoint Security debe [asignar automáticamente todas las aplicaciones desconocidas](#). Las aplicaciones que se iniciaron antes de Kaspersky Endpoint Security se mueven automáticamente al grupo de confianza especificado en la ventana [de configuración del componente Prevención de intrusiones en el host](#).

En las aplicaciones que se iniciaron antes que Kaspersky Endpoint Security, solo se controla la actividad de la red. El control se realiza según las reglas de red [especificadas en la configuración del Firewall](#).

## Cambiar el grupo de confianza de una aplicación

Cuando la aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host comprueba la seguridad de la aplicación y la coloca en uno de los [grupos de confianza](#).

Los especialistas de Kaspersky no recomiendan mover aplicaciones del grupo de confianza asignado automáticamente a otro grupo diferente. Considere, en cambio, [modificar los derechos de una aplicación en particular](#) cuando resulte necesario.


[Cómo cambiar el grupo de confianza de una aplicación en la Consola de administración \(MMC\)](#) 


1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
7. Seleccione la pestaña **Derechos de la aplicación**.
8. Haga clic en el botón **Añadir**.
9. En la ventana abierta, introduzca los criterios para buscar la aplicación cuyo grupo de confianza desea cambiar.  
Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.
10. Haga clic en el botón **Actualizar**.  
Kaspersky Endpoint Security buscará la aplicación en la lista consolidada de aplicaciones instaladas en equipos administrados. Kaspersky Endpoint Security mostrará una lista de aplicaciones que coincidan con sus criterios de búsqueda.
11. Seleccione la aplicación pertinente.
12. En la lista desplegable **Añadir aplicaciones seleccionadas al grupo de confianza**, seleccione el grupo de confianza necesario para la aplicación.
13. Guarde los cambios.

[Cómo cambiar el grupo de confianza de una aplicación en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
6. Seleccione la pestaña **Derechos de la aplicación**.  
Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.
7. Haga clic en el botón **Añadir**.  
Se inicia el Asistente para añadir una aplicación a un grupo de confianza.
8. Seleccione el grupo de confianza correspondiente para la aplicación.
9. Seleccione el tipo de **aplicación**. Haga clic en **Siguiente**.  
Si desea cambiar el grupo de confianza para varias aplicaciones, seleccione el tipo **Grupo** y defina un nombre para el grupo de aplicaciones.
10. En la lista de aplicaciones abiertas, seleccione las aplicaciones cuyo grupo de confianza desea cambiar.  
Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres  \* y  ? al introducir una máscara.
11. Haga clic en **Aceptar** para finalizar el Asistente.  
La aplicación se añadirá al grupo de confianza.
12. Guarde los cambios.

[Cómo cambiar el grupo de confianza de una aplicación en la interfaz de la aplicación](#) 

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Haga clic en el botón **Administrar aplicaciones**.  
Esto abre la lista de aplicaciones instaladas.
4. Seleccione la aplicación pertinente.
5. En el menú contextual de la aplicación, haga clic en **Restricciones** → **<grupo de confianza>**.
6. Guarde los cambios.

En consecuencia, la aplicación se colocará en el otro grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza. Se asignarán los estados  (*definidos por el usuario*) a la aplicación. Si se cambia la reputación de la aplicación en Kaspersky Security Network, el componente de prevención de intrusiones en el host dejará el grupo de confianza de esta aplicación sin cambios.

## Configuración de derechos del grupo de confianza

Los [derechos de aplicación óptimos](#) se crean para diferentes grupos de confianza de forma predeterminada. Los grupos de aplicaciones que forman parte de un grupo de confianza heredan de este la configuración de sus derechos.

[Cómo cambiar los derechos del grupo de confianza en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
7. Seleccione la pestaña **Derechos de la aplicación**.
8. Seleccione el grupo de confianza pertinente.
9. Seleccione **Derechos del grupo** en el menú contextual del grupo de confianza.  
Se abren las propiedades del grupo de confianza.
10. Realice una de las siguientes acciones:
  - Para modificar los derechos de grupos de confianza que rigen las operaciones con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones, seleccione la pestaña **Archivos y registro del sistema**.
  - Si desea editar los derechos de los grupos de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione la pestaña **Derechos**.


La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.

11. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y elegir la opción necesaria: **Heredar**, **Permitir** (✓) o **Bloquear** (⊗).
12. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (✓/⊗).  
Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.
13. Guarde los cambios.




[Cómo cambiar los derechos de un grupo de confianza en Web Console y Cloud Console](#) ?


1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
  5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
  6. Seleccione la pestaña **Derechos de la aplicación**.  
Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.
  7. En la parte izquierda de la ventana, seleccione el grupo de confianza relevante.
  8. En la parte derecha de la ventana, en la lista desplegable, lleve a cabo una de las siguientes acciones:
    - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
    - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Derechos**.
- La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.
9. Para el recurso relevante, en la columna de la acción correspondiente, seleccione la opción necesaria: **Heredar**, **Permitir** (✓) o **Prohibir** (✗).
  10. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (✓/✗).  
Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.
  11. Guarde los cambios.

## [Cómo cambiar los derechos del grupo de confianza en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Haga clic en el botón **Administrar aplicaciones**.  
Esto abre la lista de aplicaciones instaladas.
4. Seleccione el grupo de confianza pertinente.
5. En el menú contextual del grupo de confianza, seleccione **Detalles y reglas**.  
Se abren las propiedades del grupo de confianza.
6. Realice una de las siguientes acciones:
  - Para modificar los derechos de grupos de confianza que rigen las operaciones con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones, seleccione la pestaña **Archivos y registro del sistema**.
  - Si desea editar los derechos de los grupos de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione la pestaña **Derechos**.

La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.

7. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione la opción necesaria: **Heredar**, **Permitir** () , **Denegar** ().
8. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** ().  
Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.
9. Guarde los cambios.

Se cambiarán los derechos del grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza. El estado  (*Configuración de usuario*) se asignará al grupo de confianza.

## Seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security

En las aplicaciones que se iniciaron antes que Kaspersky Endpoint Security, solo se controla la actividad de la red. El control se realiza según las [reglas de red](#) especificadas en la configuración del Firewall. Para especificar qué reglas de red se deben aplicar a la supervisión de la actividad de la red de tales aplicaciones, debe seleccionar un grupo de confianza.

[Cómo seleccionar un grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security en la Consola de administración \(MMC\)](#) 




1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Editar**.
7. Para el parámetro **Grupo de confianza para aplicaciones que se lancen antes que Kaspersky Endpoint Security para Windows comience a funcionar**, seleccione el [grupo de confianza](#) apropiado.
8. Guarde los cambios.

### [Cómo seleccionar un grupo de confianza para las aplicaciones iniciadas antes de Kaspersky Endpoint Security en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. Para el parámetro **Grupo de confianza para aplicaciones que se lancen antes que Kaspersky Endpoint Security para Windows comience a funcionar**, seleccione el [grupo de confianza](#) apropiado.
6. Guarde los cambios.

### [Cómo seleccionar un grupo de confianza para aplicaciones iniciadas antes de Kaspersky Endpoint Security en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Debajo de **Grupo de confianza para aplicaciones que se lancen antes que Kaspersky Endpoint Security para Windows comience a funcionar**, seleccione el [grupo de confianza](#) apropiado.
4. Guarde los cambios.

Como resultado, una aplicación que se inicia antes que Kaspersky Endpoint Security se incluirá en el otro grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación según el grupo de confianza.

## Selección de un grupo de confianza para aplicaciones desconocidas

Durante el primer inicio de una aplicación, el componente Prevención de intrusiones en el host determina el [grupo de confianza](#) para la aplicación. Si no tiene acceso a Internet o si Kaspersky Security Network no tiene información sobre esta aplicación, Kaspersky Endpoint Security colocará la aplicación en el grupo Restricción mínima de forma predeterminada. Cuando se detecta información sobre una aplicación previamente desconocida en KSN, Kaspersky Endpoint Security actualizará los derechos de esta aplicación. Luego, [los derechos de la aplicación pueden modificarse manualmente](#).

### [Cómo seleccionar un grupo de confianza para aplicaciones desconocidas en la Consola de administración \(MMC\)](#)


1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Reglas de procesamiento de la aplicación**, use la lista desplegable **Grupo de confianza para aplicaciones que no se pudieron agregar a grupos existentes** para seleccionar el grupo de confianza necesario.  

Si se activa la [participación en Kaspersky Security Network](#), Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta recibida, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración del componente Prevención de intrusiones en el host.
7. Utilice la casilla de verificación **Actualizar derechos para aplicaciones anteriormente desconocidas usando la base de datos de KSN** para configurar la actualización automática de los derechos de aplicaciones desconocidas.
8. Guarde los cambios.

### [Cómo seleccionar un grupo de confianza para aplicaciones desconocidas en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de la aplicación**, use la lista desplegable **Grupo de confianza para aplicaciones que no se pudieron agregar a grupos existentes** para seleccionar el grupo de confianza necesario.  
  
Si se activa la [participación en Kaspersky Security Network](#), Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta recibida, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración del componente Prevención de intrusiones en el host.
6. Utilice la casilla de verificación **Actualizar derechos para aplicaciones anteriormente desconocidas usando la base de datos de KSN** para configurar la actualización automática de los derechos de aplicaciones desconocidas.
7. Guarde los cambios.

### [Cómo seleccionar un grupo de confianza para aplicaciones desconocidas en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Debajo de **Reglas de procesamiento de la aplicación**, seleccione el grupo de confianza necesario.  
  
Si se activa la [participación en Kaspersky Security Network](#), Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta recibida, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración del componente Prevención de intrusiones en el host.
4. Utilice la casilla de verificación **Actualizar reglas de aplicaciones anteriormente desconocidas desde KSN** para configurar la actualización automática de los derechos de aplicaciones desconocidas.
5. Guarde los cambios.

## Seleccionar un grupo de confianza para aplicaciones firmadas digitalmente

Kaspersky Endpoint Security siempre coloca las aplicaciones firmadas por certificados de Microsoft o certificados de Kaspersky en el grupo De confianza.


### [Cómo seleccionar un grupo de confianza para aplicaciones firmadas digitalmente en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Reglas de procesamiento de la aplicación**, use la casilla de verificación **Confiar en aplicaciones firmadas digitalmente** para activar o desactivar la asignación automática al grupo de confianza para las aplicaciones que contienen la firma digital de los proveedores de confianza.  
*Los proveedores de confianza* son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede [añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual](#).  
Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera de confianza las aplicaciones con firma digital y utiliza otros parámetros para determinar su [grupo de confianza](#).
7. Guarde los cambios.

### [Cómo seleccionar un grupo de confianza para aplicaciones firmadas digitalmente en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de la aplicación**, use la casilla de verificación **Confiar en aplicaciones firmadas digitalmente** para activar o desactivar la asignación automática al grupo de confianza para las aplicaciones que contienen la firma digital de los proveedores de confianza.  
*Los proveedores de confianza* son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede [añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual](#).  
Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera de confianza las aplicaciones con firma digital y utiliza otros parámetros para determinar su [grupo de confianza](#).
6. Guarde los cambios.

### [Cómo seleccionar un grupo de confianza para aplicaciones firmadas digitalmente en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.

3. En el bloque **Reglas de procesamiento de la aplicación**, use la casilla de verificación **Confiar en aplicaciones firmadas digitalmente** para activar o desactivar la asignación automática al grupo de confianza para las aplicaciones que contienen la firma digital de los proveedores de confianza.

*Los proveedores de confianza* son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede [añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual](#).

Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera de confianza las aplicaciones con firma digital y utiliza otros parámetros para determinar su [grupo de confianza](#).

4. Guarde los cambios.

## Administración de los derechos de las aplicaciones

De manera predeterminada, la actividad de la aplicación se controla en función de los derechos de la aplicación que se definen para el [grupo de confianza](#) específico que Kaspersky Endpoint Security asignó a la aplicación cuando se inició por primera vez. Si es necesario, puede [modificar los derechos de la aplicación para un grupo de confianza completo](#), para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza.

Los derechos de la aplicación definidos manualmente tienen una prioridad más alta que los derechos de la aplicación definidos para un grupo de confianza. En otras palabras, si los derechos de aplicaciones definidos manualmente difieren de los derechos de aplicaciones definidos para un grupo de confianza, el componente Prevención de intrusiones en el host controla la actividad de la aplicación de acuerdo con los derechos de aplicaciones definidos en forma manual.

Las aplicaciones secundarias heredan las reglas que usted crea para las aplicaciones. Por ejemplo, si impide toda la actividad de red de cmd.exe, también se impedirá toda la actividad de red para notepad.exe si se inicia mediante cmd.exe. Las reglas no se heredan cuando una aplicación se inicia de manera indirecta por otra aplicación, pero no es secundaria de la aplicación de la que se ejecuta.

[Cómo cambiar los derechos de la aplicación en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
7. Seleccione la pestaña **Derechos de la aplicación**.
8. Haga clic en el botón **Añadir**.
9. En la ventana abierta, introduzca los criterios para buscar la aplicación cuyos derechos desea cambiar.  
Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres **\*** y **?** al introducir una máscara.
10. Haga clic en el botón **Actualizar**.  
Kaspersky Endpoint Security buscará la aplicación en la lista consolidada de aplicaciones instaladas en equipos administrados. Kaspersky Endpoint Security mostrará una lista de aplicaciones que coincidan con sus criterios de búsqueda.
11. Seleccione la aplicación pertinente.
12. En la lista desplegable **Añadir aplicaciones seleccionadas al grupo de confianza**, seleccione **Grupos predeterminados** y haga clic en **Aceptar**.  
La aplicación se añadirá al grupo predeterminado.
13. Seleccione la aplicación correspondiente y luego seleccione **Derechos de la aplicación** en el menú contextual de la aplicación.  
Se abren las propiedades de la aplicación.
14. Realice una de las siguientes acciones:
  - Para modificar los derechos de grupos de confianza que rigen las operaciones con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones, seleccione la pestaña **Archivos y registro del sistema**.
  - Si desea editar los derechos de los grupos de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione la pestaña **Derechos**.

La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.

15. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y elegir la opción necesaria: **Heredar**, **Permitir** (✓) o **Bloquear** (⊗).

16. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (✓/⊗).

Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

17. Guarde los cambios.

[Cómo cambiar los derechos de la aplicación en Web Console y Cloud Console](#) 





1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
  2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
  5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
  6. Seleccione la pestaña **Derechos de la aplicación**.  
Verá una lista de grupos de confianza en el lado izquierdo de la ventana y sus propiedades en el lado derecho.
  7. Haga clic en el botón **Añadir**.  
Se inicia el Asistente para añadir una aplicación a un grupo de confianza.
  8. Seleccione el grupo de confianza correspondiente para la aplicación.
  9. Seleccione el tipo de **aplicación**. Haga clic en **Siguiente**.  
Si desea cambiar el grupo de confianza para varias aplicaciones, seleccione el tipo **Grupo** y defina un nombre para el grupo de aplicaciones.
  10. En la lista de aplicaciones abiertas, seleccione las aplicaciones cuyos derechos desea cambiar.  
Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre del proveedor. Kaspersky Endpoint Security admite variables de entorno y los caracteres  \* y  ? al introducir una máscara.
  11. Haga clic en **Aceptar** para finalizar el Asistente.  
La aplicación se añadirá al grupo de confianza.
  12. En la parte izquierda de la ventana, seleccione la aplicación relevante.
  13. En la parte derecha de la ventana, en la lista desplegable, lleve a cabo una de las siguientes acciones:
    - Si desea editar los derechos de los grupos de confianza que regulan las operaciones con el registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione **Archivos y registro del sistema**.
    - Si desea editar los derechos del grupo de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione **Derechos**.
- La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.
14. Para el recurso relevante, en la columna de la acción correspondiente, seleccione la opción necesaria: **Heredar**, **Permitir** (🟢) o **Prohibir** (🔴).
  15. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** (🟢🔴).



Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

16. Guarde los cambios.

[Cómo cambiar los derechos de la aplicación en la interfaz de la aplicación](#) 

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Haga clic en el botón **Administrar aplicaciones**.  
Esto abre la lista de aplicaciones instaladas.
4. Seleccione la aplicación pertinente.
5. En el menú contextual de la aplicación, seleccione **Detalles y reglas**.  
Se abren las propiedades de la aplicación.
6. Realice una de las siguientes acciones:
  - Para modificar los derechos de grupos de confianza que rigen las operaciones con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones, seleccione la pestaña **Archivos y registro del sistema**.
  - Si desea editar los derechos de los grupos de confianza que regulan el acceso a los procesos y objetos del sistema operativo, seleccione la pestaña **Derechos**.
7. Para el recurso pertinente, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione la opción necesaria: **Heredar**, **Permitir** , **Denegar** .
8. Si desea supervisar el uso de los recursos del equipo, seleccione **Registrar eventos** .  
Kaspersky Endpoint Security registrará información sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.
9. Seleccione la pestaña **Exclusiones** y establezca la configuración avanzada de la aplicación (consulte la tabla a continuación).
10. Guarde los cambios.

Configuración avanzada de la aplicación

Parámetro	Descripción
<b>No analizar archivos abiertos</b>	Todos los archivos abiertos por la aplicación quedan excluidos de los análisis de Kaspersky Endpoint Security. Por ejemplo, si utiliza aplicaciones para realizar copias de seguridad de archivos, esta función ayuda a reducir el consumo de recursos de Kaspersky Endpoint Security.
<b>No supervisar la actividad de la aplicación</b>	Kaspersky Endpoint Security no supervisaré la actividad de red y archivos de la aplicación en el sistema operativo. La actividad de la aplicación se supervisa a través de los siguientes componentes: <a href="#">Detección de comportamiento</a> , <a href="#">Prevención de exploits</a> , <a href="#">Prevención de intrusiones en el host</a> , <a href="#">Motor de reparación</a> y <a href="#">Firewall</a> .
<b>No heredar restricciones del proceso principal (aplicación)</b>	Kaspersky Endpoint Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal se inicia a través de una aplicación para la que se configuran los <a href="#">derechos de aplicación</a> (Prevención de intrusiones en el host) y las <a href="#">reglas de red de la aplicación</a> (Firewall).
<b>No supervisar la</b>	Kaspersky Endpoint Security no supervisaré la actividad de archivos ni redes de las aplicaciones iniciadas por esta aplicación.

<b>actividad de las aplicaciones secundarias</b>	
<b>Permitir la interacción con la interfaz de la aplicación</b>	<a href="#">Autoprotección de Kaspersky Endpoint Security</a> bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona la casilla de verificación, la aplicación de acceso remoto tiene autorización para administrar la configuración de Kaspersky Endpoint Security mediante la interfaz de Kaspersky Endpoint Security.
<b>No analizar el tráfico cifrado/No analizar todo el tráfico</b>	El tráfico de red iniciado por la aplicación se excluirá de los análisis de Kaspersky Endpoint Security. Puede excluir todo el tráfico o solo el tráfico cifrado de los análisis. También puede excluir direcciones IP individuales y números de puerto de los análisis.

## Protección de recursos del sistema operativo y de datos personales

El componente Prevención de intrusiones en el host administra los derechos de las aplicaciones de realizar acciones en varias categorías de los recursos del sistema operativo y datos personales. Los especialistas de Kaspersky han creado categorías predefinidas de recursos protegidos. Por ejemplo, la categoría *Sistema operativo* tiene una subcategoría *Configuración de inicio* que enumera todas las claves de registro asociadas con la ejecución automática de aplicaciones. No puede editar ni eliminar las categorías predefinidas de recursos protegidos, ni los recursos protegidos que hay dentro de esas categorías.



[Cómo añadir o un recurso protegido en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el botón **Configuración**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
7. Seleccione la pestaña **Recursos protegidos**.  
Verá una lista de recursos protegidos en la parte izquierda de la ventana y los derechos correspondientes para acceder a esos recursos según el grupo de confianza específico.
8. Seleccione la categoría de recursos protegidos a los que desea añadir un nuevo recurso protegido.  
Si desea añadir una subcategoría, haga clic en **Añadir** → **Categoría**.
9. Haga clic en el botón **Añadir**. En la lista desplegable, seleccione el tipo de recurso que desee añadir:  
**Archivo o carpeta** o **Clave de registro**.
10. En la ventana abierta, seleccione un archivo, carpeta o clave de registro.  
Puede ver los derechos de las aplicaciones para acceder a los recursos añadidos. Para hacerlo, seleccione un recurso añadido en la parte izquierda de la ventana y Kaspersky Endpoint Security mostrará los derechos de acceso para cada grupo de confianza. También puede desactivar el control de la actividad de la aplicación con recursos utilizando la casilla de verificación junto a un nuevo recurso.
11. Guarde los cambios.

[Cómo añadir un recurso protegido en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el enlace **Derechos de aplicaciones y recursos protegidos**.  
Se abre la ventana de configuración de derechos de la aplicación y la lista de recursos protegidos.
6. Seleccione la pestaña **Recursos protegidos**.  
Verá una lista de recursos protegidos en la parte izquierda de la ventana y los derechos correspondientes para acceder a esos recursos según el grupo de confianza específico.
7. Haga clic en el botón **Añadir**.  
Se abre el Asistente de recurso nuevo.
8. Haga clic en el enlace **Nombre de grupo** para seleccionar la categoría de recursos protegidos a la que desea añadir un recurso protegido nuevo.  
Si desea añadir una subcategoría, seleccione la opción **Categoría de recursos protegidos**.
9. Seleccione el tipo de recurso que desee añadir: **Archivo o carpeta** o **Clave de registro**.
10. Seleccione un archivo, carpeta o clave de registro.
11. Haga clic en **Aceptar** para finalizar el Asistente.  
Puede ver los derechos de las aplicaciones para acceder a los recursos añadidos. Para hacerlo, seleccione un recurso añadido en la parte izquierda de la ventana y Kaspersky Endpoint Security mostrará los derechos de acceso para cada grupo de confianza. También puede usar la casilla de verificación en la columna **Estado** para desactivar el control de la actividad de la aplicación con recursos.
12. Guarde los cambios.

### [Cómo añadir un recurso protegido en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. Haga clic en el botón **Administrar recursos**.  
Se abre la lista de Recursos protegidos.
4. Seleccione la categoría de recursos protegidos a los que desea añadir un nuevo recurso protegido.  
Si desea añadir una subcategoría, haga clic en **Añadir** → **Categoría**.
5. Haga clic en el botón **Añadir**. En la lista desplegable, seleccione el tipo de recurso que desee añadir: **Archivo o carpeta** o **Clave de registro**.
6. En la ventana abierta, seleccione un archivo, carpeta o clave de registro.  
Puede ver los derechos de las aplicaciones para acceder a los recursos añadidos. Para hacerlo, seleccione un recurso añadido en la parte izquierda de la ventana y Kaspersky Endpoint Security mostrará una lista de aplicaciones y los derechos de acceso para cada aplicación. También puede desactivar el control de la actividad de la aplicación con recursos con el botón  **Desactivar control** en la columna **Estado**.
7. Guarde los cambios.

Kaspersky Endpoint Security controlará el acceso a los recursos añadidos del sistema operativo y a los datos personales. Kaspersky Endpoint Security controla el acceso de una aplicación a los recursos según el grupo de confianza asignado a la aplicación. Además, puede [cambiar el grupo de confianza de una aplicación](#).

## Eliminación de información sobre aplicaciones sin uso

Kaspersky Endpoint Security emplea los derechos de las aplicaciones para controlar las actividades de las aplicaciones. Los derechos de las aplicaciones se determinan según su grupo de confianza. Kaspersky Endpoint Security incluye una aplicación en un [grupo de confianza](#) cuando la aplicación se inicia por primera vez. Puede [cambiar manualmente el grupo de confianza de una aplicación](#). También puede [configurar manualmente los derechos de una aplicación en particular](#). Kaspersky Endpoint Security almacena la siguiente información sobre una aplicación: grupo de confianza de la aplicación y derechos de la aplicación.

Kaspersky Endpoint Security elimina automáticamente la información sobre las aplicaciones sin uso para ahorrar recursos informáticos. Kaspersky Endpoint Security elimina la información de las aplicaciones siguiendo las reglas siguientes:

- Si el grupo de confianza y los derechos de una aplicación se han determinado automáticamente, Kaspersky Endpoint Security elimina la información sobre esta aplicación después de 30 días. No es posible cambiar el período de almacenamiento para la información de las aplicaciones ni desactivar la eliminación automática.
- Si coloca manualmente una aplicación en un grupo de confianza o configura sus derechos de acceso, Kaspersky Endpoint Security elimina la información sobre esta aplicación después de 60 días (período de almacenamiento predeterminado). Puede cambiar el período de almacenamiento para la información de las aplicaciones y desactivar la eliminación automática (consulte las instrucciones más abajo).

Cuando inicia una aplicación cuya información se ha eliminado, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

## [Cómo configurar la eliminación automática de información sobre aplicaciones no utilizadas en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
6. En el bloque **Reglas de procesamiento de la aplicación**, lleve a cabo una de las siguientes acciones:

- Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días** e introduzca el número de días.

Kaspersky Endpoint Security eliminará información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, después del número definido de días. Kaspersky Endpoint Security también eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.

- Si desea desactivar la eliminación automática, desactive la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días**.

Kaspersky Endpoint Security almacenará de forma indefinida información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, sin límites en el período de almacenamiento. Kaspersky Endpoint Security solo eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.


7. Guarde los cambios.

## [Cómo configurar la eliminación automática de información sobre aplicaciones no utilizadas en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de la aplicación**, lleve a cabo una de las siguientes acciones:
  - Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días** e introduzca el número de días.  
Kaspersky Endpoint Security eliminará información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, después del número definido de días. Kaspersky Endpoint Security también eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.
  - Si desea desactivar la eliminación automática, desactive la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días**.  
Kaspersky Endpoint Security almacenará de forma indefinida información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, sin límites en el período de almacenamiento. Kaspersky Endpoint Security solo eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.
6. Guarde los cambios.

[Cómo configurar la eliminación automática de información sobre aplicaciones no utilizadas en la interfaz de la aplicación](#) 



1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Prevención de intrusiones en el host**.
3. En el bloque **Reglas de procesamiento de la aplicación**, lleve a cabo una de las siguientes acciones:
  - Si desea configurar la eliminación automática, seleccione la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días** e introduzca el número de días.  
Kaspersky Endpoint Security eliminará información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, después del número definido de días. Kaspersky Endpoint Security también eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.
  - Si desea desactivar la eliminación automática, desactive la casilla de verificación **Eliminar reglas de aplicaciones que no se hayan iniciado durante más de N días**.  
Kaspersky Endpoint Security almacenará de forma indefinida información sobre las aplicaciones que coloque manualmente en un grupo de confianza o cuyos derechos de acceso configuró manualmente, sin límites en el período de almacenamiento. Kaspersky Endpoint Security solo eliminará la información de aplicaciones cuyo grupo de confianza y derechos de las aplicaciones se hayan determinado automáticamente después de 30 días.
4. Guarde los cambios.

## Control de prevención de intrusiones en el host

Puede recibir informes sobre el funcionamiento del componente Prevención de intrusiones en el host. Los informes contienen datos sobre operaciones con recursos informáticos realizadas por la aplicación (permitidas o prohibidas). Los informes también contienen información sobre las aplicaciones que utilizan cada recurso.

Para supervisar las operaciones de prevención de intrusiones en el host, debe activar la redacción de informes. Por ejemplo, puede [activar el reenvío de informes para aplicaciones individuales en la configuración del componente Prevención de intrusiones en el host](#).

Al configurar la supervisión de prevención de intrusiones en el host, tenga en cuenta la carga potencial de la red al reenviar eventos a Kaspersky Security Center. También puede activar el guardado de informes solo en el registro local de Kaspersky Endpoint Security.

## Protección del acceso a audio y vídeo

Los ciberdelincuentes pueden usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web). Kaspersky Endpoint Security controla cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada.

De forma predeterminada, Kaspersky Endpoint Security controla el acceso de las aplicaciones a la transmisión de audio y vídeo de la siguiente manera:

- Las aplicaciones de confianza y de restricción mínima pueden recibir la transmisión de audios y vídeo de los dispositivos de manera predeterminada.
- Las aplicaciones de restricción máxima y no confiables no pueden recibir la transmisión de audio y vídeo de los dispositivos de forma predeterminada.

De forma manual, puede [permitir que las aplicaciones reciban transmisión de audio y vídeo](#).

## Características especiales de la protección de transmisión de audio

La protección del flujo de audio tiene las siguientes características especiales:

- El [componente Prevención de intrusiones en el host se debe activar](#) para que esta funcionalidad esté activa.
- Si la aplicación empezó a recibir el flujo de audio antes de que se iniciara el componente Prevención de intrusiones en el host, Kaspersky Endpoint Security permite que la aplicación reciba el flujo de audio y no muestre ninguna notificación.
- Si movió la aplicación al grupo No confiable o al grupo Restricción máxima después de que la aplicación comenzase a recibir el flujo de audio, Kaspersky Endpoint Security permite que la aplicación reciba el flujo de audio y no muestra ninguna notificación.
- Después de modificar la configuración del acceso a la aplicación a dispositivos de grabación de sonido (por ejemplo, si se [ha bloqueado la recepción del flujo de audio por parte de la aplicación](#)), esta aplicación se debe reiniciar para que deje de recibir el flujo de audio.
- El control del acceso a las secuencias de audio de los dispositivos de registro de sonidos no depende de la configuración de acceso a la cámara web de una aplicación.
- Kaspersky Endpoint Security protege el acceso únicamente los micrófonos integrados y micrófonos externos. El resto de los dispositivos de flujo de audio no son compatibles.
- Kaspersky Endpoint Security no puede garantizar la protección de un flujo de audio desde dispositivos como cámaras DSLR, videocámaras portátiles y cámaras de acción.
- Cuando ejecuta la grabación de vídeo y audio o aplicaciones de reproducción por primera vez desde la instalación de Kaspersky Endpoint Security, puede que se interrumpa la reproducción o grabación de vídeo y audio. Esto es necesario a fin de activar la funcionalidad que controla el acceso a los dispositivos de grabación de sonido por aplicaciones. El servicio del sistema que controla el hardware de audio se reiniciará cuando Kaspersky Endpoint Security se ejecute por primera vez.

## Características especiales de la protección de acceso a la cámara web de la aplicación

La funcionalidad de protección del acceso a la cámara web tiene las siguientes consideraciones especiales y limitaciones:

- La aplicación controla el vídeo y las imágenes estáticas derivados del procesamiento de los datos de la cámara web.
- La aplicación controla el flujo de audio si este forma parte del flujo de vídeo recibido a través de la cámara web.

- La aplicación controla solo las cámaras web conectadas mediante USB o IEEE1394 que se muestran como Dispositivos de imagen en el Administrador del dispositivos de Windows.
- Kaspersky Endpoint Security admite las siguientes cámaras web:
  - Cámara web Logitech HD C270
  - Cámara web Logitech HD C310
  - Cámara web Logitech C210
  - Cámara web Logitech Pro 9000
  - Cámara web Logitech HD 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.

## Motor de reparación

El Motor de reparación permite a Kaspersky Endpoint Security anular acciones que han sido realizadas por el malware en el sistema operativo.

Al anular la actividad de malware en el sistema operativo, Kaspersky Endpoint Security tramita los siguientes tipos de actividad de malware:

- **Actividad de archivos**

Kaspersky Endpoint Security realiza las siguientes acciones:

- Elimina 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 modificado o eliminado.

- **Actividad del sistema**

Kaspersky Endpoint Security realiza las siguientes acciones:

- Finaliza los procesos iniciados por el malware.
- Finaliza los procesos en los que haya penetrado una aplicación maliciosa.
- No reanuda procesos que el malware haya suspendido.

- **Actividad de red**

Kaspersky Endpoint Security realiza las siguientes acciones:

- Bloquea la actividad de red del malware.
- Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.

La reversión de acciones puede iniciarse durante un [análisis antivirus](#) o a pedido de los componentes [Protección contra archivos peligrosos](#) y [Detección de comportamientos](#).

Deshacer las operaciones de un software malicioso (malware) afecta a un conjunto de datos definidos rigurosamente. La anulación no tiene efectos adversos en el sistema operativo ni en la integridad de los datos del equipo.


### [Cómo activar o desactivar el componente Motor de reparación en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección frente a amenazas avanzadas** → **Motor de reparación**.
6. Utilice la casilla de verificación **Motor de reparación** para activar o desactivar el componente.
7. Guarde los cambios.

### [Cómo activar o desactivar el componente Motor de reparación en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Motor de reparación**.
5. Utilice el interruptor **Motor de reparación** para activar o desactivar el componente.
6. Guarde los cambios.

### [Cómo activar o desactivar el componente Motor de reparación en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Motor de reparación**.
3. Utilice el interruptor **Motor de reparación** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si el Motor de reparación está activado, Kaspersky Endpoint Security revertirá las acciones realizadas por aplicaciones maliciosas en el sistema operativo.

## Kaspersky Security Network

A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

*Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security podrá utilizar los servicios de KSN para conocer la categoría y la reputación de los archivos analizados u obtener información sobre la reputación de las direcciones web que se analicen.

El uso de Kaspersky Security Network es voluntario. La aplicación le invita a usar en KSN durante la configuración inicial de la aplicación. Los usuarios podrán reanudar o interrumpir su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el [sitio web de Kaspersky](#) contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. El archivo ksn\_<identificador del idioma>.txt, que forma parte del [kit de distribución](#) de la aplicación, contiene el texto de la Declaración de Kaspersky Security Network.

Para reducir la carga de los servidores de KSN, los expertos de Kaspersky pueden publicar actualizaciones para la aplicación que impidan temporalmente o restrinjan parcialmente la capacidad de enviar solicitudes a Kaspersky Security Network. Bajo estas condiciones, el estado de conexión a KSN cambia a *Habilitado con restricciones* en la interfaz local de la aplicación.

## Infraestructura de KSN

Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura de KSN:

- *KSN Global*. Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky Security Network y, a su vez, envían a Kaspersky información sobre los objetos que se detectan en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos de Kaspersky Security Network.
- *KSN privada*. Esta es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky Security Network y a otros datos estadísticos sin enviar datos a KSN desde sus propios equipos. KSN Privada se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:
  - porque las estaciones de trabajo locales no tienen acceso a Internet;
  - porque, por motivos legales o debido a las políticas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

De forma predeterminada, Kaspersky Security Center usa KSN Global. Puede configurar el uso de KSN privada en la Consola de administración (MMC), en Kaspersky Security Center Web Console y en la [línea de comando](#). No se puede configurar el uso de KSN privada en Kaspersky Security Center Cloud Console.

Para más información sobre KSN Privada, consulte la documentación de Kaspersky Private Security Network.

## Activación y desactivación del uso de Kaspersky Security Network

*Para activar o desactivar el uso de Kaspersky Security Network:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Kaspersky Security Network**.
3. Utilice el interruptor **Kaspersky Security Network** para activar o desactivar el componente.  
Si activó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte las condiciones de uso de la Declaración de Kaspersky Security Network (KSN), si está de acuerdo con ellas.  
De forma predeterminada, Kaspersky Endpoint Security emplea el modo KSN ampliado. El *modo KSN ampliado* es un modo en el que Kaspersky Endpoint Security envía [información adicional](#) a Kaspersky.
4. De ser necesario, desactive la opción **Activar el modo ampliado de KSN** con el interruptor.
5. Guarde los cambios.

Como resultado, si el uso de KSN está activado, Kaspersky Endpoint Security usa la información sobre la reputación de archivos, recursos web y aplicaciones recibida de Kaspersky Security Network.

## Limitaciones de KSN privado

KSN privado (en lo sucesivo también denominado KPSN) le permite utilizar su propia base de datos de reputación local para comprobar la reputación de los objetos (archivos o direcciones web). La reputación de un objeto añadido a la base de datos de reputación local tiene mayor prioridad que uno añadido a KSN/KPSN. Por ejemplo, imagine que Kaspersky Endpoint Security está analizando un equipo y solicita la reputación de un archivo en KSN/KPSN. Si el archivo tiene una reputación "no confiable" 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 confiable" y tomará la acción definida para las amenazas detectadas.

Sin embargo, en algunos casos, es posible que Kaspersky Endpoint Security no solicite la reputación de un objeto en KSN/KPSN. Si este es el caso, Kaspersky Endpoint Security no recibirá datos de la base de datos de reputación local de KPSN. Es posible que Kaspersky Endpoint Security no solicite la reputación de un objeto en KSN/KPSN por las siguientes razones:

- Las aplicaciones de Kaspersky utilizan bases de datos de reputación offline. Las bases de datos de reputación offline están diseñadas para optimizar los recursos durante el funcionamiento de las aplicaciones de Kaspersky y para proteger los objetos de importancia crítica en el equipo. Las bases de datos de reputación offline son creadas por expertos de Kaspersky basándose en datos de Kaspersky Security Network. Las aplicaciones de Kaspersky actualizan las bases de datos de reputación offline con bases de datos antivirus de la aplicación específica. Si las bases de datos de reputación offline contienen información sobre un objeto que se está analizando, la aplicación no solicita la reputación de este objeto a KSN/KPSN.
- Las exclusiones de análisis ([zona de confianza](#)) se configuran en la configuración de la aplicación. Si este es el caso, la aplicación no tiene en cuenta la reputación del objeto en la base de datos de reputación local.
- La aplicación utiliza tecnologías de optimización de análisis, como iSwift o iChecker, o almacena en caché solicitudes de reputación en KSN/KPSN. Si este es el caso, es posible que la aplicación no solicite la reputación de los objetos analizados anteriormente.
- Para optimizar su carga de trabajo, la aplicación analiza archivos de cierto formato y tamaño. Los expertos de Kaspersky determinan la lista de formatos relevantes y límites de tamaño. Esta lista se actualiza con las bases de datos antivirus de la aplicación. También puede establecer la configuración de optimización del análisis en la interfaz de la aplicación, por ejemplo, para el [componente de Protección frente a amenazas en archivos](#).

## Activar y desactivar el modo Cloud para los componentes de protección

*Modo nube* es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky.

La funcionalidad del modo Cloud está disponible desde la versión 3.0 de Kaspersky Private Security Network.

*Para activar y desactivar el modo Cloud para los componentes de protección:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Kaspersky Security Network**.
3. Utilice el interruptor **Activar modo nube** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security descarga una versión ligera o una versión completa de las bases de datos antivirus durante la próxima actualización.

Si no está disponible la versión ligera de bases de datos antivirus, Kaspersky Endpoint Security cambia automáticamente a la versión premium.

## Configuración del proxy de KSN

Los equipos de los usuarios que gestionen el servidor de administración de Kaspersky Security Center pueden interactuar con KSN mediante el servicio de proxy de KSN.

El servicio de proxy de KSN ofrece las siguientes funcionalidades:

- El equipo del usuario puede consultar y enviar información a KSN, aunque no tenga acceso directo a Internet.
- El servicio almacena los datos procesados en una caché; con ello, el equipo recibe más rápido la información que solicita y se reduce la congestión en el canal externo de comunicaciones por red.


De forma predeterminada, después de activar KSN y de aceptar la declaración de KSN, la aplicación utiliza un servidor proxy para conectarse con Kaspersky Security Network. El servidor proxy que utiliza la aplicación es el Servidor de administración de Kaspersky Security Center, a través del puerto TCP 13111. De este modo, si el proxy de KSN no está disponible, debe comprobar lo siguiente:

- Que el servicio *ksnproxy* esté en ejecución en el Servidor de administración.
- Que el firewall en el equipo no esté bloqueando el puerto 13111.

Puede configurar el uso del proxy de KSN de la siguiente manera: active o desactive el proxy de KSN y configure el puerto para la conexión. Para hacerlo, necesita abrir las propiedades del Servidor de administración. Para obtener detalles sobre la configuración del proxy de KSN, consulte la Ayuda de Kaspersky Security Center. También puede activar o desactivar el proxy de KSN para equipos individuales en la directiva de Kaspersky Endpoint Security.

[Cómo activar o desactivar el proxy de KSN en la Consola de administración \(MMC\)](#) 



1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección frente a amenazas avanzadas** → **Kaspersky Security Network**.
3. En el bloque **Configuración del proxy de KSN**, utilice la casilla de verificación **Usar Proxy de KSN** para activar o desactivar el proxy de KSN.
4. Si es necesario, elija la casilla de verificación **Utilizar servidores de KSN cuando el Proxy de KSN no esté disponible**.  
Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores KSN pueden ubicarse tanto en el lado de Kaspersky (cuando se utiliza KSN global) como en el lado de terceros (cuando se utiliza KSN privada).
5. Guarde los cambios.

### Cómo activar o desactivar el proxy de KSN en Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 frente a amenazas avanzadas** → **Kaspersky Security Network**.
5. Utilice la casilla de verificación **Usar Proxy de KSN** para activar o desactivar el proxy de KSN.
6. Si es necesario, elija la casilla de verificación **Utilizar servidores de KSN cuando el Proxy de KSN no esté disponible**.  
Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores KSN pueden ubicarse tanto en el lado de Kaspersky (cuando se utiliza KSN global) como en el lado de terceros (cuando se utiliza KSN privada).
7. Guarde los cambios.

La dirección del proxy de KSN coincide con la dirección del Servidor de administración. Cuando el nombre de dominio del Servidor de administración se modifica, debe actualizar manualmente la dirección del proxy de KSN.

*Para configurar la dirección del proxy de KSN:*

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Adicional** → **Instalación remota** → **Paquetes de instalación**.
2. En el menú contextual de la carpeta **Paquetes de instalación**, elija **Propiedades**.
3. En la pestaña **General** de la ventana abierta, especifique la nueva dirección del servidor proxy de KSN.
4. Guarde los cambios.

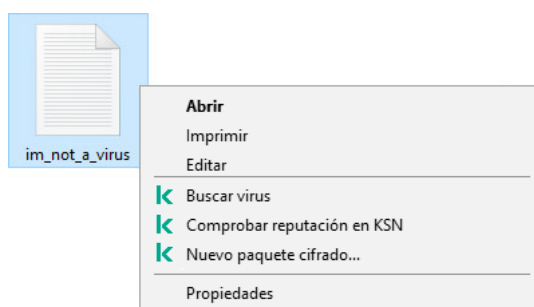
## Comprobar la reputación de un archivo en Kaspersky Security Network

Si tiene dudas sobre la seguridad de un archivo, puede comprobar su reputación en Kaspersky Security Network.

Puede comprobar la reputación de un archivo si ha aceptado los términos de la [Declaración de Kaspersky Security Network](#).


Para comprobar la reputación de un archivo en Kaspersky Security Network:


Abra el menú contextual del archivo y seleccione la opción **Comprobar reputación en KSN** (vea la imagen más abajo).




Menú contextual Archivo

Kaspersky Endpoint Security muestra la reputación del archivo:

 **De confianza (Kaspersky Security Network).** La mayoría de los usuarios de Kaspersky Security Network han confirmado que el archivo es de confianza.

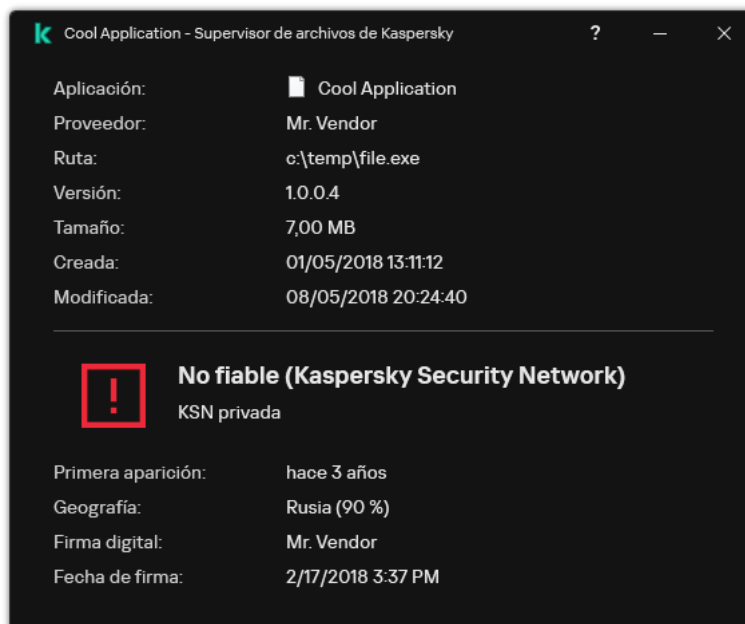
 **Software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.** Aunque no poseen ninguna función maliciosa, dichas aplicaciones pueden ser aprovechadas por los intrusos. Para obtener más información sobre el software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos personales de un usuario, visite el [sitio web de la Enciclopedia de Kaspersky](#). Puede [añadir estas aplicaciones a la lista de confianza](#).

 **No fiable (Kaspersky Security Network).** Un virus u otra aplicación que [representa una amenaza](#).

 **Desconocido (Kaspersky Security Network).** Kaspersky Security Network no tiene ninguna información sobre el archivo. Puede analizar un archivo utilizando bases de datos antivirus (la opción **Buscar virus** del menú contextual).

Kaspersky Endpoint Security muestra la solución KSN que se utilizó para determinar la reputación del archivo: *KSN Global* o *KSN privada*.

Kaspersky Endpoint Security también muestra información adicional sobre el archivo (vea la imagen más abajo).



Reputación de un archivo en Kaspersky Security Network

## Análisis de conexiones cifradas


Tras la instalación, Kaspersky Endpoint Security añade el certificado de Kaspersky al almacenamiento del sistema de certificados de confianza (Tienda de certificados de Windows). Kaspersky Endpoint Security también incluye el uso del almacenamiento del sistema de certificados de confianza en Firefox y Thunderbird para analizar el tráfico de estas aplicaciones.

Los componentes [Control web](#), [Protección frente a amenazas en el correo](#) y [Protección frente a amenazas web](#) pueden descifrar y analizar el tráfico de red que se transmite a través de conexiones cifradas que usen los siguientes protocolos:

- SSL 3.0
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

## Configuración los parámetros del análisis de conexiones cifradas.

*Para configurar las opciones de análisis para conexiones cifradas:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, seleccione el modo de análisis de conexiones cifradas:
  - **No analizar las conexiones cifradas.** Kaspersky Endpoint Security no tendrá acceso al contenido de sitios web cuyas direcciones comiencen con `https://`.
  - **Analizar las conexiones cifradas cuando lo soliciten los componentes de protección.** Kaspersky Endpoint Security analizará el tráfico cifrado solo cuando los componentes Protección frente a amenazas en

archivos, Protección frente a amenazas en el correo y Control web lo soliciten.

- **Analizar conexiones cifradas siempre.** Kaspersky Endpoint Security analizará el tráfico de red cifrado incluso cuando los componentes de protección están desactivados.

Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por [aplicaciones de confianza para las que el análisis de tráfico está desactivado](#). Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza solo en la interfaz de Kaspersky Endpoint Security. No puede ver la lista en la Consola de Kaspersky Security Center.

4. Si es necesario, [añada exclusiones de análisis: direcciones y aplicaciones de confianza](#).
5. Establezca la configuración para analizar conexiones cifradas (consulte la tabla a continuación).
6. Guarde los cambios.

Configuración del análisis de conexiones cifradas

Parámetro	Descripción
<b>Cuando se visite un dominio cuyo certificado no sea de confianza</b>	<ul style="list-style-type: none"><li>• <b>Autorizar.</b> Cuando se elige esta opción y se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security permite que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para advertirle que acceder a ese dominio en particular no es recomendable e indicarle por qué. La página contiene un enlace para obtener acceso al recurso web solicitado. Una vez que el usuario hace clic en el enlace, dispone de una hora para visitar otros recursos alojados en el mismo dominio sin que Kaspersky Endpoint Security le advierta sobre la falta de confianza en el certificado.</li><li>• <b>Bloquear conexión.</b> Cuando se elige esta opción y se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security impide que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para explicarle por qué ese dominio en particular se ha bloqueado.</li></ul>
<b>Si se presentan errores al analizar una conexión cifrada</b>	<ul style="list-style-type: none"><li>• <b>Bloquear conexión.</b> Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red.</li><li>• <b>Agregar dominio a exclusiones.</b> Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security añade el dominio con el que se presentó el problema a la lista de dominios con errores de análisis y deja de controlar el tráfico de red cifrado que se genera al visitarlo. La lista de dominios con errores de análisis de conexiones cifradas solo puede consultarse a través de la interfaz local de la aplicación. Para borrar el contenido de la lista, deberá seleccionar <b>Bloquear conexión</b>.</li></ul>
<b>Bloquear conexiones SSL 2.0 (recomendado)</b>	Cuando la casilla está activada, Kaspersky Endpoint Security bloquea las conexiones de red que se establecen con el protocolo SSL 2.0.

	<p>Cuando la casilla no está activada, Kaspersky Endpoint Security no bloquea las conexiones de red que se establecen con el protocolo SSL 2.0 ni controla el tráfico que se transmite por ellas.</p>
<p><b>Descifrar una conexión cifrada al sitio web que usa certificados EV</b></p>	<p>Los certificados de EV (certificados de validación extendida) confirman la autenticidad de los sitios web y mejoran la seguridad de la conexión. Cuando un sitio web cuente con un certificado de EV, verá un candado en la barra de direcciones del navegador. Es posible, además, que la barra de direcciones esté total o parcialmente sombreada en verde.</p> <p>Cuando esta casilla está activada, Kaspersky Endpoint Security descifra y controla las conexiones cifradas con sitios web que usan un certificado de EV.</p> <p>Cuando esta casilla no está activada, Kaspersky Endpoint Security no tiene acceso al contenido del tráfico HTTPS. Esto significa que la aplicación únicamente puede controlar el tráfico HTTPS sobre la base de la dirección del sitio web (por ejemplo, <a href="https://google.com">https://google.com</a>).</p> <p>Cuando visite un sitio web con certificado de EV por primera vez, la conexión cifrada se descifrará independientemente de que la casilla esté o no activada.</p>

## Analizar conexiones cifradas en Firefox y Thunderbird


Tras la instalación, Kaspersky Endpoint Security añade el certificado de Kaspersky al almacenamiento del sistema de certificados de confianza (Tienda de certificados de Windows). De forma predeterminada, Firefox y Thunderbird utilizan su propia tienda de certificados patentada de Mozilla en lugar de la tienda de certificados de Windows. Si Kaspersky Security Center está implementado en su organización y se está aplicando una directiva a un equipo, Kaspersky Endpoint Security habilita automáticamente el uso de la tienda de certificados de Windows en Firefox y Thunderbird para analizar el tráfico de estas aplicaciones. Si no se aplica una directiva al equipo, puede elegir el almacenamiento de certificados que utilizarán las aplicaciones de Mozilla. Si seleccionó la tienda de certificados de Mozilla, añada manualmente un certificado de Kaspersky. Esto ayudará a evitar errores al trabajar con tráfico HTTPS.

Para analizar el tráfico en el navegador Mozilla Firefox y el cliente de correo Thunderbird, debe [activar el Análisis de conexiones cifradas](#). Si el Análisis de conexiones cifradas está desactivado, Kaspersky Endpoint Security no analiza el tráfico en el navegador Mozilla Firefox ni en el cliente de correo Thunderbird.

Antes de añadir un certificado a la tienda de Mozilla, exporte el certificado de Kaspersky desde el Panel de control de Windows (propiedades del navegador). Para obtener información sobre cómo exportar el certificado de Kaspersky, consulte la [Base de conocimientos del Soporte técnico](#). Para obtener detalles sobre cómo añadir un certificado al almacenamiento, visite el [sitio web de soporte técnico de Mozilla](#).

Puede elegir la tienda de certificados solo en la interfaz local de la aplicación.

*Para elegir una tienda de certificados para analizar conexiones cifradas en Firefox y Thunderbird:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En la sección **Mozilla Firefox y Thunderbird**, seleccione la casilla **Utilizar el almacén de certificados seleccionado para analizar las conexiones cifradas en las aplicaciones de Mozilla**.

4. Seleccionar una tienda de certificados:


- **Usar el almacén de certificados de Windows (recomendado).** El certificado raíz de Kaspersky se añade a esta tienda durante la instalación de Kaspersky Endpoint Security.
- **Usar almacenamiento de certificados de Mozilla.** Mozilla Firefox y Thunderbird utilizan sus propias tiendas de certificados. Si se selecciona la tienda de certificados de Mozilla, debe añadir manualmente el certificado raíz de Kaspersky a esta tienda a través de las propiedades del navegador.

5. Guarde los cambios.

## Exclusión de conexiones cifradas del análisis

La mayoría de los recursos web usan conexiones cifradas. Los expertos de Kaspersky recomiendan que active el [análisis de conexiones cifradas](#). Si el análisis de conexiones cifradas interfiere con la actividad relacionada con el trabajo, puede añadir un sitio web a las exclusiones llamadas *direcciones de confianza*. Si una aplicación de confianza usa una conexión cifrada, puede [desactivar el análisis de conexiones cifradas para esta aplicación](#). Por ejemplo, puede desactivar el análisis de conexiones cifradas para aplicaciones de almacenamiento en la nube que usan la autenticación de dos factores con su propio certificado.

*Para excluir una dirección web del análisis de conexiones cifradas:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Direcciones de confianza**.
4. Haga clic en el botón **Añadir**.
5. Introduzca el nombre de dominio o la dirección IP. Kaspersky Endpoint Security no analizará las conexiones cifradas que se establezcan al visitar el dominio especificado.

Kaspersky Endpoint Security admite el carácter  para introducir una máscara en el nombre de dominio.

Kaspersky Endpoint Security no es compatible con las máscaras para direcciones IP. Puede introducir un rango de direcciones IP en la interfaz de la aplicación local (por ejemplo, 198.51.100.0/24). No puede introducir un rango de direcciones IP en la consola de Kaspersky Security Center.


Ejemplos:

- **domain.com:** el registro incluye las siguientes direcciones: <https://domain.com>, <https://www.domain.com>, <https://domain.com/page123>. El registro es exclusivo de subdominios (por ejemplo, [subdomain.domain.com](https://subdomain.domain.com)).
- **subdomain.domain.com:** el registro incluye las siguientes direcciones: <https://subdomain.domain.com>, <https://subdomain.domain.com/page123>. El registro es exclusivo del dominio [domain.com](https://domain.com).
- **\*.domain.com:** el registro incluye las siguientes direcciones: <https://movies.domain.com>, <https://images.domain.com/page123>. El registro es exclusivo del dominio [domain.com](https://domain.com).

6. Guarde los cambios.

De forma predeterminada, Kaspersky Endpoint Security no analiza las conexiones cifradas cuando se producen errores y añade el sitio web a una lista especial de *dominios con errores de análisis*. Kaspersky Endpoint Security compila una lista separada para cada usuario y no envía datos a Kaspersky Security Center. Puede [activar el bloqueo de la conexión cuando se produce un error de análisis](#). La lista de dominios con errores de análisis de conexiones cifradas solo puede consultarse a través de la interfaz local de la aplicación.


*Para ver la lista de dominios con errores de análisis:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, haga clic en el botón **Dominios con errores de análisis**.

Se abre una lista de dominios con errores de análisis. Para restablecer la lista, active el bloqueo de la conexión cuando ocurran errores de análisis en la directiva, aplique la directiva y, a continuación, restablezca el parámetro a su valor inicial y vuelva a aplicar la directiva.

Los especialistas de Kaspersky hacen una lista de *excepciones globales*: sitios web de confianza que Kaspersky Endpoint Security no verifica independientemente de la configuración de la aplicación.

*Para ver las exclusiones globales aplicadas al análisis de tráfico cifrado:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Análisis de conexiones cifradas**, haga clic en la lista de enlaces de sitios web de confianza.

Esto abre una lista de sitios web compilada por expertos de Kaspersky. Kaspersky Endpoint Security no analiza las conexiones protegidas para los sitios web de la lista. La lista puede sufrir cambios cada vez que se actualizan las bases de datos y los módulos de Kaspersky Endpoint Security.

## Eliminación de datos

Kaspersky Endpoint Security cuenta con una tarea para eliminar información a distancia de los equipos de los usuarios.

En Kaspersky Endpoint Security, la eliminación de datos funciona:

- en modo silencioso;
- en los discos duros y en las unidades extraíbles;
- en todas las cuentas de usuario del equipo.

Kaspersky Endpoint Security ejecutará la tarea *Eliminación de datos* sin importar el tipo de licencia que se esté utilizando y con independencia de que esta haya caducado.

## Modos de eliminación de datos

La tarea ofrece los siguientes modos de eliminación:

- Eliminación de datos inmediata.

Utilice este modo para, por ejemplo, eliminar información antigua que esté ocupando espacio innecesariamente.

- Eliminación de datos pospuesta.

Este modo está pensado para, por ejemplo, proteger los datos de un equipo portátil robado o extraviado. Es posible determinar que los datos de un equipo deberán eliminarse automáticamente si este abandona la red corporativa o no se sincroniza con Kaspersky Security Center durante un tiempo prolongado.

No se puede establecer una planificación para eliminar datos en las propiedades de la tarea. Solo puede eliminar datos inmediatamente después de iniciar la tarea manualmente, o configurar la eliminación de datos retrasada si no hay conexión con Kaspersky Security Center.

## Limitaciones

La tarea Eliminación de datos tiene las siguientes limitaciones:

- Solo los administradores de Kaspersky Security Center pueden controlar la tarea *Eliminación de datos*. La tarea no puede iniciarse ni detenerse desde la interfaz local de Kaspersky Endpoint Security.
- Para el sistema de archivos NTFS, Kaspersky Endpoint Security elimina solo los nombres de los flujos de datos principales. Los nombres alternativos de flujos de datos no se pueden eliminar.
- Cuando elimina un archivo de enlace simbólico, Kaspersky Endpoint Security también elimina los archivos cuyas rutas se especifican en el enlace simbólico.

## Creación de una tarea Eliminación de datos

*Para eliminar información de los equipos de los usuarios:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en el botón **Añadir**.  
El Asistente de tareas comienza.
3. Configure los parámetros de la tarea:
  - a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.
  - 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 la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.



Si se añaden nuevos equipos a un grupo de administración dentro del ámbito de la tarea, la tarea de eliminación de datos inmediata se ejecutará en los nuevos equipos únicamente si la tarea se completa en los cinco minutos posteriores a la incorporación de dichos equipos.

5. 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 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. Es prácticamente imposible restaurar los datos después de que se eliminen.

9. Si desea posponer la eliminación de datos, seleccione la casilla **Eliminar automáticamente los datos cuando no haya habido conexión con Kaspersky Security Center en más de N días**. Defina el número de días.

La tarea de eliminación pospuesta se ejecutará cada vez que no haya conexión con Kaspersky Security Center durante el período definido.

Al configurar la eliminación de datos pospuesta, recuerde que los empleados pueden apagar sus equipos cuando se van de vacaciones. En ese caso, la eliminación se llevará a cabo aunque ese sea el motivo por el que se ha excedido el plazo de desconexión. 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 esta casilla no está activada, la tarea se ejecutará después de que se realice la sincronización con Kaspersky Security Center.

10. Cree la lista de objetos que desee eliminar:

- **Carpetas.** Kaspersky Endpoint Security eliminará todos los archivos y todas las subcarpetas de la carpeta. La ruta de acceso a la carpeta no puede contener máscaras ni variables de entorno.
- **Archivos por extensión** Kaspersky Endpoint Security buscará los archivos que tengan la extensión especificada en todas las unidades del equipo, incluidas las extraíbles. Para especificar más de una extensión, use los caracteres ";" o ",".
- **Alcance predefinido.** Kaspersky Endpoint Security eliminará archivos de las siguientes áreas:
  - **Documentos.** Los archivos en la carpeta estándar *Documentos* del sistema operativo y sus subcarpetas.
  - **Cookies.** Los archivos en los que el navegador guarda datos de los sitios web visitados por el usuario (como los datos de autorización del usuario).
  - **Escritorio.** Los archivos en la carpeta estándar *Escritorio* del sistema operativo y sus subcarpetas.

- **Archivos temporales de Internet Explorer.** Archivos temporales relacionados con el funcionamiento de Internet Explorer, como copias de páginas web, imágenes y archivos multimedia.
- **Archivos temporales.** Archivos temporales relacionados con el funcionamiento de aplicaciones instaladas en el equipo. Por ejemplo, las aplicaciones de Microsoft Office crean archivos temporales que contienen copias de seguridad de documentos.
- **Archivos de Outlook.** Archivos relacionados con el funcionamiento del cliente de correo Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de libretas de direcciones sin conexión (OAB) y archivos de libretas de direcciones personales (PAB).
- **Perfil del usuario.** Conjunto de archivos y carpetas en los que el sistema operativo almacena la configuración asociada a la cuenta local del usuario.

Puede crear una lista de objetos que desee eliminar en cada pestaña. Kaspersky Endpoint Security creará una lista consolidada y eliminará los archivos de esta lista cuando se complete una tarea.

Los archivos que Kaspersky Endpoint Security necesita para funcionar no pueden eliminarse.

11. Guarde los cambios.

12. Active la casilla ubicada junto a la tarea.

13. Haga clic en el botón **Ejecutar**.

Como resultado, la información de los equipos se eliminará según el modo que se haya seleccionado, es decir, de inmediato o cuando no haya habido conexión. Si un archivo no pudiera eliminarse (por ejemplo, porque el usuario está trabajando con él), Kaspersky Endpoint Security no intentará eliminarlo una segunda vez. Para completar la eliminación de datos, deberá ejecutar la tarea nuevamente.

# Control del equipo

## Control Web

Control web permite regular el acceso de los usuarios a los recursos web. El componente ayuda a reducir tanto el volumen de tráfico como el tiempo que se malgasta en actividades no laborales. Cuando un usuario intenta abrir un sitio web que se ha restringido mediante Control web, Kaspersky Endpoint Security bloqueará el acceso o le mostrará una advertencia (vea la imagen más abajo).

Kaspersky Endpoint Security solo puede supervisar tráfico HTTP y HTTPS.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario [activar el análisis de conexiones cifradas](#).

## Métodos para regular el acceso a los sitios web

Control web permite configurar el acceso a los sitios web a través de estos criterios:

- **Categorías de sitios web.** Para categorizar los sitios web, la aplicación utiliza el servicio en la nube Kaspersky Security Network, el análisis heurístico y la base de datos de sitios web conocidos, que está incluida con las demás bases de datos de la aplicación. Por ejemplo, puede restringir el acceso de los usuarios a la categoría "Redes sociales" o a [otras categorías](#).
- **Tipo de datos.** Puede restringir el acceso 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 "Archivos de gráficos".

- **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 Office" solo para la categoría de sitios web "Correo electrónico basado en Web".


## Reglas de acceso a sitios web

Control web regula el acceso de los usuarios a los sitios web a través de *reglas de acceso*. Para cada una de estas reglas, puede configurar las siguientes opciones avanzadas:

- **Usuarios alcanzados por la regla.**  
Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.
- **Planificación de reglas.**  
Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

## Prioridad de las reglas de acceso

Cada regla tiene una prioridad. Cuanto más alta sea la posición de una regla en la lista, mayor prioridad tendrá. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web "Redes sociales" y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.



No se puede proporcionar la página web solicitada.


Dirección: <http://kaspersky.ru/>.

La regla kasp ha bloqueado la página web.

Razón: el recurso web pertenece a las categorías de contenido Sin determinar y a las categorías de tipos de datos Sin determinar.

Este recurso web está prohibido en la empresa. Si considera que el bloqueo es un error, o si necesita acceder a este recurso web, póngase en contacto con el administrador de la red corporativa local ([Solicitar acceso](#)).

Mensaje generado: 10/14/2020 4:05:34 AM



La página web solicitada puede no ser segura o estar prohibida por la directiva de la empresa.

Dirección: <http://kaspersky.ru/>.

La regla kasp ha bloqueado la página web.

Motivo: el recurso web pertenece a las categorías de contenido Sin determinar y a las categorías de tipo de datos Sin determinar.

Haga clic en el vínculo <http://kaspersky.ru/> para abrir la página web solicitada.

Haga clic en el vínculo [http://kaspersky.ru/\\*](http://kaspersky.ru/*) para obtener acceso a todo el contenido del sitio web en el que se encuentra la página web solicitada.

Haga clic en el vínculo [\\*/\\*.kaspersky.ru/\\*](*/*.kaspersky.ru/*) para obtener acceso a todos los dominios existentes de nivel inferior o igual al que está marcado con \"\*\".

Se concederá acceso a los recursos web enumerados anteriormente en la sesión actual de la aplicación.

Si ha recibido esta advertencia por error, póngase en contacto con el administrador de la red corporativa local ([Solicitar acceso](#)).


Mensaje generado: 10/14/2020 4:06:16 AM

Mensajes de Control web

## Activación y desactivación de Control Web

De forma predeterminada, Control Web está activado.

Para activar o desactivar el Control web:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.
3. Utilice interruptor **Control web** para activar o desactivar el componente.
4. Guarde los cambios.

## Acciones con reglas de acceso a recursos web

No se recomienda crear más de 1000 reglas de acceso a recursos web, ya que esto puede provocar inestabilidad en el sistema.

Una regla de acceso a recursos web es un conjunto de filtros y acciones que Kaspersky Endpoint Security realiza cuando el usuario visita recursos web que se describen en la regla durante el lapso de tiempo indicado en la planificación de reglas. Los filtros permiten especificar de forma precisa un conjunto de recursos web para los que el componente Control Web controla el acceso.

Están disponibles los siguientes filtros:


- **Filtrar por contenido.** Control Web categoriza los [recursos web por contenido](#) y tipo de datos. Puede controlar el acceso de los usuarios a los recursos web con tipos de datos y contenido que entran dentro de esas categorías. Cuando los usuarios visitan recursos web que pertenecen a la categoría de contenido o de tipo de dato seleccionada, Kaspersky Endpoint Security realiza la acción especificada en la regla.
- **Filtrar por direcciones de recursos web.** Puede controlar el acceso de los usuarios a todas las direcciones de recursos web, a direcciones de recursos web individuales o a grupos de direcciones de recursos web.  
Si se especifica el filtro por contenido y por direcciones de recursos web, y las direcciones de recursos web o los grupos de direcciones de recursos web especificados pertenecen a las categorías de contenido o de tipo de dato seleccionadas, Kaspersky Endpoint Security no controla el acceso a todos los recursos web en dichas categorías de contenido o de tipo de datos. En lugar de ello, la aplicación controla el acceso únicamente a las direcciones de recursos web o a los grupos de direcciones de recursos web.
- **Filtrar por nombres de usuarios y grupos de usuarios.** Puede especificar los nombres de los usuarios o grupos de usuarios para los que el acceso a los recursos web esté controlado de acuerdo con la regla.
- **Planificación de reglas.** Puede especificar la planificación de reglas. La planificación de reglas determina el intervalo de tiempo durante el que Kaspersky Endpoint Security supervisa el acceso a los recursos web cubiertos por la regla.

Tras instalar Kaspersky Endpoint Security, la lista de reglas del componente Control Web deja de estar en blanco. Se predefinen dos reglas:

- La regla de scripts y hojas de estilo, que concede acceso a todos los usuarios y en todo momento a los recursos web cuyas direcciones contienen los nombres de los archivos con las extensiones CSS, JS o VBS. Por ejemplo: `http://www.example.com/style.css`, `http://www.example.com/style.css?mode=normal`.
- 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.

## Adición de una regla de acceso a recursos web

Para añadir y editar una regla de acceso a recursos web:

1. En la ventana de la aplicación principal, haga clic en el botón .
  2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.
  3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.
  4. En la ventana que se abre, haga clic en el botón **Añadir**.  
Se abre la ventana **Regla de acceso a recursos web**.
  5. En el campo **Nombre de la regla**, introduzca el nombre de la regla.
  6. Seleccione el estado **Activo** para la regla de acceso a recursos web.  
Puede usar el interruptor para [desactivar la regla de acceso a recursos web](#) en cualquier momento.
  7. En el bloque **Acción**, seleccione la opción correspondiente:
    - **Autorizar**. Si se selecciona este valor, Kaspersky Endpoint Security permite el acceso a los recursos de Internet que coinciden con los parámetros de la regla.
    - **Bloquear**. Si se selecciona este valor, Kaspersky Endpoint Security bloquea el acceso a los recursos de Internet que coinciden con los parámetros de la regla.
    - **Advertir**. Si se selecciona este valor, Kaspersky Endpoint Security muestra una advertencia de que un recurso web es no deseado cuando el usuario intenta acceder a recursos web que coincidan con la regla. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.
  8. En el bloque **Contenido del filtro**, seleccione el filtro de contenido relevante:
    - **Por categorías de contenido**. Puede controlar el acceso de los usuarios a los recursos web por [categoría](#) (por ejemplo, la categoría *Redes sociales*).
    - **Por tipos de datos**. Puede controlar el acceso de los usuarios a los recursos web en función del tipo de datos específico de sus datos publicados (por ejemplo, *Imágenes gráficas*).
- Para configurar el filtro de contenido:
- a. Haga clic en el enlace **Configuración**.
  - b. Seleccione las casillas de verificación junto a los nombres de las categorías de contenido y de tipos de datos requeridas.  
Al seleccionar la casilla de verificación junto al nombre de una categoría de contenido o de tipos de datos, Kaspersky Endpoint Security aplica la regla para controlar el acceso a los recursos web que pertenecen a las categorías de contenido o a las categorías de tipos de datos seleccionadas.
  - c. Regrese a la ventana para configurar la regla de acceso a recursos web.
9. En el bloque **Direcciones**, seleccione el filtro de direcciones de recursos web correspondiente:
    - **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. Para crear una lista de direcciones de recursos web:
  - a. Haga clic en el botón **Añadir dirección** o **Añadir un grupo de direcciones**.
  - b. En la ventana abierta, 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](#).
  - c. Regrese a la ventana para configurar la regla de acceso a recursos web.

Si el [Análisis de conexiones cifradas no está activado](#), en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

10. En el bloque **Usuarios**, seleccione el filtro correspondiente para los usuarios:

- **A todos los usuarios.** Control web no filtrará recursos web para usuarios específicos.
- **A usuarios individuales o grupos.** Control web filtrará los recursos web solo para usuarios específicos. Para crear una lista de usuarios a los que desea aplicar la regla:
  - a. Haga clic en el botón **Añadir**.
  - b. En la ventana abierta, seleccione los usuarios o el grupo 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.

11. En la lista desplegable **Planificación de reglas**, seleccione el nombre de la planificación necesaria o genere una nueva planificación basada en la planificación de la regla seleccionada. Para ello:


- a. Haga clic en el botón **Editar o añadir nuevo**.
- b. En la ventana que se abre, haga clic en el botón **Añadir**.
- c. En la ventana abierta, introduzca el nombre de la planificación de reglas.
- d. Configure la planificación de acceso a los recursos web para los usuarios.
- e. Regrese a la ventana para configurar la regla de acceso a recursos web.

12. Guarde los cambios.

## Asignación de prioridades a reglas de acceso a recursos web

Puede asignar prioridades a cada regla de la lista de reglas, organizando las reglas de un modo determinado.


*Para asignar una prioridad a una regla de acceso a un recurso web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.

3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.
4. En la ventana abierta, seleccione la regla cuya prioridad quiere cambiar.
5. Utilice los botones **Arriba** y **Abajo** para mover la regla a la posición relevante en la lista de reglas de acceso a recursos web.
6. Guarde los cambios.

## Activación y desactivación de una regla de acceso a recursos web

*Para activar o desactivar una regla de acceso a recursos web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.
3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.
4. En ventana abierta, seleccione la regla que desee activar o desactivar.
5. En la columna **Estado**, haga lo siguiente:
  - Si desea activar el uso de la regla, seleccione el valor **Activo**.
  - Si desea desactivar el uso de la regla, seleccione el valor **Inactivo**.
6. Guarde los cambios.

## Exportación e importación de la lista de direcciones web de confianza

Puede exportar la lista de reglas de Control Web a un archivo XML. Luego puede modificar el archivo para, por ejemplo, añadir una gran cantidad de direcciones del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de Control Web o para migrar la lista a un servidor diferente.

[Cómo exportar e importar una lista de reglas de Control Web en la Consola de administración \(MMC\)](#) 



1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control Web**.
6. Para exportar la lista de reglas de Control Web, haga lo siguiente:
  - a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.  
Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.
7. Para importar la lista de reglas de Control Web, haga lo siguiente:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.


[Cómo exportar e importar una lista de reglas de Control Web en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 las reglas que quiera exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las reglas seleccionadas o exportar la lista completa.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas a un archivo XML en la carpeta de descargas predeterminada.
6. Para importar la lista de reglas, en el bloque **Lista de reglas**:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
7. Guarde los cambios.

## Comprobación de las reglas de acceso a recursos web

Para comprobar la coherencia de las reglas de Control Web, puede probarlas. Con este fin, el componente Control Web incluye la función Diagnóstico de reglas.

*Para probar las reglas de acceso a recursos web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.
3. En el bloque **Configuración**, haga clic en el enlace **Diagnóstico de reglas**.  
Se abre la ventana **Diagnóstico de reglas**.
4. Si quiere probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a un recurso web específico, seleccione la casilla de verificación **Especificar dirección** e introduzca la dirección del recurso web en el campo siguiente.


5. Si quiere probar las reglas que Kaspersky Endpoint Security utiliza para controlar el acceso a recursos web para usuarios y grupos de usuarios especificados, especifique una lista de usuarios o grupos de usuarios.
6. Si quiere probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a recursos web de ciertas categorías de contenido o categorías de tipos de datos, seleccione la casilla de verificación **Filtrar contenido** y elija la opción correspondiente de la lista desplegable (**Por categorías de contenido**, **Por tipos de datos** o **Por categorías de contenido y tipos de datos**).
7. Si quiere probar las reglas que tienen en cuenta la hora y el día de la semana cuando se realiza un intento de acceder a los recursos web especificados en las condiciones del diagnóstico de reglas, seleccione la casilla de verificación **Incluir hora del intento de acceso**. A continuación, especifique el día de la semana y la hora.
8. Haga clic en el botón **Análisis**.

Después de que se complete la prueba, aparece un mensaje con información sobre la acción que realiza Kaspersky Endpoint Security, de acuerdo con la primera regla activada ante un intento de acceso al recurso web especificado (autorizar, bloquear o advertencia). La primera regla que se activa es la primera con un rango en la lista de reglas de Control Web superior al de otras reglas que cumplen las condiciones de diagnóstico. El mensaje se muestra a la derecha del botón **Análisis**. La siguiente tabla incluye las reglas restantes activadas, en las que se especifica la acción que ha llevado a cabo Kaspersky Endpoint Security. Las reglas se incluyen en orden de prioridad decreciente.

## Exportación e importación de la lista de direcciones de recursos web

Si ha creado una lista de direcciones de recursos web en una regla de acceso a recursos web, puede exportarla a un archivo .txt. Puede importar en veces sucesivas la lista desde este archivo para evitar la creación de una nueva lista de direcciones de recursos web manualmente al configurar una regla de acceso. La opción de exportación e importación de la lista de direcciones de recursos web puede ser útil si, por ejemplo, crea reglas de acceso con parámetros similares.

*Para importar o exportar una lista de direcciones de recursos web a un archivo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.
3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso a recursos web**.
4. Seleccione la regla cuya lista de direcciones de recursos web desee exportar o importar.
5. Para exportar la lista de direcciones web de confianza, haga lo siguiente en el bloque **Direcciones**:
  - a. Seleccione las direcciones que desea exportar.  
Si no seleccionó ninguna dirección, Kaspersky Endpoint Security exportará todas las direcciones.
  - b. Haga clic en el botón **Exportar**.
  - c. En la ventana que se abre, introduzca el nombre del archivo TXT al que desea exportar la lista de direcciones de recursos web y seleccione la carpeta en la que desea guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de direcciones de recursos web a un archivo TXT.
6. Para importar la lista de recursos web, haga lo siguiente en el bloque **Direcciones**:

a. Haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo TXT del que importar la lista de recursos web.

b. Abra el archivo.




Si el equipo ya tiene una lista de direcciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo TXT.

7. Guarde los cambios.

## Supervisión de las actividades de los usuarios en Internet

Kaspersky Endpoint Security puede registrar información sobre todos los sitios web que visitan los usuarios, incluso cuando se trata de sitios web permitidos. Esto hace posible obtener un historial de navegación completo. Kaspersky Endpoint Security envía los eventos sobre las actividades de los usuarios a Kaspersky Security Center, al [registro local de Kaspersky Endpoint Security](#) y al registro de eventos de Windows. Para recibir estos eventos en Kaspersky Security Center, deberá configurar los ajustes de los eventos en una directiva, ya sea a través de Web Console o con la Consola de administración. Dependiendo de la configuración, los eventos de Control web también pueden transmitirse por correo electrónico o mostrarse en el equipo del usuario a través de notificaciones en pantalla.


Cuando un usuario utiliza Internet, Kaspersky Endpoint Security crea los siguientes eventos:

- Bloqueo de un sitio web (estado , correspondiente a los *Eventos críticos*).
- Visita a un sitio web no recomendado (estado , correspondiente a las *Advertencias*).
- Visita a un sitio web permitido (estado , correspondiente a los *Mensajes informativos*).

Antes de activar la supervisión de la actividad de Internet del usuario, debe hacer lo siguiente:

- Inyecte un script de interacción de la página web en el tráfico web (consulte las instrucciones a continuación). El script permite el registro de eventos de Control web.
- Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario [activar el análisis de conexiones cifradas](#).

*Para inyectar un script de interacción de página web en el tráfico web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En el bloque **Procesamiento de tráfico**, seleccione la casilla de verificación **Insertar scripts en el tráfico web para interactuar con las páginas web**.
4. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security inyectará un script de interacción de la página web en el tráfico web. Este script permite el registro de eventos de Control web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los [informes](#).

*Para que los eventos de Control web se registren en el equipo del usuario:*

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

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

3. En el bloque **Notificaciones**, haga clic en el botón **Configuración de notificación**.

4. En la ventana que se abre, seleccione la sección **Control Web**.

Se abrirá una tabla con los eventos de Control web y los distintos métodos de notificación.

5. Configure el método de notificación para cada evento: **Guardar en informe local** o **Guardar en Registro de eventos de Windows**.

Para que se registren las visitas a sitios web permitidos, también deberá hacer cambios en la configuración de Control web (consulte las instrucciones más abajo).

A través de la tabla de eventos también podrá activar las notificaciones en pantalla y las notificaciones por correo electrónico. Para que la aplicación envíe notificaciones por correo electrónico, deberá configurar los ajustes del servidor SMTP. Para obtener más información sobre el envío de notificaciones por correo electrónico, consulte la [Ayuda de Kaspersky Security Center](#).

6. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security comenzará a registrar los eventos relacionados con las actividades en Internet del usuario.

Control web envía los eventos sobre las actividades de los usuarios a Kaspersky Security Center de la siguiente manera:

- Si utiliza Kaspersky Security Center, Control web envía los eventos para todos los objetos que componen la página web. Por este motivo, cada página web bloqueada podría dar lugar a más de un evento. Por ejemplo, si se bloquea la página web <http://www.example.com>, Kaspersky Endpoint Security podría transmitir eventos sobre los objetos <http://www.example.com>, <http://www.example.com/icono.ico>, <http://www.example.com/archivo.js>, etc.
- Si utiliza Kaspersky Security Center Cloud Console, Control web agrupa los eventos y solo envía el protocolo y el dominio del sitio web. Por ejemplo, si un usuario abre las páginas web no recomendadas <http://www.example.com/main>, <http://www.example.com/contact> y <http://www.example.com/gallery>, Kaspersky Endpoint Seguridad enviará solo un evento con el objeto <http://www.example.com>.

*Para que se registren las visitas a sitios web permitidos:*

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

2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.

3. En el bloque **Adicional**, haga clic en el botón **Configuración avanzada**.

4. En la ventana que se abre, active la casilla **Registrar el acceso a páginas permitidas**.

5. Guarde los cambios.

Como resultado, podrá ver el historial de navegación completo.


## Edición de plantillas de mensajes de Control Web

Dependiendo del tipo de acción seleccionado en las propiedades de las reglas de Control Web, Kaspersky Endpoint Security muestra un mensaje de uno de los siguientes tipos cuando los usuarios intentan acceder a recursos de Internet (la aplicación sustituye una página HTML por un mensaje para la respuesta para el servidor HTTP):

- **Mensaje de advertencia.** Este mensaje advierte al usuario de que no se recomienda visitar el recurso web o de que este infringe la directiva corporativa de seguridad. Kaspersky Endpoint Security muestra un mensaje de advertencia si se selecciona la opción **Advertir** en la configuración de la regla que describe este recurso web.  
Si el usuario cree que la advertencia es un error, este puede hacer clic en el enlace de la advertencia para enviar un mensaje generado previamente al administrador de la red de área local.
- **Mensaje que informe del bloqueo de un recurso web.** Kaspersky Endpoint Security muestra un mensaje que informa de que se ha bloqueado un recurso web si se selecciona la opción **Bloquear** en la configuración de la regla que describe este recurso web.  
Si el usuario cree que el recurso web está bloqueado por error, este puede hacer clic en el enlace del mensaje que informa del bloqueo del recurso web para enviar un mensaje generado previamente y enviárselo al administrador de la red de área local.

Se proporcionan plantillas especiales para un mensaje de advertencia, el mensaje que informe de que se ha bloqueado un recurso web y el mensaje que se envía al administrador de la LAN. Puede modificar su contenido.

*Para cambiar la plantilla de mensajes de Control Web:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control Web**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control web:
  - **Advertencia.** El campo de entrada consta de una plantilla del mensaje que se muestra si se activa una regla de advertencia sobre intentos de acceso a un recurso web no deseado.
  - **Mensaje sobre el bloqueo.** El campo de entrada contiene la plantilla del mensaje que aparece si se activa una regla que bloquee el acceso a un recurso web.
  - **Mensaje para el administrador.** La plantilla del mensaje que se enviará al administrador de la LAN si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso a la página web**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.
4. Guarde los cambios.

## Edición de máscaras para direcciones de recursos web

El uso de una *máscara para direcciones de recursos web* (también denominada "máscara de dirección") puede resultar útil si tiene que introducir varias direcciones de recursos web similares al crear una regla de acceso a recursos web. Si se elabora correctamente, una máscara de dirección puede sustituir un gran número de direcciones de recursos web.

Siga estas reglas si va a crear una máscara de dirección:

1. El carácter `*` sustituye cualquier secuencia que contenga cero caracteres o más.

Por ejemplo, si introduce la máscara de dirección `*abc*`, la regla de acceso se aplica a todos los recursos web que contengan la secuencia `abc`. Ejemplo: `http://www.ejemplo.com/pagina_0-9abcdef.html`.

2. Una secuencia de caracteres `*.` (conocida como *máscara de dominio*) le permite seleccionar todos los dominios de una dirección. La máscara de dominio `*.` representa cualquier nombre de dominio, nombre de subdominio o una línea en blanco.

Ejemplo: la máscara `*.ejemplo.com` representa las siguientes direcciones:

- `http://imágenes.ejemplo.com`. La máscara de dominio `*.` representa `imágenes.`
- `http://usuario.imágenes.ejemplo.com`. La máscara de dominio `*.` representa `imágenes.` y `usuario.`
- `http://ejemplo.com`. La máscara de dominio `*.` se interpreta como una línea en blanco.

3. La secuencia de caracteres `www.` que se encuentra al comienzo de cualquier máscara de dirección se interpreta como `*.`

Ejemplo: la máscara de dirección `www.example.com` se interpreta como `*.example.com`. Esta máscara cubre las direcciones `www2.ejemplo.com` y `www.imágenes.ejemplo.com`.

4. Si una máscara de dirección no comienza con el carácter `*`, su contenido será equivalente al mismo contenido con el prefijo `*.`

5. Si una máscara de dirección termina con un carácter distinto de `/` o `*`, su contenido será equivalente al mismo contenido que con el sufijo `/*`.

Ejemplo: la máscara de dirección `http://www.example.com` incluye direcciones como `http://www.example.com/abc` donde `a`, `b` y `c` son cualesquiera caracteres.

6. Si una máscara de dirección termina con el carácter `/`, su contenido será equivalente al mismo contenido que con el sufijo `/*`.

7. La secuencia de caracteres `/*` al final de una máscara de dirección se considera como `/*` o como una cadena vacía.

8. Las direcciones de recursos web se contrastan con una máscara de dirección y se tiene en cuenta el protocolo (`http` o `https`):

- Si la máscara de dirección no contiene ningún protocolo de red, dicha máscara de dirección abarca direcciones con cualquier protocolo de red.

Ejemplo: la máscara de dirección `ejemplo.com` incluye las direcciones `http://ejemplo.com` y `https://ejemplo.com`.

- Si la máscara de dirección contiene un protocolo de red, dicha máscara de dirección abarca únicamente direcciones con el mismo protocolo de red que el de la máscara de dirección.

Ejemplo: la máscara de dirección `http://*.example.com` incluye la dirección `http://www.example.com`, pero no incluye `https://www.example.com`.

9. Una máscara de dirección entre comillas dobles se trata sin tener en cuenta ninguna sustitución adicional, excepto el carácter `*` si se ha incluido inicialmente en la máscara de dirección. Las reglas 5 y 7 no se aplican a las máscaras de dirección que aparezcan dentro de dobles comillas (ver ejemplos 14-18 en la siguiente tabla).

10. Durante la comparación con la máscara de dirección de un recurso web no se tienen en cuenta el nombre de usuario, la contraseña, el puerto de conexión ni la diferencia entre mayúsculas y minúsculas de los caracteres.

No.	Máscara de dirección	Dirección de un recurso web para verificar	Es la dirección que abarca la máscara de 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 y 1.
7	www.example.com	https://www.example.com	Sí	Consulte las reglas 3, 2 y 1.
8	http://www.*.example.com	http://123.example.com	Sí	Consulte las reglas 3, 4 y 1.
9	www.example.com	http://www.example.com/abc	Sí	Consulte las reglas 3, 5 y 1.
10	example.com	http://www.example.com	Sí	Consulte las reglas 3 y 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 y 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Sí	Consulte las reglas 1 y 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Sí	Consulte las reglas 9 y 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	Una máscara de dirección contiene más información aparte de la dirección de un recurso web.



## Migración de reglas de acceso a recursos web de las versiones previas de la aplicación

Cuando Kaspersky Endpoint Security 10 Service Pack 2 para Windows o una versión anterior de la aplicación se actualiza a Kaspersky Endpoint Security para Windows 11.8.0, las reglas de acceso a recursos web basadas en categorías de contenido de recursos web se migran conforme a los principios siguientes:

- Las reglas de acceso a recursos web basadas en una o varias categorías de contenido de recursos web de las listas "Chats y foros", "Correo electrónico basado en Web" y "Redes sociales" migran a la categoría de contenido de recursos web "Comunicación por Internet".
- Las reglas de acceso a recursos web basadas en una o varias categorías de contenido de recursos web de las listas "Tiendas en línea" y "Sistemas de pago" migran a la categoría de contenido de recursos web "Tiendas en línea, bancos, sistemas de pago".
- Las reglas de acceso a recursos web basadas en la categoría de contenido de recursos web "Apuestas" migran a la categoría de contenido "Apuestas, loterías, sorteos".
- Las reglas de acceso a recursos web basadas en la categoría "Juegos de Internet" migran a la categoría de contenido "Videojuegos".
- Las reglas de acceso a recursos web basadas en categorías de contenido de recursos web no incluidas en la lista anterior se migran sin cambios.

## Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi). Esto le permite proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos.

### Niveles de acceso a dispositivos

Control de dispositivos controla el acceso a los siguientes niveles:

- **Tipo de dispositivo.** Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

Puede configurar el acceso a los dispositivos del siguiente modo:

- Autorizar – ✓.
  - Bloquear – ⛔.
  - Depende del bus de conexión (excepto para wifi) – 🌈.
  - Bloquear con excepciones (solo wifi) – 🚫.
- **Bus de conexión.** Un *bus de conexión* es una interfaz usada para conectar dispositivos al equipo (por ejemplo, USB o FireWire). Por lo tanto, puede restringir la conexión de todos los dispositivos, por ejemplo, vía USB.

Puede configurar el acceso a los dispositivos del siguiente modo:

- Autorizar – ✓.
- Bloquear – 0.
- **Dispositivos de confianza.** Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

Puede añadir dispositivos de confianza según los siguientes datos:

- **Dispositivos por ID.** Cada dispositivo tiene un identificador exclusivo (ID de hardware o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. ID de dispositivo de ejemplo: SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.
- **Dispositivos por modelo.** Cada dispositivos tiene un ID de proveedor (VID) y un ID de producto (PID). Puede ver los ID en las propiedades del dispositivo usando herramientas del sistema operativo. Plantilla para introducir el VID y el PID: VID\_1234&PID\_5678. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.
- **Dispositivos por máscara de ID.** Si utiliza varios dispositivos con ID similares, puede añadir dispositivos a la lista de confianza usando máscaras. El carácter \* sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter ? al introducir una máscara. Por ejemplo, WDC\_C\*.
- **Dispositivos por máscara de modelo.** Si utiliza varios dispositivos con VID y PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza usando máscaras. El carácter \* sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter ? al introducir una máscara. Por ejemplo, VID\_05AC & PID\_ \*.

Control de dispositivos regula el acceso de los usuarios a dispositivos usando [reglas de acceso](#). Control de dispositivos también le permite guardar eventos de conexión/desconexión de dispositivos. Para guardar eventos, tiene que configurar el registro de eventos en una directiva.

Quando el acceso a un dispositivo dependa del bus de conexión (estado 🌈), Kaspersky Endpoint Security no guardará ningún evento relacionado con la conexión o desconexión del dispositivo. Para que Kaspersky Endpoint Security guarde eventos de conexión/desconexión, debe autorizar el acceso al tipo de dispositivo correspondiente (estado ✓) o añadir el dispositivo a la lista de dispositivos de confianza.

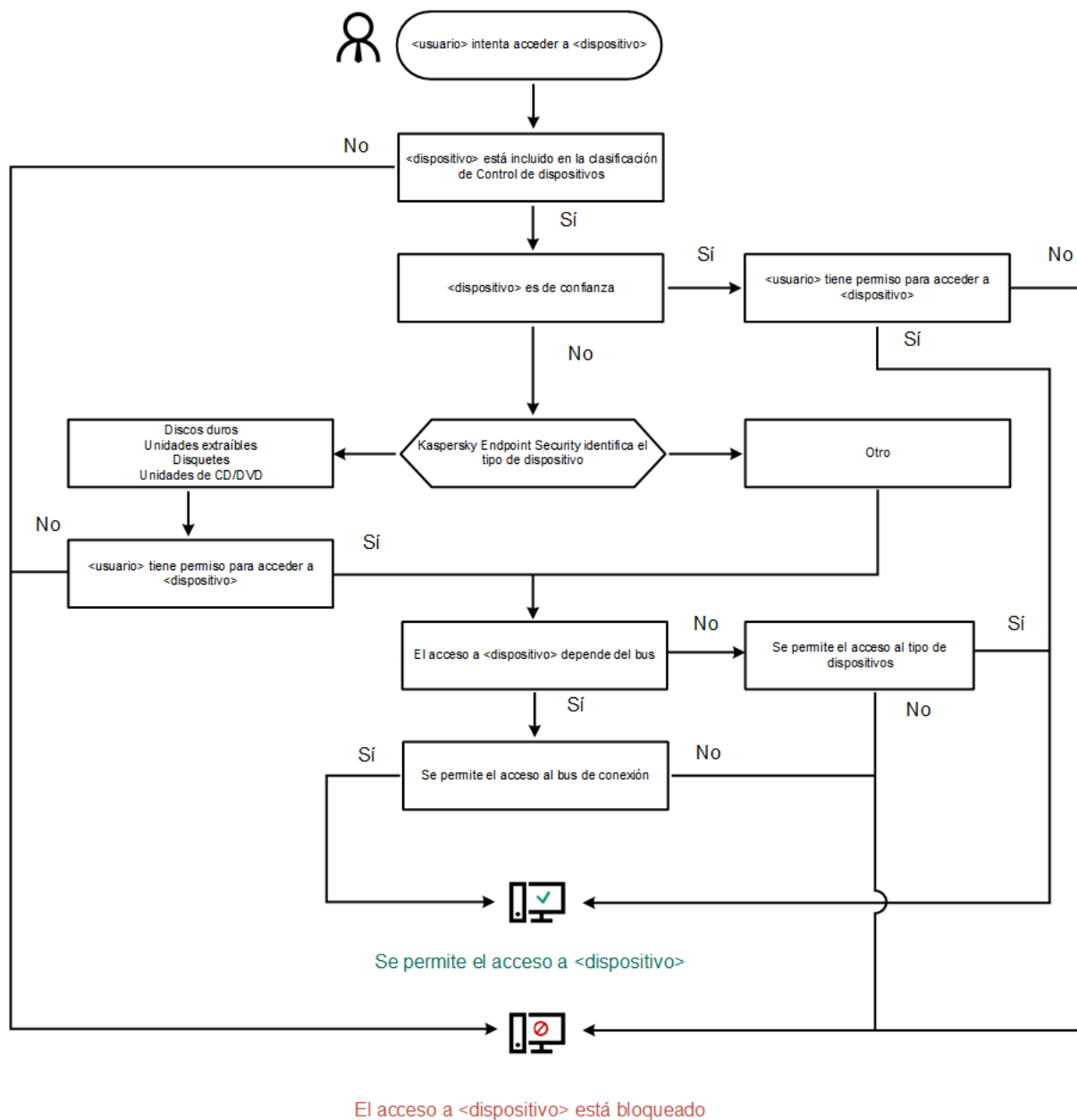
Quando un dispositivo que está bloqueado por Control de dispositivos se conecte al equipo, Kaspersky Endpoint Security bloqueará el acceso y mostrará una notificación (véase la figura siguiente).



Notificación de Control de dispositivos

## Algoritmo de funcionamiento de Control de dispositivos

Kaspersky Endpoint Security toma una decisión sobre si permitir el acceso a un dispositivo después de que el usuario conecte un dispositivo al equipo de la siguiente imagen.



Algoritmo de funcionamiento de Control de dispositivos


Si conecta un dispositivo y se le permite acceder a él, puede editar la regla de acceso y bloquear la posibilidad de utilizarlo. Cuando alguien intente acceder al dispositivo nuevamente (por ejemplo, para ver la estructura de carpetas o para realizar una operación de lectura o escritura), Kaspersky Endpoint Security bloqueará el acceso. Un dispositivo sin sistema de archivos solo se bloquea la próxima vez que se conecta el dispositivo.

Si un usuario del equipo donde se ha instalado Kaspersky Endpoint Security debe solicitar el acceso a un dispositivo que el usuario cree que se bloqueó por equivocación, envíe al usuario las [instrucciones para solicitar acceso](#).

## Activación y desactivación del Control de dispositivos

De forma predeterminada, Control de dispositivos está activado.

*Para activar o desactivar el Control de dispositivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. Utilice el interruptor **Control de dispositivos** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si el Control de dispositivos está activado, la aplicación transmite información sobre los dispositivos conectados a Kaspersky Security Center. Puede ver la lista de dispositivos conectados en Kaspersky Security Center en la carpeta **Avanzado** → **Almacenes** → **Hardware**.

## Sobre las reglas de acceso

Las *reglas de acceso* constituyen un grupo de ajustes de configuración que determinan qué usuarios pueden usar dispositivos instalados en un equipo o conectados a él. No puede añadir un dispositivo que no pertenezca a la clasificación de Control de dispositivos. El acceso a tales dispositivos está permitido para todos los usuarios.

### Reglas de acceso a dispositivos

El grupo de ajustes de configuración para una regla del acceso depende del tipo de dispositivo (consulte la tabla a continuación).

Ajustes de reglas de acceso



Dispositivos	Control de acceso	Planificar el acceso a un dispositivo	Asignación de usuarios y/o un grupo de usuarios	Prioridad	Permiso de lectura/escritura
Discos duros	✓	✓	✓	✓	✓
Unidades extraíbles	✓	✓	✓	✓	✓
Impresoras	✓	–	–	–	–
Disquetes	✓	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓	✓
Módems	✓	–	–	–	–
Unidades de cinta	✓	–	–	–	–
Dispositivos multifuncionales	✓	–	–	–	–
Lectores de tarjetas inteligentes	✓	–	–	–	–
Dispositivos Windows CE USB ActiveSync	✓	–	–	–	–


Adaptadores de red externos	✓	–	–	–	–
Dispositivos portátiles (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	–	–	–	–
Cámaras y escáneres	✓	–	–	–	–

## Reglas de acceso a dispositivos móviles




Los dispositivos móviles con Android o iOS se categorizan como dispositivos portátiles (MTP). Cuando un dispositivo móvil se conecta a un equipo, el sistema operativo determina de qué tipo de dispositivo se trata. Si las aplicaciones Android Debug Bridge (ADB), iTunes o equivalentes están instaladas, el dispositivo móvil se reconoce como dispositivo 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 de dispositivo móvil.

Tenga en cuenta las siguientes consideraciones especiales respecto al acceso a dispositivos ADB o iTunes:

- No puede configurar una planificación de acceso a dispositivos. Si el acceso a dispositivos está restringido por reglas (tienen el estado ) , los dispositivos ADB y iTunes son accesibles siempre.
- No puede configurar el acceso a dispositivos para usuarios individuales ni configurar los permisos de acceso (lectura/escritura). Si el acceso a dispositivos está restringido por reglas (tienen el estado ) , los dispositivos ADB y iTunes son accesibles para todos los usuarios con todos los permisos.
- No puede configurar el acceso a dispositivos ADB o iTunes de confianza para usuarios individuales. Si el dispositivo es de confianza, los dispositivos ADB y iTunes son accesibles para todos los usuarios.
- Si ha instalado las aplicaciones ADB o iTunes después de conectar un dispositivo al equipo, el ID único del dispositivo se podría restablecer. Esto significa que Kaspersky Endpoint Security detectará este dispositivo como dispositivo nuevo. Si un dispositivo es de confianza, vuelva a añadir el dispositivo a la lista de confianza.

De forma predeterminada, las reglas de acceso conceden acceso completo a los dispositivos para todos los usuarios en todo momento, si se permite el acceso a los buses de conexión de los tipos respectivos de dispositivos (estado ) .

## Reglas de acceso para redes wifi

Una regla del acceso de red wifi determina si el uso de redes wifi se permite (estado ) o se prohíbe (estado ) . Puede añadir una *red wifi de confianza* (estado ) a una regla. El uso de una red wifi de confianza se permite sin limitaciones. De forma predeterminada, una regla del acceso a red wifi permite acceder a cualquier red wifi.


## Reglas de acceso a los buses de conexión

Las reglas del acceso de bus de conexión determinan si la conexión de dispositivos se permite (estado ✓) o se prohíbe (estado ✗). Las reglas que permiten el acceso a los buses se crean de forma predeterminada para todos los buses de conexión presentes en la clasificación del componente Control de dispositivos.

## Edición de una regla de acceso a dispositivos

Una *regla de acceso al dispositivo* es un grupo de ajustes de configuración que determina cómo los usuarios pueden acceder a dispositivos instalados en un equipo o conectados a él. Esta configuración incluye acceso a un dispositivo específico, un horario de acceso y permisos de lectura o escritura.

*Para editar la regla de acceso a un dispositivo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

4. En el bloque **Acceso a dispositivos de almacenamiento**, seleccione la regla de acceso que desea editar. El bloque contiene dispositivos que tienen un sistema de archivos para el que puede establecer configuración de acceso adicional. De forma predeterminada, una regla de acceso al dispositivo concede a los usuarios acceso total al tipo de dispositivos especificado en cualquier momento.

a. En la columna **Acceso**, seleccione la opción de acceso al dispositivo correspondiente:

- **Autorizar.**
- **Bloquear.**
- **Depende del bus de conexión.**

Para bloquear o permitir el acceso a un dispositivo, [configure el acceso al bus de conexión](#).

- **Restringir por reglas.**

Esta opción le permite configurar los derechos de usuario, los permisos y un cronograma para el acceso al dispositivo.

b. En el bloque **Derechos de los usuarios**, haga clic en el botón **Añadir**.

Esto abre una ventana para agregar una nueva regla de acceso al dispositivo.

c. Asigne una prioridad a la *regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

Una regla tiene una prioridad específica. Si se ha añadido un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo según la regla con la mayor prioridad. Kaspersky Endpoint Security permite asignar prioridad de 0 a 10 000. Cuanto mayor sea el valor, mayor será la prioridad. En otras palabras, una entrada con valor 0 tiene la menor prioridad.


Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 al grupo de administradores y asigne una prioridad de 0 al grupo Todos.

La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. En otras palabras, si se ha añadido un usuario a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo según cualquier regla de bloqueo existente.

- d. Establezca el estado **Activo** para la regla de acceso al dispositivo.
  - e. Configure los permisos de acceso al dispositivo de los usuarios: lectura o escritura.
  - f. Seleccione los usuarios o el grupo de usuarios a los que desea aplicar la regla de acceso al dispositivo.
  - g. Configure un horario de acceso al dispositivo para los usuarios.
  - h. Haga clic en el botón **Añadir**.
5. En el bloque **Acceso a dispositivos externos**, elija la regla y configure el acceso: **Permitir**, **Bloquear** o **Depende del bus de conexión**. Si es necesario, [configure el acceso al bus de conexión](#).
  6. En el bloque **Acceso a redes wifi**, haga clic en el enlace **wifi** y configure el acceso: **Permitir**, **Bloquear** o **Bloquear con excepciones**. Si es necesario, [añada una red wifi a la lista de confianza](#).
  7. Guarde los cambios.

## Edición de una regla de acceso a bus de conexión

*Para editar una regla de acceso a bus de conexión:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Buses de conexión**.  
La ventana abierta muestra las reglas de acceso para todos los buses de conexión que se incluyen en la clasificación del componente Control de dispositivos.
4. Seleccione la regla de acceso que quiera editar.
5. En la columna **Acceso**, elija si desea permitir el acceso al bus de conexión: **Permitir** o **Bloquear**.
6. Guarde los cambios.

## Añadir una red wifi a la lista de confianza

Puede permitir que los usuarios se conecten a redes wifi que considera seguras, como una red wifi corporativa. Para ello, debe añadir la red a la lista de redes wifi de confianza. Control de dispositivos bloqueará el acceso a todas las redes wifi excepto las especificadas en la lista de confianza.

*Para añadir una red wifi a la lista de confianza:*

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

2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.

La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

4. En el bloque **Acceso a redes wifi**, haga clic en el enlace **Wifi**.

La ventana abierta muestra las reglas de acceso a la red wifi.

5. En el bloque **Acceso**, seleccione **Bloquear con excepciones**.

6. En el bloque **Redes wifi de confianza**, haga clic en el botón **Añadir**.

7. En la ventana abierta, haga lo siguiente:

a. En el campo **Nombre de red**, especifique el nombre de la red wifi que desea añadir a la lista de confianza.

b. En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación utilizada al conectarse a la red wifi de confianza.

c. En la lista desplegable **Tipo de cifrado**, seleccione el tipo de cifrado usado para asegurar el tráfico de la red wifi de confianza.

d. En el campo **Comentario**, puede especificar cualquier información sobre la red wifi que se ha añadido.

Una red wifi se considera de confianza si sus ajustes coinciden con todos los que se especifican en la regla.

8. Guarde los cambios.

## Seguimiento del uso de unidades extraíbles

La supervisión del uso de unidades extraíbles incluye lo siguiente:

- Supervisión de operaciones en archivos en unidades extraíbles.
- Supervisión de la conexión y desconexión de unidades extraíbles de confianza.

Kaspersky Endpoint Security permite supervisar la conexión y desconexión de todos los dispositivos de confianza y no solo las unidades extraíbles. Puede activar el registro de eventos en la [configuración de notificaciones](#) para el componente de Control de dispositivos. Los eventos tienen el nivel de gravedad de *Mensaje de información*.

*Para activar el seguimiento del uso de unidades extraíbles:*

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

2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes wifi**.



La ventana abierta muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

4. En el bloque **Acceso a dispositivos de almacenamiento**, seleccione **Unidades extraíbles**.
5. En la ventana que se abre, seleccione la pestaña **Registro**.
6. Active el interruptor **Registro**.
7. En el bloque **Operaciones de archivo**, seleccione las operaciones que desea supervisar: **Escribir, Eliminar**.
8. En el bloque **Filtrar por formatos de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas deben ser registradas por Control de dispositivos.
9. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.
10. Guarde los cambios.

Como resultado, cuando los usuarios escriben en archivos ubicados en unidades extraíbles o eliminan archivos de unidades extraíbles, Kaspersky Endpoint Security guarda la información sobre esas operaciones en el registro de eventos y envía eventos a Kaspersky Security Center. Puede ver eventos asociados con archivos en unidades extraíbles en la Consola de administración de Kaspersky Security Center, en el espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Eventos**. Para que los eventos se muestren en el registro de eventos local de Kaspersky Endpoint Security, debe seleccionar la casilla **Operación de archivo realizada** en la [configuración de notificación](#) para el componente Control de dispositivos.

## Cambiar la duración del almacenamiento en caché

El componente Control de dispositivos registra eventos relacionados con los dispositivos supervisados, como la conexión y desconexión de un dispositivo, la lectura de un archivo de un dispositivo, la escritura de un archivo en un dispositivo y otros eventos. Luego, Control de dispositivos permite o bloquea la acción de acuerdo con la configuración de Kaspersky Endpoint Security.

Control de dispositivos guarda información sobre eventos durante un período específico llamado *período de almacenamiento en caché*. Si la información sobre un evento se almacena en caché y este evento se repite, no es necesario notificarlo a Kaspersky Endpoint Security ni mostrar otro mensaje para otorgar acceso a la acción correspondiente, como conectar un dispositivo. Esto hace que sea más conveniente trabajar con un dispositivo.

Un evento se considera un evento duplicado si toda la configuración de los eventos siguientes coincide con el registro en el caché:

- ID de dispositivo
- SID de la cuenta de usuario que intenta acceder
- Categoría de dispositivo
- Acción realizada con el dispositivo
- Veredicto del permiso de solicitud para esta acción: permitido o denegado
- Ruta del proceso utilizado para realizar la acción
- Archivo al que se accede

Antes de cambiar el período de almacenamiento en caché, [desactive Autoprotección de Kaspersky Endpoint Security](#). Después de cambiar el período de almacenamiento en caché, active Autoprotección.

Para cambiar el período de almacenamiento en caché:

1. Abra el editor de registro en el equipo.
2. En el editor de registro, vaya a la siguiente sección:
  - Para sistemas operativos de 64 bits:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\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 en los que Control de dispositivos debe guardar información sobre un evento antes de que se elimine esta información.

## Acciones con dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

Para trabajar con dispositivos de confianza, puede otorgar acceso a un usuario individual, a un grupo de usuarios o a todos los usuarios de la organización.

Por ejemplo, si su organización no permite el uso de unidades extraíbles, pero los administradores usan unidades extraíbles en su trabajo, puede permitir unidades extraíbles solo para un grupo de administradores. Para hacerlo, añada unidades extraíbles a la lista de confianza y configure los permisos de acceso de usuario.

No se recomienda añadir más de 1000 dispositivos de confianza, ya que esto puede provocar inestabilidad en el sistema.

Kaspersky Endpoint Security le permite añadir un dispositivo a la lista de confianza de las siguientes maneras:

- Si no utiliza Kaspersky Security Center en su organización, puede conectar el dispositivo al equipo y [añadirlo a la lista de confianza en la configuración de la aplicación](#). Para distribuir la lista de dispositivos de confianza a todos los equipos de su organización, puede activar la combinación de listas de dispositivos de confianza en una directiva o usar el [procedimiento de exportación/importación](#).
- Si utiliza Kaspersky Security Center en su organización, puede detectar todos los dispositivos conectados remotamente y [crear una lista de dispositivos de confianza en la directiva](#). La lista de dispositivos de confianza estará disponible en todos los equipos a los que se aplica la directiva.

Kaspersky Endpoint Security permite controlar el uso de dispositivos de confianza (conexión y desconexión). Puede activar el registro de eventos en la [configuración de notificaciones](#) para el componente de Control de dispositivos. Los eventos tienen el nivel de severidad *Informativo*.


Kaspersky Endpoint Security tiene las siguientes limitaciones cuando trabaja con dispositivos de confianza:

- Las versiones 11.0.0–11.2.0 del complemento de administración de Kaspersky Endpoint Security no pueden funcionar con una lista de dispositivos de confianza creada en Kaspersky Endpoint Security versión 11.3.0 y 11.4.0. Para trabajar con una lista de dispositivos de confianza de estas versiones, el complemento de administración debe actualizarse a la versión 11.3.0 y 11.4.0, respectivamente.
- El complemento de administración de Kaspersky Endpoint Security versión 11.3.0 y 11.4.0 no puede funcionar con una lista de dispositivos de confianza creada en Kaspersky Endpoint Security versión 11.2.0 o anterior. Para que estas versiones funcionen con una lista de dispositivos de confianza, la aplicación debe actualizarse a la versión 11.3.0 y 11.4.0, respectivamente. También puede enviar una solicitud con una descripción de su situación al Soporte técnico a través de [Kaspersky CompanyAccount](#) <sup>2</sup>.
- Para migrar una lista de dispositivos de confianza de Kaspersky Endpoint Security versión 11.2.0 a la versión 11.3.0, envíe una solicitud que contenga una descripción de su situación al Soporte técnico a través de [Kaspersky CompanyAccount](#) <sup>2</sup>.

## Adición de un dispositivo a la lista de confianza en la interfaz de la aplicación

De forma predeterminada, al añadir un dispositivo a la lista de dispositivos de confianza, a todos los usuarios (el grupo de usuarios Todos) se les concede acceso a este dispositivo.

*Para añadir un dispositivo a la lista de confianza en la interfaz de la aplicación:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos de confianza**.  
Esto abre la lista de dispositivos de confianza.
4. Haga clic en el botón **Seleccionar**.  
Esto abre la lista de dispositivos conectados. La lista de dispositivos depende del valor que se seleccione en la lista desplegable **Mostrar dispositivos conectados**.
5. En la lista de dispositivos, seleccione el dispositivo que desea añadir a la lista de confianza.
6. En el campo **Comentario**, puede proporcionar cualquier información relevante sobre el dispositivo de confianza.
7. Seleccione los usuarios o el grupo de usuarios a los que desea permitir el acceso a los dispositivos de confianza.
8. Guarde los cambios.

## Adición de un dispositivo a la lista de confianza desde Kaspersky Security Center

Kaspersky Security Center recibe información sobre los dispositivos si Kaspersky Endpoint Security está instalado en los equipos y el [Control de dispositivos está activado](#). No se puede añadir un dispositivo a la lista de confianza a menos que la información sobre ese dispositivo esté disponible en Kaspersky Security Center.

Puede añadir un dispositivo a la lista de confianza según los datos siguientes:

- **Dispositivos por ID.** Cada dispositivo tiene un identificador exclusivo (ID de hardware o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. ID de dispositivo de ejemplo: SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.
- **Dispositivos por modelo.** Cada dispositivos tiene un ID de proveedor (VID) y un ID de producto (PID). Puede ver los ID en las propiedades del dispositivo usando herramientas del sistema operativo. Plantilla para introducir el VID y el PID: VID\_1234&PID\_5678. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.
- **Dispositivos por máscara de ID.** Si utiliza varios dispositivos con ID similares, puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `WDC_C*`.
- **Dispositivos por máscara de modelo.** Si utiliza varios dispositivos con VID y PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `VID_05AC & PID_*`.

*Para añadir dispositivos a la lista de dispositivos de confianza:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de dispositivos**.
6. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.
7. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de dispositivos de confianza para todos los equipos de la empresa.  
  
Se fusionarán las listas de dispositivos de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Los dispositivos de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar dispositivos de confianza de la directiva principal.
8. Haga clic en el botón **Añadir** y seleccione un método para añadir un dispositivo a la lista de confianza.
9. Para filtrar dispositivos, seleccione un tipo de dispositivo de la lista desplegable **Tipo de dispositivo** (por ejemplo, **Unidades extraíbles**).
10. En el campo **Nombre o modelo**, introduzca el ID de dispositivo, modelo (VID y PID) o máscara, según el método para añadir seleccionado.

Añadir dispositivos por máscara de modelo (VID y PID) funciona de la siguiente manera: si introduce una máscara de modelo que no coincida con ningún modelo, Kaspersky Endpoint Security verifica si el ID de dispositivo (HWID) coincide con la máscara. Kaspersky Endpoint Security solo verifica la parte del ID de dispositivo que determina el fabricante y el tipo de dispositivo (SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000). Si la máscara de modelo coincide con esta parte del ID de dispositivo, los dispositivos que coinciden con la máscara se añadirán a la lista de dispositivos de confianza en el equipo. Al mismo tiempo, la lista de dispositivos en Kaspersky Security Center permanece vacía cuando hace clic en el botón **Actualizar**. Para mostrar la lista de dispositivos correctamente, puede añadir dispositivos por la máscara de ID de dispositivo.

11. Para filtrar dispositivos, en el campo **Nombre del equipo**, introduzca el nombre del equipo o una máscara para el nombre del equipo al que está conectado el dispositivo.

El carácter **\*** sustituye cualquier conjunto de caracteres. El carácter **?** sustituye cualquier carácter único.

12. Haga clic en el botón **Actualizar**.

La tabla muestra una lista de dispositivos que satisfacen los criterios de filtrado definidos.

13. Seleccione las casillas de verificación junto a los nombres de los dispositivos que quiera añadir a la lista de confianza.

14. En el campo **Comentario**, introduzca una descripción del motivo para añadir dispositivos a la lista de confianza.

15. Haga clic en el botón **Seleccionar**, que se encuentra a la derecha del campo **Permitir a usuarios y/o grupos de usuarios**.

16. Seleccione un usuario o un grupo de Active Directory y confirme su selección.

De forma predeterminada, el acceso a los dispositivos de confianza está permitido para el grupo "Todos".

17. Guarde los cambios.

Cuando se conecta un dispositivo, Kaspersky Endpoint Security comprueba la lista de dispositivos de confianza para un usuario autorizado. Si el dispositivo es de confianza, Kaspersky Endpoint Security permite el acceso al dispositivo con todos los permisos, incluso si se deniega el acceso al tipo de dispositivo o al bus de conexión. Si el dispositivo no es de confianza y se le deniega el acceso, puede [solicitar acceso al dispositivo bloqueado](#).

## Exportación e importación de la lista de dispositivos de confianza


Para distribuir la lista de dispositivos de confianza a todos los equipos de su organización, puede usar el procedimiento de exportación/importación.

Por ejemplo, si necesita distribuir una lista de unidades extraíbles de confianza, tiene que hacer lo siguiente:

1. Conecte las unidades extraíbles a su equipo secuencialmente.
2. En la configuración de Kaspersky Endpoint Security, [añada las unidades extraíbles a la lista de confianza](#). De ser necesario, configure los permisos de acceso de usuario. Por ejemplo, permita que solo los administradores accedan a las unidades extraíbles.
3. Exporte la lista de dispositivos de confianza en la configuración de Kaspersky Endpoint Security (consulte las instrucciones más abajo).

4. Distribuya el archivo de la lista de dispositivos de confianza a otros equipos de su organización. Por ejemplo, coloque el archivo en una carpeta compartida.
5. Importe la lista de dispositivos de confianza en la configuración de Kaspersky Endpoint Security en otros equipos de la organización (consulte las instrucciones más abajo).

*Para importar o exportar la lista de dispositivos de confianza:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos de confianza**.  
Esto abre la lista de dispositivos de confianza.
4. Para exportar la lista de dispositivos de confianza:
  - a. Seleccione los dispositivos de confianza que desee exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de dispositivos de confianza y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de dispositivos de confianza al archivo XML.
5. Para importar la lista de dispositivos de confianza:
  - a. En la lista desplegable **Importar**, seleccione la acción correspondiente: **Importar y añadir al existente** o **Importar y sustituir el existente**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de dispositivos de confianza.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de dispositivos de confianza, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
6. Guarde los cambios.

Cuando se conecta un dispositivo, Kaspersky Endpoint Security comprueba la lista de dispositivos de confianza para un usuario autorizado. Si el dispositivo es de confianza, Kaspersky Endpoint Security permite el acceso al dispositivo con todos los permisos, incluso si se deniega el acceso al tipo de dispositivo o al bus de conexión.

## Obtención de acceso a un dispositivo bloqueado

Al configurar el componente Control de dispositivos, existe el riesgo de bloquear inadvertidamente el acceso a un dispositivo que se necesita para trabajar.

Si no utiliza Kaspersky Security Center en su organización, puede brindar acceso a un dispositivo a través de los ajustes de Kaspersky Endpoint Security. Por ejemplo, puede [añadir el dispositivo a la lista de dispositivos de confianza](#) o [desactivar el componente Control de dispositivos](#) en forma temporal.

Si en su organización sí utilizan Kaspersky Security Center y los equipos tienen una directiva aplicada, puede otorgar acceso al dispositivo a través de la Consola de administración.

## Modo con conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo con conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. También es necesario que el equipo pueda comunicarse con el Servidor de administración.

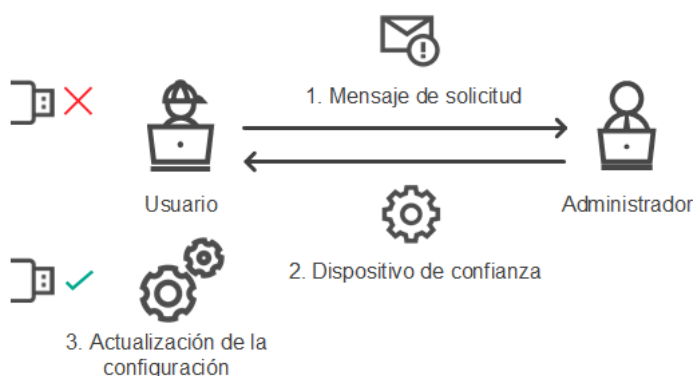
Estos son los pasos para otorgar acceso a un dispositivo en el modo con conexión:

1. El usuario envía un mensaje con una solicitud de acceso al administrador.

2. El administrador añade el dispositivo a la lista de dispositivos de confianza.

Para añadir un dispositivo de confianza, existen dos alternativas: modificar una directiva aplicada al grupo de administración o modificar la configuración local de la aplicación instalada en un equipo específico.

3. El administrador actualiza la configuración de Kaspersky Endpoint Security en el equipo del usuario.



Esquema para otorgar acceso a un dispositivo en el modo con conexión

## Modo sin conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo sin conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. En la configuración de la directiva, dentro de la sección **Control de dispositivos**, la casilla **Permitir solicitudes de acceso temporal** debe estar activada.

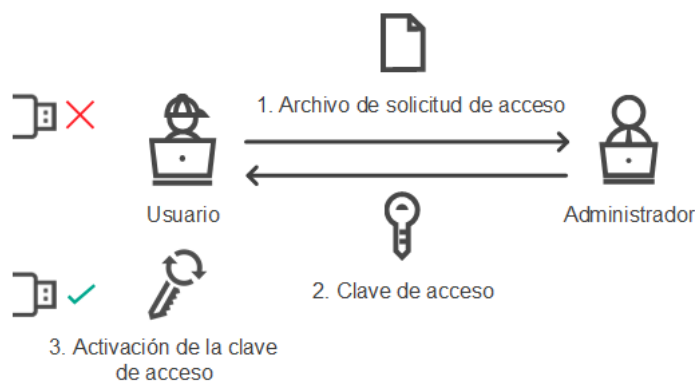
Si necesita otorgar acceso temporal a un dispositivo, pero no puede [añadirlo a la lista de dispositivos de confianza](#), puede utilizar el modo sin conexión. Este modo permite otorgar acceso a un dispositivo bloqueado aun cuando un equipo no tiene conexión a la red o se encuentra fuera de la red corporativa.

Estos son los pasos para otorgar acceso a un dispositivo en el modo sin conexión:

1. El usuario crea un archivo de solicitud de acceso y se lo envía al administrador.

2. Con el archivo de solicitud de acceso, el administrador crea una clave de acceso y se la envía al usuario.

3. El usuario activa la clave de acceso.



Esquema para otorgar acceso a un dispositivo en el modo sin conexión

## Modo con conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo con conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. También es necesario que el equipo pueda comunicarse con el Servidor de administración.

*Para solicitar acceso a un dispositivo bloqueado como usuario:*

1. Conecte el dispositivo al equipo.

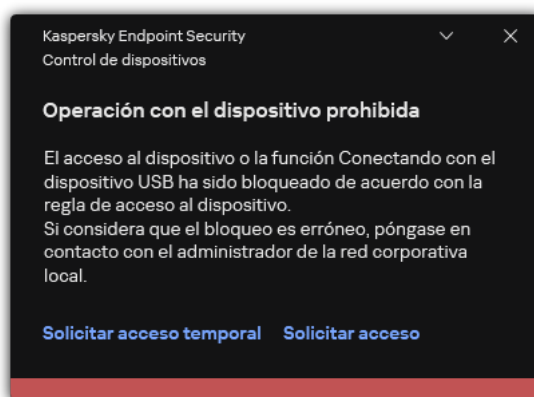
Kaspersky Endpoint Security mostrará una notificación para indicar que el acceso al dispositivo está bloqueado (vea la imagen de más abajo).

2. Haga clic en el enlace **Solicitar acceso**.

Se abre una ventana con un mensaje para el administrador. El mensaje contendrá información sobre el dispositivo bloqueado.

3. Haga clic en el botón **Enviar**.

El administrador recibirá, por correo electrónico u otro medio, un mensaje con una solicitud de acceso. Para más detalles sobre cómo se procesan las solicitudes de los usuarios, consulte la [Ayuda de Kaspersky Security Center](#). El usuario podrá acceder al dispositivo una vez que [se lo añada a la lista de dispositivos de confianza](#) y la configuración de Kaspersky Endpoint Security se actualice en el equipo.



Notificación de Control de dispositivos



## 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 solicitud de acceso temporal** debe estar activada.

*Para solicitar acceso a un dispositivo bloqueado como usuario:*

1. Conecte el dispositivo al equipo.  
Kaspersky Endpoint Security mostrará una notificación para indicar que el acceso al dispositivo está bloqueado (vea la imagen de más abajo).
2. Haga clic en el enlace **Solicitar acceso temporal**.  
Esto abre una ventana que incluye una lista de dispositivos conectados.
3. En la lista de dispositivos conectados, seleccione el dispositivo al que desee obtener acceso.
4. Haga clic en **Generar archivo de solicitud de acceso**.
5. En el campo **Duración del acceso**, especifique el período de tiempo durante el que desea disponer de acceso al dispositivo.
6. Guarde el archivo en el equipo.

Como resultado, se descargará al equipo un archivo de solicitud de acceso (cuya extensión será \*.akey). Envíe este archivo al administrador de la LAN corporativa utilizando cualquier método a su disposición.



Notificación de Control de dispositivos

[Cómo puede el administrador crear una clave de acceso para el dispositivo bloqueado en la Consola de administración \(MMC\)](#)


1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la lista de equipos cliente, seleccione el equipo de un usuario que necesite obtener acceso temporal a un dispositivo bloqueado.
5. En el menú contextual del equipo, seleccione el elemento **Conceder acceso en modo sin conexión**.
6. En la ventana que se abre, seleccione la ficha **Control de dispositivos**.
7. Haga clic en el botón **Examinar** y descargue el archivo de solicitud de acceso que recibió del usuario.  
Verá información sobre el dispositivo bloqueado al que el usuario desea acceder.
8. De ser necesario, cambie el valor del parámetro **Duración del acceso**.  
De manera predeterminada, el valor de **Duración del acceso** es el mismo que indicó el usuario al crear el archivo de solicitud de acceso.
9. Especifique el valor del parámetro **Activar el**.  
Este parámetro define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado mediante la clave de acceso proporcionada.
10. Guarde el archivo clave de acceso en el equipo.

[Cómo puede el administrador crear una clave de acceso para el dispositivo bloqueado en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. En la lista de equipos cliente, seleccione el equipo de un usuario que necesite obtener acceso temporal a un dispositivo bloqueado.
3. Haga clic en el botón de elipsis ( ) sobre la lista de equipos y, a continuación, en el botón **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione la sección **Control de dispositivos**.
5. Haga clic en el botón **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 de tiempo durante el que se puede activar la clave de acceso en el dispositivo. Este parámetro define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado mediante la clave de acceso proporcionada.
8. Guarde el archivo clave de acceso en el equipo.

Como resultado, se descargará al equipo una clave de acceso para el dispositivo bloqueado. Los archivos clave de acceso tienen la extensión \*.acode. Envíe el archivo clave de acceso al usuario utilizando cualquier método a su disposición.

*Para activar una clave de acceso como usuario:*

1. En la [ventana de la aplicación principal](#), haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Solicitud de acceso**, haga clic en el botón **Solicitar acceso al dispositivo**.
4. En la ventana que se abre, haga clic en el botón **Activar clave de acceso**.
5. En la ventana que se abre, seleccione el archivo con la clave de acceso que le envió el administrador de la LAN corporativa. Se abrirá una ventana con información sobre el acceso que le han otorgado.
6. Haga clic en **Aceptar**.


Como resultado, el usuario obtendrá acceso al dispositivo por el tiempo que haya definido el administrador. El usuario tendrá acceso completo (derechos de lectura y de escritura) al dispositivo. Cuando la clave caduque, se bloqueará el acceso al dispositivo. Si el usuario necesita acceso permanente al dispositivo, [añada el dispositivo a la lista de dispositivos de confianza](#).

## Edición de plantillas de mensajes de Control de dispositivos

Cuando el usuario intenta acceder a un dispositivo bloqueado, Kaspersky Endpoint Security muestra un mensaje que afirma que el acceso al dispositivo está bloqueado o que una operación con los contenidos del dispositivo está prohibida. Si el usuario cree que el acceso al dispositivo se bloqueó por error o que una operación con contenidos del dispositivo se prohibió por error, el usuario puede enviar un mensaje al administrador de la red corporativa local haciendo clic en el enlace del mensaje mostrado sobre la acción bloqueada.

Hay plantillas disponibles para mensajes sobre el acceso bloqueado a dispositivos o sobre operaciones prohibidas con los contenidos del dispositivo, así como para mensajes enviados al administrador. Puede modificar las plantillas de los mensajes.

*Para editar la plantilla para mensajes de Control de dispositivos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Modelos de mensajes**, configure las plantillas para mensajes de Control de dispositivos:
  - **Mensaje sobre el bloqueo.** Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo.
  - **Mensaje para el administrador.** Una plantilla del mensaje que se envía al administrador de la LAN cuando el usuario cree que el acceso al dispositivo está bloqueado o que se ha prohibido una operación con el contenido del dispositivo por error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso al dispositivo**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.
4. Guarde los cambios.

## Anti-Bridging

Anti-Bridging impide establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red. La finalidad es resguardar la red de la empresa de los ataques que puedan realizarse a través de redes desprotegidas y no autorizadas.

Para regular la posibilidad de establecer conexiones de red, Anti-Bridging utiliza *reglas de conexión*.

Las reglas de conexión se crean para estos tipos predefinidos de dispositivos:

- Adaptadores de red;
- Adaptadores wifi;
- Módems.

Si una regla de conexión está activada, Kaspersky Endpoint Security:


- Bloquea la conexión activa al establecer una nueva conexión si el tipo de dispositivo especificado en la regla se usa para ambas conexiones;

- Bloquea las conexiones que se establecen usando los tipos de dispositivos para los que se utilizan reglas de prioridad inferior.

## Activar el componente Anti-Bridging

La función Anti-Bridging está desactivada de forma predeterminada.


*Para activar el componente Anti-Bridging:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Anti-Bridging**.
4. Utilice el interruptor **Activar el componente Anti-Bridging** para activar o desactivar esta función.
5. Guarde los cambios.

Con Anti-Bridging activado, Kaspersky Endpoint Security bloquea conexiones ya establecidas según lo indicado en las reglas de conexión.


## Cambio del estado de una regla de conexión

*Para cambiar el estado de una regla de conexión:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Anti-Bridging**.
4. En el bloque **Reglas para dispositivos**, seleccione la regla cuyo estado desea cambiar.
5. Utilice los interruptores de la columna **Control** para activar o desactivar la regla.
6. Guarde los cambios.

## Cambio de la prioridad de una regla de conexión

*Para cambiar la prioridad de una regla de conexión:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione → **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración de acceso**, haga clic en el botón **Anti-Bridging**.
4. En el bloque **Reglas para dispositivos**, seleccione la regla cuya prioridad desea cambiar.
5. Utilice los botones **Arriba/Abajo** para establecer la prioridad de la regla de conexión.

Cuanto más arriba está una regla en la tabla, mayor es su prioridad. Anti-Bridging bloquea todas las conexiones excepto una conexión establecida usando el tipo de dispositivo para el que se utiliza la regla de la prioridad más alta.

6. Guarde los cambios.

## Control de anomalías adaptativo

Este componente está disponible solo para Kaspersky Endpoint Security for Business Advanced y Kaspersky Total Security for Business. Para obtener más información sobre Kaspersky Endpoint Security for Business, visite el [sitio web de Kaspersky](#).

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos en una red de la empresa. El Control de anomalías adaptativo utiliza un conjunto de reglas para supervisar el comportamiento inusual (por ejemplo, la regla *Inicio de Microsoft PowerShell desde la aplicación Office*). Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa. Puede configurar el modo en que el Control de anomalías adaptativo gestiona cada regla y, por ejemplo, permitir la ejecución de scripts de PowerShell que automatizan determinadas tareas de flujo de trabajo. Kaspersky Endpoint Security actualiza el conjunto de reglas junto con las bases de datos de la aplicación. Las actualizaciones de los conjuntos de reglas deben [confirmarse manualmente](#).

## Parámetros del Control de anomalías adaptativo

Para configurar el Control de anomalías adaptativo se tienen que realizar los pasos siguientes:

1. Autoaprendizaje del Control de anomalías adaptativo.

Después de habilitar el Control de anomalías adaptativo, sus reglas funcionan en el *modo de autoaprendizaje*. Durante el aprendizaje, el Control de anomalías adaptativo supervisa la activación de reglas y envía eventos de activación a Kaspersky Security Center. Cada regla tiene su propia duración del modo de autoaprendizaje. La duración del modo de autoaprendizaje es establecida por los expertos de Kaspersky. Por lo general, el modo de autoaprendizaje está activo durante dos semanas.

Si una regla no se ha activado nunca durante el autoaprendizaje, el Control de anomalías adaptativo considerará las acciones asociadas a esta regla como no típicas. Kaspersky Endpoint Security bloqueará todas las acciones asociadas a esa regla.

Si se activó una regla durante el autoaprendizaje, Kaspersky Endpoint Security registra los eventos en el [informe de activación de las reglas](#) y en el repositorio de **Activación de reglas en el estado Aprendizaje inteligente**.

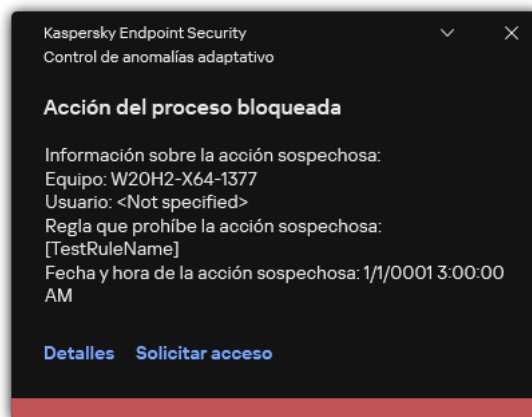
2. Analizar el informe de activación de las reglas.

El administrador analiza el [informe de activación de las reglas](#) o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. A continuación, el administrador puede seleccionar el comportamiento del Control de anomalías adaptativo cuando se active la regla para bloquearlo o permitirlo. El administrador también puede seguir supervisando el funcionamiento de la regla y ampliar su duración durante el modo de autoaprendizaje. Si el administrador no realiza ninguna acción, la aplicación también seguirá funcionando en el modo de autoaprendizaje. El plazo de aprendizaje se reiniciará.

El Control de anomalías adaptativo se configura en tiempo real. El Control de anomalías adaptativo se configura a través de los siguientes canales:

- El Control de anomalías adaptativo empieza a bloquear automáticamente las acciones asociadas con las reglas que no se activaron nunca en el modo de autoaprendizaje.
- Kaspersky Endpoint Security añade nuevas reglas o elimina las obsoletas.
- El administrador configura el funcionamiento del Control de anomalías adaptativo tras revisar el informe de activación de las reglas o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. Se recomienda comprobar el informe de activación de las reglas o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**.

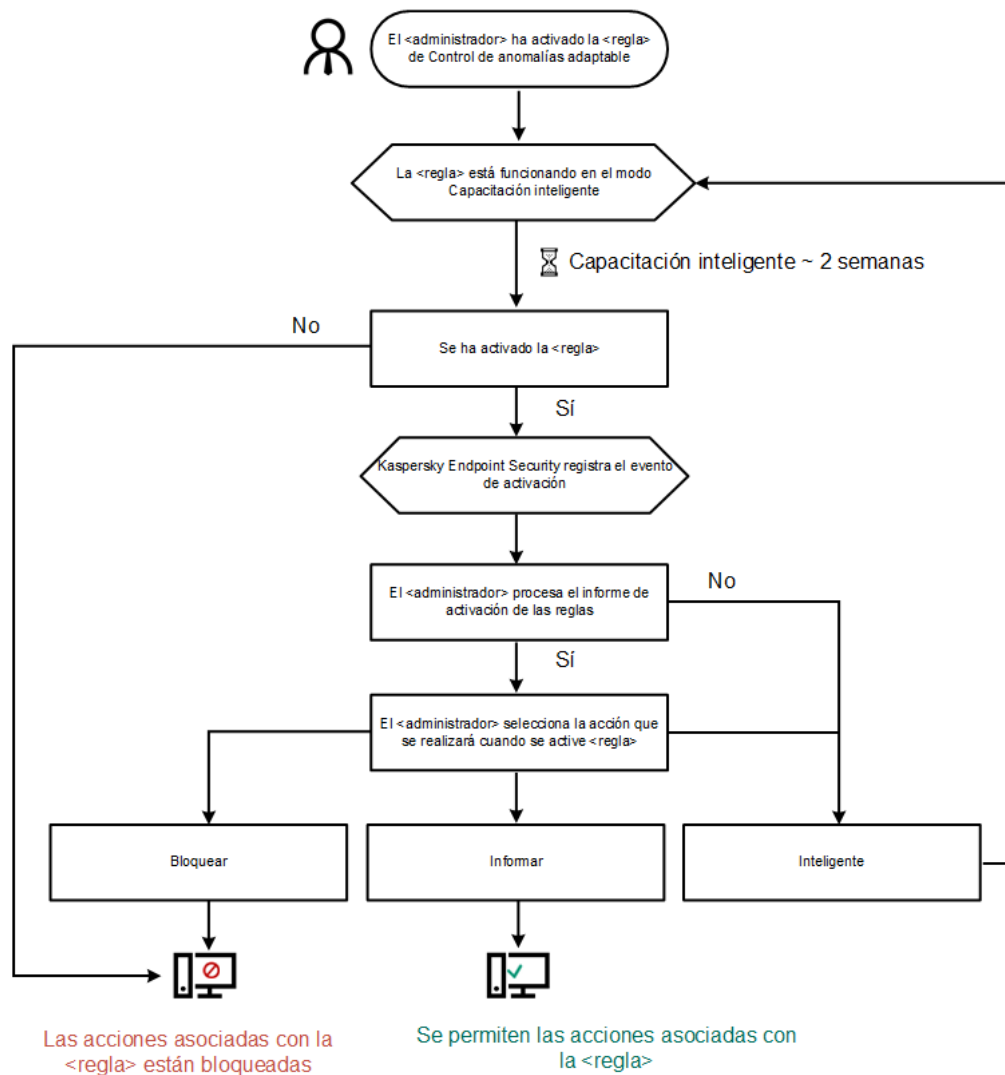
Cuando una aplicación maliciosa intenta realizar una acción, Kaspersky Endpoint Security bloqueará dicha acción y mostrará una notificación (vea la figura a continuación).



Notificación del Control de anomalías adaptativo

## Algoritmo de funcionamiento del Control de anomalías adaptativo

Kaspersky Endpoint Security decide si se autoriza o se bloquea una acción que esté asociada con una regla de acuerdo al siguiente algoritmo (consulte la siguiente figura).




Algoritmo de funcionamiento del Control de anomalías adaptativo

## Activación y desactivación del Control de anomalías adaptativo

De manera predeterminada, el Control adaptable de anomalías está activado.

Para activar o desactivar Control de anomalías adaptativo, haga lo siguiente:

1. En la [ventana de la aplicación principal](#), haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. Utilice interruptor **Control de anomalías adaptativo** para activar o desactivar el componente.
4. Guarde los cambios.


Como resultado, el Control de anomalías adaptativo cambiará al modo de entrenamiento. Durante el entrenamiento, el Control de anomalías adaptativo supervisa la activación de reglas. Cuando se completa el entrenamiento, el Control de anomalías adaptativo comienza a bloquear acciones que no son típicas de los equipos de una red empresarial.



Si su organización ha comenzado a usar herramientas nuevas y el Control de anomalías adaptativo bloquea las acciones de esas herramientas, puede restablecer los resultados del modo de entrenamiento y repetir el entrenamiento. Para ello, necesita [cambiar la acción que se realiza cuando se activa la regla](#) (por ejemplo, configurarla en **Notificar**). Luego debe volver a activar el modo de entrenamiento (establecer el valor **Inteligente**).


## Activación y desactivación de una regla del Control de anomalías adaptativo

*Para activar o desactivar una regla del Control adaptable de anomalías:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.  
Se abre la lista de reglas de Control de anomalías adaptativo.
4. En la tabla, seleccione un conjunto de reglas (por ejemplo, *Actividad de las aplicaciones de oficina*) y amplíe el conjunto.
5. Seleccione una regla (por ejemplo, *Iniciar Windows PowerShell desde aplicaciones de oficina*).
6. Utilice el interruptor en la columna **Estado** para activar o desactivar la regla de Control de anomalías adaptativo.
7. Guarde los cambios.

## Cambio de la acción que se realiza al activarse una regla del Control de anomalías adaptativo

*Para cambiar lo que ocurre cuando se activa una regla del Control de anomalías adaptativo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.  
Se abre la lista de reglas de Control de anomalías adaptativo.
4. Seleccione una regla en la tabla.
5. Haga clic en el botón **Editar**.  
Se abre la ventana de propiedades de las reglas de Control de anomalías adaptativo.
6. En el bloque **Acción**, seleccione una de las opciones siguientes:

- **Inteligente.** Si elige esta opción, la regla del Control de anomalías adaptativo funcionará en estado Aprendizaje inteligente durante el plazo definido por los expertos de Kaspersky. En este modo, cuando una regla del Control de anomalías adaptativo se activa, Kaspersky Endpoint Security permite la actividad determinada por la regla y añade una entrada de registro en el repositorio **Activación de reglas en el estado Aprendizaje inteligente** del Servidor de administración de Kaspersky Security Center. Cuando concluye el período de trabajo en el estado Aprendizaje inteligente, Kaspersky Endpoint Security bloquea la actividad determinada por la regla y añade una entrada de registro con información sobre la actividad.
- **Bloquear.** Si se selecciona esta acción, cuando se active una regla del Control de anomalías adaptativo, Kaspersky Endpoint Security bloqueará la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.
- **Notificar.** Si se selecciona esta acción, cuando se active una regla de Control de anomalías adaptativo, Kaspersky Endpoint Security permitirá la actividad definida por la regla y guardará en un registro una entrada con información sobre la actividad.


7. Guarde los cambios.

## Crear una exclusión de una regla del Control de anomalías adaptativo

No es posible crear más de 1000 exclusiones para las reglas del Control de anomalías adaptativo. No se recomienda crear más de 200 exclusiones. Si necesita reducir el número de exclusiones que utiliza, considere usar máscaras en la configuración de las exclusiones.

Una exclusión de una regla del Control de anomalías adaptable incluye una descripción de los objetos de origen y de destino. El *objeto de origen* es el que realiza las acciones. El *objeto de destino* es el que se ve afectado por dichas acciones. Supongamos que se abre un archivo denominado `archivo.xlsx`. Como resultado se carga en la memoria del equipo un archivo de biblioteca con la extensión DLL. Esta biblioteca se utiliza en un navegador (archivo ejecutable denominado `browser.exe`). En el marco de este ejemplo, `archivo.xlsx` es el objeto de origen, Excel es el proceso de origen, `navegador.exe` es el objeto de destino y Navegador es el proceso de destino.

*Para crear una exclusión de una regla del Control de anomalías adaptativo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.  
Se abre la lista de reglas de Control de anomalías adaptativo.
4. Seleccione una regla en la tabla.
5. Haga clic en el botón **Editar**.  
Se abre la ventana de propiedades de las reglas de Control de anomalías adaptativo.
6. En el bloque **Exclusiones**, haga clic en el botón **Añadir**.  
Se abre la ventana de propiedades de exclusiones.
7. Seleccione el usuario para el que desea configurar una exclusión.

El Control de anomalías adaptativo no admite exclusiones para grupos de usuarios. Si selecciona un grupo de usuarios, Kaspersky Endpoint Security no aplicará la exclusión.

8. En el campo **Descripción**, describa la exclusión.

9. Defina los parámetros del objeto de origen o de el proceso de origen iniciados por el objeto:

- **Proceso de origen.** Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, C:\Dir\Archivo.exe o Dir\\*.exe).

- **Hash del proceso de origen.** Código hash del archivo.

- **Objeto de origen.** Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, C:\Dir\Archivo.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://<objeto>`, reemplazando `<objeto>` con el nombre del objeto (por ejemplo, `object://sitio.web.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`). También puede usar máscaras (por ejemplo, `object://*C:\Windows\temp\*`).

- **Hash del objeto de origen.** Código hash del archivo.

La regla del Control de anomalías adaptable no se aplicará a las acciones que el objeto realice o a los procesos que el objeto inicie.

10. Especifique los parámetros del objeto de destino o de los procesos de destino iniciados en los que el objeto esté involucrado.

- **Proceso objetivo.** Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, C:\Dir\Archivo.exe o Dir\\*.exe).

- **Hash del proceso de destino.** Código hash del archivo.

- **Objeto objetivo.** Comando para iniciar el proceso de destino. Para especificar el comando, utilice el modelo `object://<comando>` (por ejemplo, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`). También puede usar máscaras (por ejemplo, `object://*C:\Windows\temp\*`).


- **Hash de objeto de destino.** Código hash del archivo.

La regla del Control de anomalías adaptable no se aplicará a las acciones que afecten al objeto o a los procesos en los que el objeto esté involucrado.

11. Guarde los cambios.

## Importar e importar exclusiones para las reglas del Control de anomalías adaptativo

*Para exportar o importar la lista de exclusiones para las reglas seleccionadas:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.  
Se abre la lista de reglas de Control de anomalías adaptativo.
4. Para exportar la lista de reglas:
  - a. Seleccione las reglas cuyas excepciones quiera exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - d. Confirme que desea exportar solo las exclusiones seleccionadas o exportar la lista completa de exclusiones.
  - e. Guarde el archivo.
5. Para importar la lista de reglas:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
6. Guarde los cambios.

## Actualización de las reglas del Control de anomalías adaptativo

Cuando se actualizan las bases de datos antivirus, la tabla de reglas del Control de anomalías adaptativo puede modificarse: puede ocurrir que se incorporen reglas nuevas y que se eliminen otras existentes. Si hay una actualización de reglas que está pendiente de aplicarse, Kaspersky Endpoint Security distingue las reglas del Control de anomalías adaptativo que van a añadirse o eliminarse.

Cuando una actualización aún no se ha aplicado, las reglas del Control de anomalías adaptativo que se eliminarán con la actualización continúan mostrándose en la tabla de reglas, pero Kaspersky Endpoint Security les asigna el estado *Deshabilitada*. No es posible cambiar la configuración de estas reglas.

*Para actualizar las reglas del Control de anomalías adaptativo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Reglas**, haga clic en el botón **Editar reglas**.

Se abre la lista de reglas de Control de anomalías adaptativo.

4. En la ventana que se abre, haga clic en el botón **Aprobar actualizaciones**.

El botón **Aprobar actualizaciones** estará activo cuando haya una actualización disponible para las reglas del Control de anomalías adaptativo.


5. Guarde los cambios.

## Modificación de las plantillas de mensajes del Control de anomalías adaptativo

Cuando un usuario intenta realizar una acción bloqueada por las reglas de Control de anomalías adaptativo, Kaspersky Endpoint Security muestra un mensaje notificando que se han bloqueado acciones potencialmente dañinas. Si el usuario cree que una acción se ha bloqueado por error, el usuario puede utilizar el enlace incluido en el texto del mensaje para enviar un mensaje al administrador de la red corporativa local.

Están disponibles plantillas especiales del mensaje sobre el bloqueo de acciones potencialmente dañinas y del mensaje se envía al administrador. Puede modificar las plantillas de los mensajes.

*Para editar una plantilla de mensaje:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control de anomalías adaptativo:
  - **Mensaje sobre el bloqueo.** Plantilla del mensaje que se muestra a un usuario cuando se activa una regla del Control de anomalías adaptativo que bloquea una acción no típica.
  - **Mensaje para el administrador.** Plantilla del mensaje que un usuario puede enviar al administrador de la red corporativa local si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo de la actividad de aplicaciones**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.
4. Guarde los cambios.

## Visualización de informes del Control de anomalías adaptable

*Para ver los informes de Control de anomalías adaptable:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

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

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

5. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de anomalías adaptativo**.

La configuración del componente Control de anomalías adaptativo se muestra en la parte derecha de la ventana.

6. Realice una de las siguientes acciones:

- Si desea ver un informe sobre la configuración de las reglas del Control de anomalías adaptativo, haga clic en **Informe de estado de reglas de Control de anomalías adaptativo**.
- Si desea ver un informe sobre la aplicación de las reglas del Control de anomalías adaptativo, haga clic en **Informe de reglas de Control de anomalías adaptativo activado**.

7. Se inicia el proceso de generación de informes.

El informe se muestra en una nueva ventana.

## Control de aplicaciones

El Control de aplicaciones gestiona el inicio de aplicaciones en los equipos de los usuarios. Esto le permite implementar una directiva corporativa de seguridad al usar aplicaciones. El Control de aplicaciones también reduce el riesgo de infección del equipo al restringir el acceso a las aplicaciones.

La configuración del Control de aplicaciones consta de los siguientes pasos:

### 1. [Creación de categorías de aplicaciones](#).

El administrador crea categorías de aplicaciones que el administrador quiere gestionar. Las categorías de aplicaciones están destinadas a todos los equipos de la red corporativa, independientemente de los grupos de administración. Para crear una categoría, puede usar los siguientes criterios: categoría KL (por ejemplo, *Navegadores*), hash de archivo, proveedor de aplicaciones y otros criterios.

### 2. [Crear reglas de Control de aplicaciones](#).

El administrador crea reglas de Control de aplicaciones en la directiva para el grupo de administración. La regla incluye las categorías de aplicaciones y el estado de inicio de las aplicaciones de estas categorías: bloqueadas o permitidas.

### 3. [Seleccionar el modo de Control de aplicaciones](#).

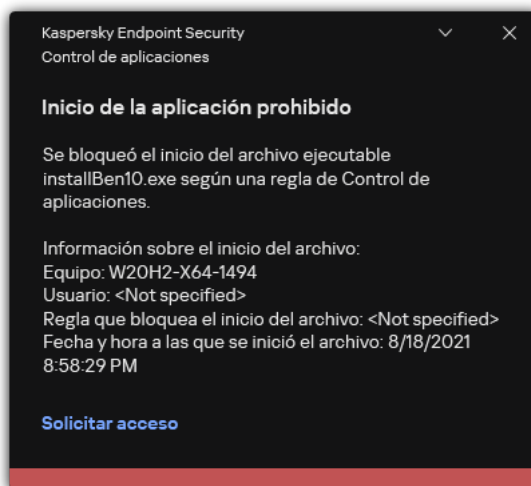
El administrador elige el modo para trabajar con las aplicaciones que no estén incluidas en ninguna de las reglas (listas de aplicaciones admitidas y rechazadas).

Cuando un usuario intenta iniciar una aplicación prohibida, Kaspersky Endpoint Security bloqueará el inicio de dicha aplicación y mostrará una notificación (vea la figura a continuación).

Se proporciona un *modo de prueba* para comprobar la configuración de Control de aplicaciones. En este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite el inicio de aplicaciones, incluidas las prohibidas.
- Muestra una notificación sobre el inicio de una aplicación prohibida y añade información al informe en el equipo del usuario.

- Envía datos sobre el inicio de aplicaciones prohibidas a Kaspersky Security Center.



Notificación de Control de aplicaciones

## Modos de funcionamiento de Control de aplicaciones

El componente Control de aplicaciones funciona en dos modos:

- **Lista de rechazados.** En este modo, Control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de Control de aplicaciones.

Este modo de Control de aplicaciones está activado de forma predeterminada.

- **Lista de admitidos.** En este modo, Control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de Control de aplicaciones. Si las reglas de autorización de Control de aplicaciones están totalmente configuradas, el componente bloquea el inicio de todas las aplicaciones nuevas que no haya verificado el administrador de la red de área local, mientras que autoriza el funcionamiento del sistema operativo y de las aplicaciones de confianza en las que los usuarios confían en su trabajo.

Puede leer las [recomendaciones sobre la configuración de reglas de Control de aplicaciones en el modo de lista de admitidos](#).

El Control de aplicaciones puede configurarse para que funcione en estos modos tanto mediante la interfaz local de Kaspersky Endpoint Security como mediante Kaspersky Security Center.

Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas que son necesarias para las siguientes tareas:

- [Creación de categorías de aplicaciones](#).

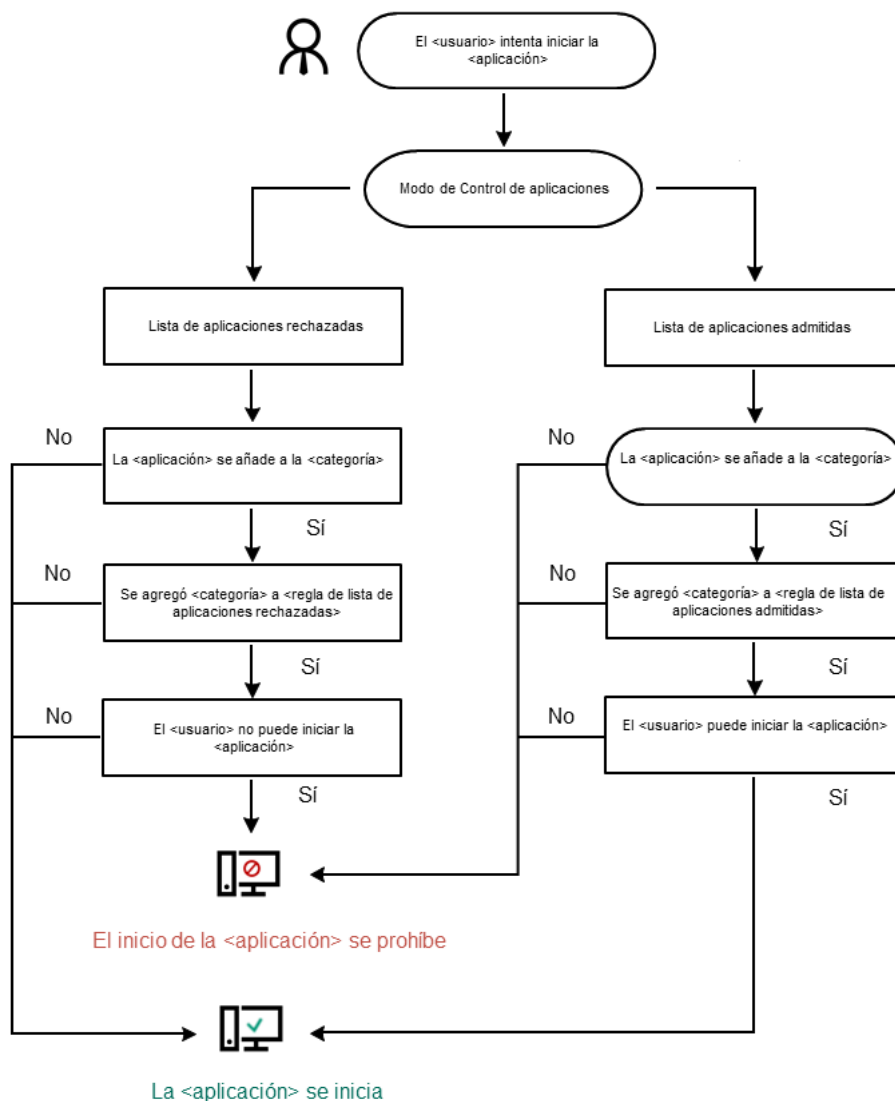
Las reglas del componente Control de aplicaciones de la consola de administración de Kaspersky Security Center se basan en categorías de aplicaciones predeterminadas, y no en reglas de inclusión y exclusión, como sucede en la interfaz local de Kaspersky Endpoint Security.

- [Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN](#).

Por eso, se recomienda usar Kaspersky Security Center para configurar el funcionamiento del componente Control de aplicaciones.

## Algoritmo de funcionamiento de Control de aplicaciones

Kaspersky Endpoint Security utiliza un algoritmo para tomar una decisión sobre el inicio de una aplicación (vea la figura a continuación).



Algoritmo de funcionamiento de Control de aplicaciones

## Limitaciones de funcionalidad de Control de aplicaciones

El funcionamiento del componente Control de aplicaciones queda limitado en los casos siguientes:

- Cuando se actualiza la versión de la aplicación, no se admite la importación de la configuración del componente Control de aplicaciones.
- Cuando se actualiza la versión de la aplicación, la importación de la configuración del componente de Control de aplicaciones solo se admite si Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores se actualiza a Kaspersky Endpoint Security 11.8.0 para Windows.



Cuando se actualizan versiones distintas de Kaspersky Endpoint Security 10 Service Pack 2 para Windows, es preciso configurar desde cero los ajustes de Control de aplicaciones, para restaurar el estado operativo de este componente.

- Si no hay conexión con los servidores del KSN, Kaspersky Endpoint Security recibe la información sobre la reputación de las aplicaciones y sus módulos solo desde las bases de datos locales.

La lista de aplicaciones que Kaspersky Endpoint Security designa como categoría KL **Otras aplicaciones**\Aplicaciones de confianza de acuerdo con la reputación en KSN puede diferir dependiendo de si está disponible o no una conexión a los servidores de KSN.

- En la base de datos de Kaspersky Security Center, es posible almacenar información acerca de 150 000 archivos procesados. Una vez que se alcance este número de archivos, no se procesarán nuevos archivos. Para reanudar las operaciones de inventario, debe eliminar los archivos que se inventariaron anteriormente en la base de datos de Kaspersky Security Center desde el equipo en el cual se instaló Kaspersky Endpoint Security.
- El componente no controla el inicio de scripts a menos que el script se envíe al intérprete mediante la línea de comandos.

Si está permitido el inicio de un intérprete por parte de reglas de Control de aplicaciones, el componente no bloqueará un script iniciado por este intérprete.

Basta que uno de los scripts especificados en la línea de comandos del intérprete esté bloqueado desde el inicio por las Reglas de control de aplicaciones, para que el componente bloquee todos los scripts especificados en la línea de comandos del intérprete.

- El componente no controla el inicio de scripts desde aquellos intérpretes no admitidos por Kaspersky Endpoint Security.

Kaspersky Endpoint Security admite los siguientes intérpretes:

- Java
- PowerShell

Se admiten los siguientes tipos de intérpretes:


- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;
- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;

- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

## Activación y desactivación de Control de aplicaciones

De forma predeterminada, Control de aplicaciones está desactivado.


*Para activar o desactivar Control de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. Utilice el interruptor **Control de aplicaciones** para activar o desactivar el componente.
4. Guarde los cambios.

Como resultado, si el Control de aplicaciones está activado, la aplicación reenvía información sobre la ejecución de archivos ejecutables a Kaspersky Security Center. Puede ver la lista de archivos ejecutables en ejecución en Kaspersky Security Center en la carpeta **Archivos ejecutables**. Para recibir información sobre todos los archivos ejecutables en lugar de ejecutar solo archivos ejecutables, ejecute la [tarea de inventario](#).

## Seleccionar el modo de Control de aplicaciones

*Para seleccionar el modo de Control de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.

3. En el bloque **Modo de control de inicio de la aplicación**, elija una de las siguientes opciones:

- **Lista de rechazados.** Si se selecciona esta opción, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto las prohibidas por las condiciones de las reglas de bloqueo de Control de aplicaciones.
- **Lista de admitidos.** Si se selecciona esta opción, Control de aplicaciones impide que los usuarios inicien las aplicaciones que no cumplen con las condiciones de las reglas de autorización de Control de aplicaciones.

La regla **Golden Image** y la regla **Actualizadores de confianza** se definen inicialmente para el modo Lista de admitidos. Estas reglas de Control de aplicaciones corresponden a las categorías KL. La categoría KL "Golden Image" incluye programas que garantizan el funcionamiento normal del sistema operativo. La categoría KL "Actualizadores de confianza" incluye programas de actualización de los proveedores de software más prestigiosos. No puede eliminar estas reglas. La configuración de estas reglas no se puede editar. De forma predeterminada, la regla **Golden Image** está activada y la regla **Actualizadores de confianza** está desactivada. Todos los usuarios tienen permiso para iniciar aplicaciones que cumplan las condiciones de activación de estas reglas.

Todas las reglas creadas durante el modo seleccionado se guardan después de cambiar el modo, de manera que las reglas se pueden utilizar de nuevo. Para volver a utilizar estas reglas, todo lo que tiene que hacer es seleccionar el modo necesario.

4. En la sección **Acción al iniciar aplicaciones bloqueadas**, seleccione la acción que realizará el componente cuando un usuario intente iniciar una aplicación bloqueada por reglas de Control de aplicaciones.
5. Seleccione la casilla **Controlar la carga de los módulos DLL** si desea que Kaspersky Endpoint Security supervise la carga de módulos DLL cuando los usuarios inician aplicaciones.

La información sobre el módulo y la aplicación que cargó dicho módulo se guardará en un informe.

Kaspersky Endpoint Security solamente supervisa los controladores y módulos DLL que se carguen desde el momento en que se selecciona la casilla de verificación. Si desea que Kaspersky Endpoint Security supervise todos los controladores y módulos DLL, incluidos los cargados antes de que se iniciara Kaspersky Endpoint Security, reinicie el equipo después de seleccionar la casilla de verificación.

Si planea activar el control sobre los controladores y módulos DLL que se carguen, asegúrese de que, en la configuración Control de aplicaciones, esté activada la regla **Golden Image** predeterminada u otra regla que contenga la categoría KL "Certificados de confianza" y garantice que los controladores y módulos DLL de confianza se carguen antes de que se inicie Kaspersky Endpoint Security. Activar la supervisión de la carga de los módulos DLL y los controladores cuando la regla **Golden Image** esté desactivada puede causar inestabilidad en el sistema operativo.

Recomendamos activar la [protección con contraseña](#) para configurar los ajustes de la aplicación, de modo que sea posible desactivar las reglas de bloqueo de inicio de módulos dll y controladores críticos desde el inicio, sin modificar la configuración de la directiva de Kaspersky Security Center.

6. Guarde los cambios.

## Trabajar con reglas de Control de aplicaciones en la interfaz de la aplicación

Kaspersky Endpoint Security controla el inicio de las aplicaciones que hayan realizado los usuarios por medio de reglas. Una regla de Control de aplicaciones especifica las condiciones de activación y las acciones realizadas por el componente Control de aplicaciones cuando se activa la regla (lo que permite o impide a los usuarios que inicien la aplicación).

## Condiciones de activación de reglas

Una condición de activación de reglas tiene la siguiente correlación: "tipo de condición - criterio de condición - valor de condición". En función de las condiciones de activación de reglas, Kaspersky Endpoint Security aplicará (o no) la regla en cuestión a una aplicación.

Los siguientes tipos de condiciones se utilizan en las reglas:

- *Condiciones de inclusión.* Kaspersky Endpoint Security aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de inclusión.
- *Condiciones de exclusión.* Kaspersky Endpoint Security no aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de exclusión, pero no cumple ninguna de las condiciones de inclusión.

Las condiciones de activación de reglas se crean a partir de criterios. Los siguientes criterios se utilizan para crear reglas en Kaspersky Endpoint Security:

- Ruta de la carpeta que contiene el archivo ejecutable de la aplicación, o bien ruta al archivo ejecutable de la aplicación.
- Metadatos: nombre del archivo ejecutable de la aplicación, versión del archivo ejecutable de la aplicación, nombre de la aplicación, versión de la aplicación, proveedor de la aplicación.
- Hash del archivo ejecutable de la aplicación.
- Certificado: emisor, asunto, huella digital.
- Inclusión de la aplicación en una categoría KL.
- Ubicación del archivo ejecutable de la aplicación en una unidad extraíble.

El valor del criterio se debe especificar para cada criterio utilizado en la condición. Si los parámetros de la aplicación que se va a iniciar coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, Control de aplicaciones realiza la acción prescrita en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, Control de aplicaciones no controla el inicio de la aplicación.

Si ha seleccionado un certificado como condición de activación de la regla, debe asegurarse de que este certificado se añada al almacenamiento del sistema de confianza en el ordenador y verificar la [configuración de uso de almacenamiento del sistema de confianza en la aplicación](#).

## Decisiones tomadas por el componente Control de aplicaciones cuando se activa una regla

Cuando se activa una regla, Control de aplicaciones permite que los usuarios (o los grupos de usuarios) inicien aplicaciones o bloquea el inicio de dichas aplicaciones, según lo que dicte la regla. Puede seleccionar usuarios particulares o grupos de usuarios que tienen o no permiso para iniciar aplicaciones que activan una regla.

A la regla que no especifica los usuarios que pueden iniciar aplicaciones que cumplan con la regla, se la denomina *regla de bloqueo*.

A la regla que no especifica los usuarios que no pueden iniciar aplicaciones que coincidan con la regla, se la denomina *regla de permiso*.

La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. Por ejemplo, si se ha especificado una regla de permiso de Control de aplicaciones para un grupo de usuarios y, al mismo tiempo, se ha especificado una regla de bloqueo de Control de aplicaciones para un usuario en este grupo de usuarios, se bloqueará a este usuario para que no ejecute la aplicación.


## Estado operativo de una regla

Las reglas de Control de Aplicaciones pueden tener uno de estos valores de estado de funcionamiento:

- **Activado.** Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Desactivado.** Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Prueba.** Este estado significa que Kaspersky Endpoint Security permite el inicio de aplicaciones a las que se aplican las reglas, pero registra en el informe datos sobre el inicio de esas aplicaciones.

## Adición de una regla de Control de aplicaciones

*Para añadir una regla de Control de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.  
Se desplegará la lista de reglas de Control de aplicaciones.
4. Haga clic en el botón **Añadir**.  
Se abre la ventana de configuración de las reglas de Control de aplicaciones.
5. En la pestaña **Configuración general**, defina la configuración principal de la regla:
  - a. En el campo **Nombre de la regla**, introduzca el nombre de la regla.
  - b. En el campo **Descripción**, introduzca una descripción de la regla.
  - c. Recopile o edite una lista de usuarios y grupos de usuarios que tengan o no autorización para iniciar aplicaciones que cumplan las condiciones de activación de la regla. Para ello, haga clic en el botón **Añadir** en la tabla **Sujetos y sus derechos**.  
De forma predeterminada, el valor **Todos** se añade a la lista de usuarios. La regla se aplica a todos los usuarios.

Si no hay ningún usuario especificado en la tabla, la regla no se puede guardar.


- d. En la tabla **Sujetos y sus derechos**, use el interruptor para definir el derecho de los usuarios a iniciar aplicaciones.
- e. Seleccione la casilla **Denegar a los demás usuarios** si quiere que la aplicación impida que se ejecuten los programas que cumplen las condiciones de activación de las reglas para todos los usuarios que no figuran en la tabla **Sujetos y sus derechos** y que no son miembros de los grupos de usuarios que figuran en la tabla **Sujetos 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 **Sujetos y sus derechos** y que no formen parte de los grupos de usuarios especificados en la tabla **Sujetos y sus derechos**.

- f. Si desea que Kaspersky Endpoint Security considere las aplicaciones que coinciden con las condiciones de activación de reglas como programas de actualización de confianza autorizados a crear archivos ejecutables utilizables posteriormente, seleccione la casilla de verificación **Actualizadores de confianza**.
6. En la pestaña **Condiciones**, [cree](#) o edite la lista de condiciones de inclusión para activar la regla.
  7. En la pestaña **Exclusiones**, 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.

## Adición de una condición de activación para una regla de Control de aplicaciones

*Para añadir una nueva condición de activación para una regla de Control de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.  
Se desplegará la lista de reglas de Control de aplicaciones.
4. Seleccione la regla para la que desea configurar una condición de activación.  
Se abre la configuración de la regla de Control de aplicaciones.
5. Seleccione la pestaña **Condiciones** o **Exclusiones** y haga clic en el botón **Añadir**.
6. Seleccione las condiciones de activación para la regla de Control de aplicaciones:
  - **Condiciones de propiedades de las aplicaciones iniciadas**. En la lista de aplicaciones en ejecución, puede seleccionar las aplicaciones a las que se aplicará la regla de Control de aplicaciones. Kaspersky Endpoint Security también enumera las aplicaciones que se estaban ejecutando anteriormente en el equipo. Debe

elegir el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta al archivo o carpeta**.

- **Condiciones "Categoría KL"**. Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL conocida como "Aplicaciones de Office" incluye a las aplicaciones del paquete Microsoft Office y a Adobe® Acrobat®, entre otros.
- **Condición personalizada**. Puede elegir el archivo de la aplicación y elegir una de las condiciones de activación de la regla: **Hash del archivo**, **Certificado**, **Metadatos** o **Ruta al archivo o carpeta**.
- **Condición por unidad de archivos (unidad extraíble)**. La regla de Control de aplicaciones se aplica solo a los archivos que se ejecutan en una unidad extraíble.
- **Condiciones de las propiedades de los archivos en la carpeta especificada**. La regla de Control de aplicaciones se aplica solo a los archivos en la carpeta especificada. También puede incluir o excluir archivos de subcarpetas. Debe elegir el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta al archivo o carpeta**.


7. Guarde los cambios.

Al añadir condiciones, tenga en cuenta las siguientes consideraciones especiales para el Control de aplicaciones:

- Kaspersky Endpoint Security no admite el hash de un archivo MD5 y no controla el inicio de aplicaciones basado en un hash de MD5. Se utiliza un hash SHA256 como condición de activación de reglas.
- No se recomienda usar solo los criterios de **Emisor** y **Sujeto** como condiciones de activación de la regla. El uso de estos criterios no es fiable.
- Si está usando enlaces simbólicos en el campo **Ruta al archivo o carpeta**, le aconsejamos resolver los enlaces simbólicos para que la regla de Control de Aplicaciones funcione correctamente. Para ello, haga clic en el botón **Resolver enlace simbólico**.

## Cambiar el estado de una regla de Control de aplicaciones

*Para cambiar el estado de una regla de Control de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.  
Se desplegará la lista de reglas de Control de aplicaciones.
4. En la columna **Estado**, abra el menú contextual y seleccione una de las siguientes:
  - **Activado**. Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
  - **Desactivado**. Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.

- **Prueba.** Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplica esta regla, pero registra en el informe datos sobre el inicio de esas aplicaciones.

5. Guarde los cambios.

## Administrar las reglas de Control de aplicaciones en Kaspersky Security Center

Kaspersky Endpoint Security controla el inicio de las aplicaciones que hayan realizado los usuarios por medio de reglas. Una regla de Control de aplicaciones especifica las condiciones de activación y las acciones realizadas por el componente Control de aplicaciones cuando se activa la regla (lo que permite o impide a los usuarios que inicien la aplicación).

### Condiciones de activación de reglas

Una condición de activación de reglas tiene la siguiente correlación: "tipo de condición - criterio de condición - valor de condición". En función de las condiciones de activación de reglas, Kaspersky Endpoint Security aplicará (o no) la regla en cuestión a una aplicación.

Los siguientes tipos de condiciones se utilizan en las reglas:

- *Condiciones de inclusión.* Kaspersky Endpoint Security aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de inclusión.
- *Condiciones de exclusión.* Kaspersky Endpoint Security no aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de exclusión, pero no cumple ninguna de las condiciones de inclusión.

Las condiciones de activación de reglas se crean a partir de criterios. Los siguientes criterios se utilizan para crear reglas en Kaspersky Endpoint Security:

- Ruta de la carpeta que contiene el archivo ejecutable de la aplicación, o bien ruta al archivo ejecutable de la aplicación.
- Metadatos: nombre del archivo ejecutable de la aplicación, versión del archivo ejecutable de la aplicación, nombre de la aplicación, versión de la aplicación, proveedor de la aplicación.
- Hash del archivo ejecutable de la aplicación.
- Certificado: emisor, asunto, huella digital.
- Inclusión de la aplicación en una categoría KL.
- Ubicación del archivo ejecutable de la aplicación en una unidad extraíble.

El valor del criterio se debe especificar para cada criterio utilizado en la condición. Si los parámetros de la aplicación que se va a iniciar coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, Control de aplicaciones realiza la acción prescrita en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, Control de aplicaciones no controla el inicio de la aplicación.



Si ha seleccionado un certificado como condición de activación de la regla, debe asegurarse de que este certificado se añada al almacenamiento del sistema de confianza en el ordenador y verificar la [configuración de uso de almacenamiento del sistema de confianza en la aplicación](#).

## Decisiones tomadas por el componente Control de aplicaciones cuando se activa una regla

Cuando se activa una regla, Control de aplicaciones permite que los usuarios (o los grupos de usuarios) inicien aplicaciones o bloquea el inicio de dichas aplicaciones, según lo que dicte la regla. Puede seleccionar usuarios particulares o grupos de usuarios que tienen o no permiso para iniciar aplicaciones que activan una regla.

A la regla que no especifica los usuarios que pueden iniciar aplicaciones que cumplan con la regla, se la denomina *regla de bloqueo*.

A la regla que no especifica los usuarios que no pueden iniciar aplicaciones que coincidan con la regla, se la denomina *regla de permiso*.

La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. Por ejemplo, si se ha especificado una regla de permiso de Control de aplicaciones para un grupo de usuarios y, al mismo tiempo, se ha especificado una regla de bloqueo de Control de aplicaciones para un usuario en este grupo de usuarios, se bloqueará a este usuario para que no ejecute la aplicación.

## Estado operativo de una regla

Las reglas de Control de Aplicaciones pueden tener uno de estos valores de estado de funcionamiento:

- **Activado.** Este estado indica que se utiliza la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Desactivado.** Este estado indica que se ignora la regla cuando el componente Control de aplicaciones está en funcionamiento.
- **Prueba.** Este estado significa que Kaspersky Endpoint Security permite el inicio de aplicaciones a las que se aplican las reglas, pero registra en el informe datos sobre el inicio de esas aplicaciones.

## Recepción de información sobre las aplicaciones que se instalan en equipos de usuarios

Para crear reglas óptimas de Control de aplicaciones, se recomienda obtener primero una imagen de las aplicaciones que se utilizan en los equipos de la red de área local corporativa. Para ello, puede obtener la siguiente información:

- Proveedores, versiones y localizaciones de las aplicaciones utilizadas en la red de área local corporativa.
- Frecuencia de las actualizaciones de la aplicación.
- Las directivas de uso de aplicaciones adoptadas en la empresa (puede tratarse de directivas de seguridad o directivas administrativas).
- Ubicación donde se almacenan los paquetes de distribución de la aplicación.

La información acerca de las aplicaciones que se utilizan en los equipos de la red de área local corporativa está disponible en las carpetas **Registro de aplicaciones** y **Archivos ejecutables**. Las carpetas **Registro de aplicaciones** y **Archivos ejecutables** están ubicadas en la carpeta **Gestión de aplicaciones** del árbol de la consola de administración de Kaspersky Security Center.

La carpeta **Registro de aplicaciones** contiene la lista de aplicaciones que detectó el [Agente de red](#) instalado en el equipo cliente.

La carpeta **Archivos ejecutables** contiene una lista de los archivos ejecutables que se han iniciado en los equipos cliente o se han detectado durante la tarea de inventario de Kaspersky Endpoint Security.

Para ver la información general acerca de la aplicación y sus archivos ejecutables, así como la lista de equipos en los que se instala una aplicación, abra la ventana de propiedades de una aplicación que esté seleccionada en la carpeta **Registro de aplicaciones** o en la carpeta **Archivos ejecutables**.

*Para abrir la ventana de propiedades de aplicaciones en la carpeta Registro de aplicaciones:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione **Avanzado** → **Administración de aplicaciones** → **Registro de aplicaciones**.
3. Seleccione una aplicación.
4. En el menú contextual de la aplicación, seleccione **Propiedades**.

*Para abrir la ventana de propiedades de un archivo ejecutable en la carpeta Archivos ejecutables:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Avanzado** → **Administración de aplicaciones** → **Archivos ejecutables**.
3. Seleccione un archivo ejecutable.
4. En el menú contextual del archivo ejecutable, seleccione **Propiedades**.

## Creación de categorías de aplicaciones

Para que crear reglas de Control de aplicaciones resulte más práctico, puede crear categorías de aplicaciones.

Se recomienda crear una categoría "Aplicaciones de trabajo" que abarque el conjunto estándar de las aplicaciones que se utilicen en la empresa. Si hay distintos grupos de usuarios que utilicen distintos conjuntos de aplicaciones en su trabajo, puede crearse una categoría de aplicaciones independiente para cada grupo de usuarios.

*Para crear un categoría de la aplicación:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Administración de aplicaciones** → **Categorías de la aplicación**.
3. Haga clic en el botón **Categoría nueva** en el espacio de trabajo.  
Se iniciará el asistente de creación de categorías del usuario.

4. Siga las instrucciones de dicho asistente de creación de categorías.

## Paso 1. Selección del tipo de categoría

En este paso, seleccione uno de los siguientes tipos de categorías de aplicaciones:

- **Categoría con contenido añadido manualmente.** Si selecciona este tipo de categoría, en los pasos "Configuración de las condiciones para incluir aplicaciones en una categoría" y "Configuración de las condiciones para excluir aplicaciones de una categoría", podrá definir los criterios por los que los archivos ejecutables se incluirán en la categoría.
- **Categoría que incluye archivos ejecutables desde dispositivos seleccionados.** Si selecciona este tipo de la categoría, en el paso "Configuración" podrá especificar un equipo cuyos archivos ejecutables se incluirán automáticamente en la categoría.
- **Categoría que incluye archivos ejecutables de una carpeta específica.** Si selecciona este tipo de categoría, en el paso "Carpeta repositorio" podrá especificar una carpeta cuyos archivos ejecutables se incluirán automáticamente en la categoría.

Al crear una categoría con contenido añadido manualmente, Kaspersky Security Center realiza un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR.

## Paso 2. Introducción de un nombre de categoría de usuario

En este paso, especifique un nombre para la categoría de aplicación.

## Paso 3. Configuración de las condiciones para incluir aplicaciones en una categoría

Este paso está disponible si selecciona el tipo de categoría **Categoría con contenido añadido manualmente**.

En este paso, en la lista desplegable **Añadir**, seleccione las condiciones para incluir aplicaciones en la categoría:

- **Desde la lista de archivos ejecutables.** Añada aplicaciones de la lista de archivos ejecutables en el dispositivo del cliente a la categoría personalizada.
- **De propiedades del archivo.** Especifique datos detallados de archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Metadatos desde archivos en carpeta.** Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de verificación de los archivos en la carpeta.** Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los hash de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Certificados para los archivos de la carpeta.** Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para añadir aplicaciones a la categoría personalizada.

No se recomienda usar condiciones cuyas propiedades no tengan el parámetro **Huella digital del certificado** especificado.

- **Metadatos de archivos del programa de instalación MSI.** Seleccione el paquete MSI. Kaspersky Security Center indicará los metadatos de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de comprobación de los archivos del programa de instalación MSI de la aplicación.** Seleccione el paquete MSI. Kaspersky Security Center indicará los hash de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **De categoría KL.** Especifique una categoría KL como condición para añadir aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL conocida como "Aplicaciones de Office" incluye a las aplicaciones del paquete Microsoft Office y a Adobe Acrobat, entre otros. Puede seleccionar todas las categorías KL para generar una lista ampliada de aplicaciones de confianza.
- **Especificar la ruta a la aplicación.** Seleccione una carpeta en el dispositivo del cliente. Kaspersky Security Center añadirá archivos ejecutables desde esta carpeta a la categoría personalizada.
- **Seleccionar el certificado del repositorio.** Seleccione los certificados que se usaron para firmar archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.

No se recomienda usar condiciones cuyas propiedades no tengan el parámetro **Huella digital del certificado** especificado.

- **Tipo de unidad.** Especifique un tipo de dispositivo de almacenamiento (todas las unidades de disco duro y extraíbles o solo las unidades extraíbles) como una condición para añadir aplicaciones a la categoría personalizada.

#### Paso 4. Configuración de las condiciones para excluir aplicaciones de una categoría

Este paso está disponible si selecciona el tipo de categoría **Categoría con contenido añadido manualmente**.

Las aplicaciones especificadas en este paso se excluyen de la categoría aunque estas aplicaciones se especificaran en el paso "Configuración de las condiciones incluir aplicaciones en una categoría".

En este paso, en la lista desplegable **Añadir**, seleccione las condiciones para excluir aplicaciones de la categoría:

- **Desde la lista de archivos ejecutables.** Añada aplicaciones de la lista de archivos ejecutables en el dispositivo del cliente a la categoría personalizada.
- **De propiedades del archivo.** Especifique datos detallados de archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Metadatos desde archivos en carpeta.** Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.

- **Sumas de verificación de los archivos en la carpeta.** Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables. Kaspersky Security Center indicará los hash de estos archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Certificados para los archivos de la carpeta.** Seleccione una carpeta en el dispositivo del cliente que contenga archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para añadir aplicaciones a la categoría personalizada.
- **Metadatos de archivos del programa de instalación MSI.** Seleccione el paquete MSI. Kaspersky Security Center indicará los metadatos de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **Sumas de comprobación de los archivos del programa de instalación MSI de la aplicación.** Seleccione el paquete MSI. Kaspersky Security Center indicará los hash de los archivos ejecutables de este paquete MSI como una condición para añadir aplicaciones a la categoría personalizada.
- **De categoría KL.** Especifique una categoría KL como condición para añadir aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL conocida como "Aplicaciones de Office" incluye a las aplicaciones del paquete Microsoft Office y a Adobe Acrobat, entre otros. Puede seleccionar todas las categorías KL para generar una lista ampliada de aplicaciones de confianza.
- **Especificar la ruta a la aplicación.** Seleccione una carpeta en el dispositivo del cliente. Kaspersky Security Center añadirá archivos ejecutables desde esta carpeta a la categoría personalizada.
- **Seleccionar el certificado del repositorio.** Seleccione los certificados que se usaron para firmar archivos ejecutables como condición para añadir aplicaciones a la categoría personalizada.
- **Tipo de unidad.** Especifique un tipo de dispositivo de almacenamiento (todas las unidades de disco duro y extraíbles o solo las unidades extraíbles) como una condición para añadir aplicaciones a la categoría personalizada.

## Paso 5. Configuración

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**.

En este paso, haga clic en el botón **Añadir** y especifique los equipos cuyos archivos ejecutables añadirá Kaspersky Security Center a la categoría de aplicaciones. Kaspersky Security Center añadirá a la categoría de aplicación todos los archivos ejecutables de los equipos especificados presentados en la carpeta [Archivos ejecutables](#).

En este paso, también puede ajustar la configuración siguiente:

- Algoritmo para cálculo de la función de hash por Kaspersky Security Center. Para elegir un algoritmo, debe marcar como mínimo una de las siguientes casillas:
  - **Calcular SHA-256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores).**
  - **Calcular MD5 para archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows).**
- 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 de verificación **Sincronizar datos con el repositorio del Servidor de administración** está desactivada, Kaspersky Security Center no realizará ninguna modificación en una categoría de aplicación después de crearla.

- Campo **Tiempo de análisis (h)**. En este campo, puede especificar el período de tiempo (en horas) después de las cuales Kaspersky Security Center borra la categoría de aplicaciones y le añade todos archivos ejecutables desde los equipos especificados incluidos en la carpeta **Archivos ejecutables**.

Este campo solamente está disponible si ha seleccionado la casilla de verificación **Sincronizar datos con el repositorio del Servidor de administración**.

## Paso 6. Carpeta repositorio

Este paso está disponible si ha seleccionado el tipo de **Categoría que incluye archivos ejecutables de una carpeta específica**.

En este paso, haga clic en el botón **Examinar** y especifique la carpeta en la cual Kaspersky Security Center buscará archivos ejecutables para añadir automáticamente aplicaciones a la categoría de aplicación.

En este paso, también puede ajustar la configuración siguiente:

- Casilla de verificación **Incluir bibliotecas de enlace dinámico (DLL) en esta categoría**. Seleccione esta casilla de verificación si desea que las bibliotecas de enlace dinámico (archivos DLL) se incluyan en la categoría de la aplicación.

Incluir archivos DLL en la categoría de aplicación puede reducir el rendimiento de Kaspersky Security Center.

- Casilla de verificación **Incluir datos de script en esta categoría**. Seleccione esta casilla de verificación si desea que los scripts se incluyan en la categoría de la aplicación.

Incluir scripts en la categoría de aplicación puede reducir el rendimiento de Kaspersky Security Center.

- Algoritmo para cálculo de la función de hash por Kaspersky Security Center. Para elegir un algoritmo, debe marcar como mínimo una de las siguientes casillas:

- **Calcular SHA-256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores).**
- **Calcular MD5 para archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows).**

- **Forzar el análisis de la carpeta en busca de cambios** casilla de verificación. Seleccione esta casilla si desea que Kaspersky Security Center busque periódicamente archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación.

Si desactiva la casilla **Forzar el análisis de la carpeta en busca de cambios**, Kaspersky Security Center busca los archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación solamente si se han realizado cambios en la carpeta, añadiendo o borrando un archivo de la misma.

- Campo **Tiempo de análisis (h)**. En este campo puede especificar el intervalo de tiempo (en horas) después del cual Kaspersky Security Center buscará archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación.

Este campo está disponible si se ha seleccionado la opción **Forzar el análisis de la carpeta en busca de cambios**.

## Paso 7. Creación de una categoría personalizada

Salga del Asistente.

### Añadir archivos ejecutables desde la carpeta Archivos ejecutables a la categoría de aplicación

En la carpeta **Archivos ejecutables** se muestra la lista de archivos ejecutables detectados en los equipos. Kaspersky Endpoint Security genera una lista de archivos ejecutables después de ejecutar la Tarea de inventario.

*Para añadir archivos ejecutables desde la carpeta Archivos ejecutables a la categoría de aplicación:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Avanzado** → **Administración de aplicaciones** → **Archivos ejecutables**.
3. En el espacio de trabajo, seleccione los archivos ejecutables que desee añadir a la categoría de aplicación.
4. Haga clic con el botón derecho para abrir el menú contextual de los archivos ejecutables seleccionados y seleccione **Agregar a categoría**.
5. En la ventana abierta, haga lo siguiente:
  - En la parte superior de la ventana, elija una de las opciones siguientes:
    - **Añadir a una nueva categoría de aplicaciones**. Elija esta opción si desea crear una nueva categoría de aplicación y añadirle archivos ejecutables.
    - **Añadir a una categoría de aplicaciones existente**. Elija esta opción si desea escoger una categoría de aplicación existente y añadirle archivos ejecutables.
  - En el bloque **Tipo de regla**, elija una de las opciones siguientes:
    - **Reglas para añadir inclusiones**. Seleccione esta opción si desea crear una condición que añada archivos ejecutables a la categoría de aplicación.
    - **Reglas para añadir exclusiones**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de aplicación.
  - En el bloque **Parámetro utilizado como condición**, seleccione una de las opciones siguientes:
    - **Detalles del certificado (o hashes SHA-256 para archivos sin certificado)**.
    - **Detalles del certificado (se omitirán los archivos sin certificado)**.
    - **Solo SHA-256 (se omitirán los archivos sin hash)**.

- Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security versión 10 Service Pack 1).

6. Guarde los cambios.

## Añadir archivos ejecutables relacionados con eventos a la categoría de aplicación

*Para añadir archivos ejecutables relacionados con los eventos de Control de aplicaciones a la categoría de la aplicación:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.
3. Elija una selección de eventos relacionados con el funcionamiento del componente Control de aplicaciones ([Ver eventos resultantes del funcionamiento del componente Control de aplicaciones](#), [Ver eventos resultantes de la comprobación del funcionamiento del componente Control de aplicaciones](#)) en la lista desplegable **Selecciones de eventos**.
4. Haga clic en el botón **Ejecutar selección**.
5. Seleccione los eventos cuyos archivos ejecutables asociados desee añadir a la categoría de aplicación.
6. Haga clic con el botón derecho para abrir el menú contextual de los eventos seleccionados y seleccione **Añadir a categoría**.
7. En la ventana abierta, configure los parámetros de la categoría de la aplicación:
  - En la parte superior de la ventana, elija una de las opciones siguientes:
    - **Añadir a una nueva categoría de aplicaciones**. Elija esta opción si desea crear una nueva categoría de aplicación y añadirle archivos ejecutables.
    - **Añadir a una categoría de aplicaciones existente**. Elija esta opción si desea escoger una categoría de aplicación existente y añadirle archivos ejecutables.
  - En el bloque **Tipo de regla**, elija una de las opciones siguientes:
    - **Reglas para añadir inclusiones**. Seleccione esta opción si desea crear una condición que añada archivos ejecutables a la categoría de aplicación.
    - **Reglas para añadir exclusiones**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de aplicación.
  - En el bloque **Parámetro utilizado como condición**, seleccione una de las opciones siguientes:
    - **Detalles del certificado (o hashes SHA-256 para archivos sin certificado)**.
    - **Detalles del certificado (se omitirán los archivos sin certificado)**.
    - **Solo SHA-256 (se omitirán los archivos sin hash)**.



- Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security versión 10 Service Pack 1).

8. Guarde los cambios.

## Añadir y modificar una regla de Control de aplicaciones con Kaspersky Security Center

*Para añadir o modificar una regla de Control de aplicaciones con Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. 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.
6. Realice una de las siguientes acciones:

- Para añadir una regla, haga clic en el botón **Añadir**.
- Si desea modificar una regla existente, selecciónela en la lista de reglas y haga clic en el botón **Modificar**.

Se abre la ventana **Regla de Control de aplicaciones**.

7. Realice una de las siguientes acciones:
  - Si desea crear una nueva categoría:
    - a. Haga clic en el botón **Crear una categoría**.  
Se iniciará el asistente de creación de categorías del usuario.
    - b. Siga las instrucciones de dicho asistente de creación de categorías.
    - 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 el botón **Propiedades**.
    - c. Modifique la configuración de la categoría de aplicaciones seleccionada.
    - d. Guarde los cambios.
    - e. En la lista desplegable **Categoría**, seleccione la categoría de aplicación en función de la cual desea crear una regla.

8. En la tabla **Sujetos y sus derechos**, haga clic en el botón **Añadir**.
9. En la ventana abierta, especifique la lista de usuarios o grupos de usuarios para los que desee configurar los permisos para iniciar aplicaciones de la categoría seleccionada.
10. En la tabla **Sujetos y sus derechos**, haga lo siguiente.
  - Si desea permitir que los usuarios o los grupos de usuarios inicien aplicaciones que pertenecen a la categoría seleccionada, seleccione la casilla **Autorizar** situada junto a esos usuarios o grupos.
  - Si quiere prohibir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione la casilla **Denegar** en las filas correspondientes.
11. Seleccione la casilla **Denegar a los demás usuarios** si quiere que todos los usuarios que no aparecen en la columna **Sujeto** y que no forman parte del grupo de usuarios especificados en la columna **Sujeto** estén bloqueados para iniciar aplicaciones que pertenezcan a la categoría seleccionada.
12. Si desea que Kaspersky Endpoint Security considere las aplicaciones incluidas en la categoría de aplicación seleccionada como actualizadores de confianza autorizados a crear archivos ejecutables utilizables posteriormente, marque la casilla **Actualizadores de confianza**.

Cuando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.

13. Guarde los cambios.

## Cambiar el estado de una regla de Control de aplicaciones mediante Kaspersky Security Center

*Para cambiar el estado de una regla de Control de aplicaciones:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. 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.
6. En la columna **Estado**, haga clic con el botón izquierdo del ratón para que se muestre el menú contextual y realice una de las siguientes acciones:
  - **Activa**. Este estado indica que la regla se usa cuando el componente Control de aplicaciones está en funcionamiento.
  - **Inactivo**. Este estado indica que la regla se omite cuando el componente Control de aplicaciones está en funcionamiento.

- **Prueba.** Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplican la regla, pero registra datos sobre el inicio de esas aplicaciones en el informe.

7. Guarde los cambios.

## Exportación e importación de reglas de Control de aplicaciones

Puede exportar la lista de reglas de Control de aplicaciones a un archivo XML. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de Control de aplicaciones o para migrar la lista a un servidor diferente.

Al exportar e importar reglas de Control de aplicaciones, tenga en cuenta las siguientes consideraciones especiales:

- Kaspersky Endpoint Security exporta la lista de reglas solo para el modo Control de aplicaciones activo. En otras palabras, si Control de aplicaciones está funcionando en modo de lista de rechazados, Kaspersky Endpoint Security exportará las reglas solo para este modo. Para exportar la lista de reglas para modo de lista de admitidos, debe cambiar de modo y volver a ejecutar la operación de exportación.
- Kaspersky Endpoint Security usa categorías de aplicaciones para que funcionen las reglas de Control de aplicaciones. Al migrar la lista de reglas de Control de aplicaciones a otro servidor, también debe migrar la lista de categorías de aplicaciones. Para obtener más detalles sobre la exportación o la importación de categorías de aplicaciones, consulte la [Ayuda de Kaspersky Security Center](#).

[Cómo exportar e importar una lista de reglas de Control de aplicaciones en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Controles de seguridad** → **Control de aplicaciones**.
6. Para exportar la lista de reglas de Control de aplicaciones:
  - a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.  
Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.
7. Para exportar una lista de reglas de Control de aplicaciones:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.

[Cómo exportar e importar una lista de reglas de Control de aplicaciones en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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. Haga clic en el enlace **Configuración de las listas de reglas**.
6. Seleccione una lista de reglas: Lista de aplicaciones admitidas o lista de aplicaciones rechazadas.
7. Para exportar la lista de reglas de Control de aplicaciones:
  - a. Seleccione las reglas que quiera exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las reglas seleccionadas o exportar la lista completa.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas a un archivo XML en la carpeta de descargas predeterminada.
8. Para exportar una lista de reglas de Control de aplicaciones:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
9. Guarde los cambios.

## Comprobación de las reglas de Control de aplicaciones con Kaspersky Security Center

Para asegurarse de que las reglas de Control de aplicaciones no bloquean las aplicaciones requeridas para el trabajo, se recomienda activar la comprobación de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear reglas nuevas. Cuando esté activado el modo de prueba de las reglas de Control de aplicaciones, Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio esté prohibido por el Control de aplicaciones, pero sí enviará notificaciones sobre su inicio al Servidor de administración.

Un análisis del funcionamiento de las reglas de Control de aplicaciones requiere la revisión de los eventos de Control de aplicaciones resultantes que se notifican a Kaspersky Security Center. Si el modo de prueba no genera eventos que implican el inicio bloqueado para todas las aplicaciones requeridas para el trabajo del usuario del equipo, esto significa que se crearon las reglas correctas. De lo contrario, se le recomienda actualizar la configuración de las reglas que ha creado, crear reglas adicionales o eliminar las reglas existentes.

De forma predeterminada, Kaspersky Endpoint Security permite el inicio de todas las aplicaciones, excepto las aplicaciones prohibidas por las reglas.

*Para activar o desactivar la comprobación de las reglas de Control de aplicaciones en Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. 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.
6. En la lista desplegable **Modo de Control**, seleccione uno de los siguientes elementos:
  - **Lista de rechazados.** Si se selecciona esta opción, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto las prohibidas por las condiciones de las reglas de bloqueo de Control de aplicaciones.
  - **Lista de admitidos.** Si se selecciona esta opción, Control de aplicaciones impide que los usuarios inicien las aplicaciones que no cumplen con las condiciones de las reglas de autorización de Control de aplicaciones.
7. Realice una de las siguientes acciones:
  - Si desea activar la comprobación para las Reglas de control de aplicaciones, seleccione la opción **Probar reglas** en la lista desplegable **Acción**.
  - Si desea activar el Control de aplicaciones para administrar el inicio de aplicaciones en los equipos de los usuarios, seleccione **Aplicar reglas** en la lista desplegable.
8. Guarde los cambios.

## Ver eventos resultantes de la comprobación del funcionamiento del componente Control de aplicaciones

*Para ver eventos de la comprobación del Control de aplicaciones recibidos por Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.
3. Haga clic en el botón **Crear una selección**.
4. En la ventana que se abre, vaya a la sección **Eventos**.
5. Haga clic en el botón **Borrar todo**.

6. En la tabla **Eventos**, seleccione las casillas **Inicio de la aplicación prohibido en modo de prueba** e **Inicio de la aplicación permitido en modo de prueba**.
7. Guarde los cambios.
8. En la lista desplegable **Selecciones de eventos**, seleccione la selección creada.
9. Haga clic en el botón **Ejecutar selección**.

## Ver un informe sobre las aplicaciones bloqueadas en el modo de prueba

*Para ver el informe sobre las aplicaciones bloqueadas en el modo de prueba:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.  
Se inicia el Asistente de nueva plantilla de informe.
4. Siga los pasos del Asistente de plantillas de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione **Otro** → **Informe sobre aplicaciones prohibidas en el modo de prueba**.  
Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.
5. Abra el informe haciendo doble clic en él.  
  
Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

## Ver eventos resultantes del funcionamiento del componente Control de aplicaciones

*Para ver los eventos resultantes del funcionamiento del componente Control de aplicaciones recibido por Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.
3. Haga clic en el botón **Crear una selección**.
4. En la ventana que se abre, vaya a la sección **Eventos**.
5. Haga clic en el botón **Borrar todo**.
6. En la tabla **Eventos**, seleccione la casilla **Inicio de la aplicación prohibido**.
7. Guarde los cambios.

8. En la lista desplegable **Selecciones de eventos**, seleccione la selección creada.
9. Haga clic en el botón **Ejecutar selección**.

## Ver un informe sobre aplicaciones bloqueadas

*Para ver el informe sobre aplicaciones bloqueadas:*


1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.  
Se inicia el Asistente de nueva plantilla de informe.
4. Siga los pasos del Asistente de plantillas de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione **Otro** → **Informe sobre aplicaciones prohibidas**.  
Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.
5. Abra el informe haciendo doble clic en él.  
  
Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

## Probar reglas de Control de aplicaciones

Para asegurarse de que las reglas de Control de aplicaciones no bloquean las aplicaciones requeridas para el trabajo, se recomienda activar la comprobación de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear reglas nuevas.

Un análisis del funcionamiento de las reglas de Control de aplicaciones requiere la revisión de los eventos de Control de aplicaciones resultantes que se notifican a Kaspersky Security Center. Si el modo de prueba no genera eventos que impliquen el inicio bloqueado para todas las aplicaciones requeridas para el trabajo del usuario del equipo, esto significa que se crearon las reglas correctas. De lo contrario, se le recomienda actualizar la configuración de las reglas que ha creado, crear reglas adicionales o eliminar las reglas existentes.

*Para activar la comprobación de las reglas de Control de aplicaciones o para seleccionar una acción de bloqueo para el Control de aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.  
Se desplegará la lista de reglas de Control de aplicaciones.
4. En la columna **Estado**, seleccione **Prueba**.  
Este estado significa que Kaspersky Endpoint Security permite siempre el inicio de aplicaciones a las que se aplica esta regla, pero registra en el informe datos sobre el inicio de esas aplicaciones.



5. Guarde los cambios.

Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio esté prohibido por el componente Control de aplicaciones, pero enviará notificaciones sobre su inicio al Servidor de administración.

## Supervisión de la actividad de aplicaciones

*Supervisión de la Actividad de Aplicaciones* es una herramienta diseñada para ver información sobre la actividad de las aplicaciones en el equipo de un usuario en tiempo real.

El uso de Supervisión de la actividad de aplicaciones requiere la instalación de los componentes Control de aplicaciones y Prevención de intrusiones en el host. Si estos componentes no están instalados, la sección Supervisión de la actividad de aplicaciones en la [ventana principal de la aplicación](#) está oculta.

*Para iniciar Supervisión de la Actividad de Aplicaciones:*

En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Supervisión de la actividad de aplicaciones**.

Se abre la ventana **Actividad de aplicaciones**. En esta ventana, la información sobre la actividad de las aplicaciones se presenta en tres pestañas:

- La pestaña **Todas las aplicaciones** muestra información sobre todas las aplicaciones instaladas en el equipo.
- La pestaña **Al ejecutar** muestra información sobre el consumo de recursos del equipo por aplicación en tiempo real. En esta pestaña, además puede configurar los permisos de una aplicación individual.
- La pestaña **Ejecutar en el inicio** muestra la lista de aplicaciones que se ejecutan cuando se inicia el sistema operativo.

Si desea ocultar la información de la actividad de la aplicación en el equipo del usuario, puede restringir el acceso del usuario a la herramienta Supervisión de la actividad de aplicaciones.

[Cómo ocultar la Supervisión de la actividad de aplicaciones en la interfaz de la aplicación mediante la Consola de administración \(MMC\)](#) <sup>2</sup>

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Interfaz**.
6. Utilice la casilla de verificación **Ocultar la sección del monitor de actividad de la aplicación** para otorgar o revocar el acceso a la herramienta.
7. Guarde los cambios.

### [Cómo ocultar la Supervisión de la actividad de aplicaciones en la interfaz de la aplicación mediante Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** → **Interfaz**.
5. Utilice la casilla de verificación **Ocultar la sección del monitor de actividad de la aplicación** para otorgar o revocar el acceso a la herramienta.
6. Guarde los cambios.

## Reglas para crear máscaras de nombre para archivos o carpetas

Una *máscara de un archivo o nombre de carpeta* es una representación del nombre de una carpeta o nombre y extensión de un archivo con caracteres comunes.

Puede usar los siguientes caracteres comunes para crear una máscara de nombre de archivo o carpeta:


- El carácter **\*** (asterisco), que toma el lugar de un grupo de caracteres (incluido un grupo vacío). Por ejemplo, la máscara `C:\*.txt` incluirá todas las rutas a archivos con la extensión `txt` ubicadas en carpetas y subcarpetas de la unidad (C:).
- El carácter **?** (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Carpeta` que tengan la extensión `TXT` y cuyo nombre sea de tres caracteres.

## Edición de plantillas de mensajes de Control de aplicaciones

Cuando un usuario intenta iniciar una aplicación que se encuentra bloqueada por una regla de Control de aplicaciones, Kaspersky Endpoint Security muestra un mensaje que indica que la aplicación está bloqueada desde el inicio. Si el usuario cree que el inicio de la aplicación se bloqueó por error, puede utilizar el enlace del texto del mensaje para enviar un mensaje al administrador de la red de área local.

Existen plantillas especiales disponibles para el mensaje que se muestra cuando se bloquea el inicio de una aplicación y para el mensaje que se envía al administrador. Puede modificar las plantillas de los mensajes.

*Para editar una plantilla de mensaje:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Controles de seguridad** → **Control de aplicaciones**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control de aplicaciones:
  - **Mensaje sobre el bloqueo.** Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.
  - **Mensaje para el administrador.** Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del inicio de la aplicación**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.
4. Guarde los cambios.

## Mejores prácticas para implementar una lista de aplicaciones permitidas

Al planear la implementación de la lista de aplicaciones permitidas, se recomienda realizar las acciones siguientes:

1. Forme los siguientes tipos de grupos:
  - Grupos de usuarios. Los grupos de usuarios para los que tiene que permitir el uso de varios conjuntos de aplicaciones.
  - Grupos de administración. Uno o varios grupos de equipos a los que Kaspersky Security Center aplicará la lista de aplicaciones permitidas. Es necesario crear varios grupos de equipos si se utiliza una configuración de lista de admitidos distinta para esos grupos.
2. Crear una lista de aplicaciones que se debe permitir comenzar.

Antes de crear una lista, se le recomienda hacer lo siguiente:

  - a. Ejecute la tarea de inventario.

La información sobre la creación, reconfiguración e inicio de una tarea de inventario está disponible en la sección Gestión de tareas.

b. Vea la [lista de archivos ejecutables](#).

## Configuración del modo de lista de admitidos para aplicaciones

Al configurar el modo de la lista de admitidos, se recomienda realizar las acciones siguientes:

1. Crear [categorías de aplicaciones](#) que contengan las aplicaciones cuya ejecución se debe permitir.

Puede seleccionar uno de los siguientes métodos para crear categorías de aplicaciones:

- **Categoría con contenido añadido manualmente.** Puede añadir contenido manualmente a esta categoría usando las condiciones siguientes:
  - Metadatos de archivo. Kaspersky Security Center añade todos los archivos ejecutables con los metadatos especificados a la categoría de aplicación.
  - Código hash del archivo. Kaspersky Security Center añade todos los archivos ejecutables con el hash especificado a la categoría de aplicación.

El uso de esta condición excluye la capacidad de instalar automáticamente actualizaciones porque las versiones diferentes de los archivos tendrán un hash diferente.

- Certificado de archivo. Kaspersky Security Center añade todos los archivos ejecutables firmados con el certificado especificado a la categoría de aplicación.
- Categoría KL. Kaspersky Security Center añade todos los archivos que están en la categoría KL especificada a la categoría de aplicación.
- Carpeta de la aplicación. Kaspersky Security Center añade todos los archivos ejecutables de esta carpeta a la categoría de aplicación.

El uso de la condición de la carpeta de la aplicación puede no ser seguro porque se permitirá la ejecución de cualquier aplicación de la carpeta especificada. Se recomienda aplicar reglas que usen las categorías de aplicaciones con la condición de la carpeta Aplicación solo para aquellos usuarios que requieran la autorización de la instalación automática de actualizaciones.

- **Categoría que incluye archivos ejecutables de una carpeta específica.** Puede especificar una carpeta desde la cual los archivos ejecutables se asignarán automáticamente a la categoría de aplicación creada.
- **Categoría que incluye archivos ejecutables desde dispositivos seleccionados.** Puede especificar un equipo para el que todos los archivos ejecutables se asignarán automáticamente a la categoría de aplicación creada.

Al usar este método de creación de categorías de aplicaciones, Kaspersky Security Center recibe información sobre las aplicaciones en el equipo desde la carpeta [Archivos ejecutables](#).

2. [Seleccione el modo de lista de admitidos](#) para el componente Control de aplicaciones.

### 3. [Cree Reglas de control de aplicaciones](#) usando las categorías de aplicaciones creadas.

La regla **Golden Image** y la regla **Actualizadores de confianza** se definen inicialmente para el modo Lista de admitidos. Estas reglas de Control de aplicaciones corresponden a las categorías KL. La categoría KL "Golden Image" incluye programas que garantizan el funcionamiento normal del sistema operativo. La categoría KL "Actualizadores de confianza" incluye programas de actualización de los proveedores de software más prestigiosos. No puede eliminar estas reglas. La configuración de estas reglas no se puede editar. De forma predeterminada, la regla **Golden Image** está activada y la regla **Actualizadores de confianza** está desactivada. Todos los usuarios tienen permiso para iniciar aplicaciones que cumplan las condiciones de activación de estas reglas.

### 4. Determine las aplicaciones para las que hay que permitir la instalación automática de actualizaciones.

Puede permitir la instalación automática de actualizaciones de una de estas formas:

- Especifique una lista ampliada de aplicaciones permitidas autorizando el inicio de todas las aplicaciones que pertenecen a una categoría KL.
- Especifique una lista ampliada de aplicaciones permitidas autorizando el inicio de todas las aplicaciones que están firmadas con certificados.

Para permitir el inicio de todas las aplicaciones firmadas con certificados, puede crear una categoría con una condición basada en el certificado que solo use el parámetro **Asunto** 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.

Quando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.

- Cree una carpeta y coloque en ella los archivos ejecutables de las aplicaciones que podrán actualizarse automáticamente. A continuación, cree una categoría de aplicaciones con la condición "Carpeta de la aplicación" y especifique la ruta de acceso a la carpeta. Por último, cree una regla de permiso y seleccione esta nueva categoría.

El uso de la condición de la carpeta de la aplicación puede no ser seguro porque se permitirá la ejecución de cualquier aplicación de la carpeta especificada. Se recomienda aplicar reglas que usen las categorías de aplicaciones con la condición de la carpeta Aplicación solo para aquellos usuarios que requieran la autorización de la instalación automática de actualizaciones.

## Prueba del modo de lista de admitidos

Para asegurarse de que las reglas de Control de aplicaciones no bloquean las aplicaciones requeridas para el trabajo, se recomienda activar la comprobación de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear reglas nuevas. Cuando esté activado el modo de prueba, Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio esté prohibido por las reglas de Control de aplicaciones, pero sí enviará notificaciones sobre su inicio al Servidor de administración.

Al probar el modo de lista de admitidos, se recomienda realizar las acciones siguientes:

1. Determine el período de pruebas (puede ser desde varios días hasta dos meses).
2. Active la [comprobación de las reglas de Control de aplicaciones](#).
3. Examine, a fin de analizar los resultados de la prueba, [los eventos que resulten de probar el funcionamiento de Control de aplicaciones](#) y los [informes sobre las aplicaciones bloqueadas en el modo de prueba](#).
4. Según los resultados de análisis, haga cambios en la configuración del modo de lista de admitidos.  
En particular, en función de los resultados de la prueba, puede añadir [archivos ejecutables relacionados con eventos a una categoría de aplicación](#).

## Soporte para el modo de lista de admitidos

Después de [seleccionar una acción de bloqueo para el Control de aplicaciones](#), se recomienda continuar admitiendo el modo de lista de admitidos con las acciones siguientes:

- [Examine los eventos generados por el funcionamiento del Control de aplicaciones y los informes sobre ejecuciones bloqueadas](#) para analizar la eficacia del Control de aplicaciones.
- Analice las solicitudes de los usuarios para acceder a las aplicaciones.
- Analice los archivos ejecutables desconocidos comprobando su reputación en [Kaspersky Security Network](#).
- Antes de instalar actualizaciones para el sistema operativo o para el software, instale esas actualizaciones en un grupo de prueba de equipos para verificar cómo serán procesadas por las reglas de Control de aplicaciones.
- Añada las aplicaciones necesarias a las categorías utilizadas en las reglas de Control de aplicaciones.


## Supervisión de puertos de red

Durante el funcionamiento de Kaspersky Endpoint Security, los componentes [Control web](#), [Protección frente a amenazas en el correo](#) y [Protección frente a amenazas web](#) supervisan los flujos de datos que se transmiten mediante protocolos específicos y que pasan a través de puertos TCP y UDP concretos que se encuentran abiertos en el equipo del usuario. Por ejemplo, el componente Protección frente a amenazas en el correo analiza la información que se transmite mediante SMTP, mientras que el componente Protección frente a amenazas web analiza la información que se transmite mediante HTTP y FTP.

Kaspersky Endpoint Security divide los puertos TCP y UDP del equipo del usuario en varios grupos, según las probabilidades de que se vean en riesgo. Algunos puertos de red están reservados para servicios vulnerables. Se recomienda prestar especial atención a ellos: existe un riesgo mucho mayor de que se los utilice en un ataque de red. Si usa servicios no estándares que dependen de puertos de red no estándares, dichos puertos de red también pueden ser el objetivo de los equipos atacantes. Puede especificar una lista de puertos de red y una lista de aplicaciones que solicitan acceso a la red. Estos puertos y aplicaciones recibirán atención especial de los componentes Protección frente a amenazas en el correo y Protección de amenazas web durante la supervisión del tráfico de red.


## Activación de la vigilancia de todos los puertos de red

Para activar la vigilancia de todos los puertos de red, haga lo siguiente:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En la sección **Puertos vigilados**, seleccione **Vigilar todos los puertos de red**.
4. Guarde los cambios.

## Creación de una lista de puertos de red supervisados

Para crear una lista de puertos de red supervisados:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En la sección **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.
4. Haga clic en el botón **Seleccionar**.

Esto despliega una lista de puertos de red que se usan normalmente para la transmisión de correos electrónicos y el tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
5. Utilice el interruptor en la columna **Estado** para activar o desactivar la supervisión del puerto de red.
6. Si no aparece un puerto de red en la lista de puertos de red, agréguelo del siguiente modo:
  - a. Haga clic en el botón **Añadir**.
  - b. En la ventana que se abre, introduzca el número de puerto de red y una breve descripción.
  - c. Configure el estado **Activo** o **Inactivo** para la supervisión del puerto de red.
7. Guarde los cambios.


Cuando el protocolo FTP se ejecuta en modo pasivo, la conexión se puede establecer a través de un puerto de red al azar que no se añade a la lista de puertos de red supervisados. Para proteger tales conexiones, [habilite la supervisión de todos los puertos de red](#) o [configure el control de los puertos de red para aplicaciones que establecen conexiones FTP](#).

## Creación de una lista de aplicaciones para las que se supervisan todos los puertos de red

Puede crear una lista de aplicaciones para las que Kaspersky Endpoint Security supervisa todos los puertos de red.

Recomendamos incluir las aplicaciones que reciben o transmiten datos mediante el protocolo FTP en la lista de aplicaciones para las que Kaspersky Endpoint Security supervisa todos los puertos de red.

*Para crear una lista de aplicaciones para las que se supervisan todos los puertos de red:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de red**.
3. En la sección **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.
4. Active la casilla **Vigilar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky**.

Cuando esta casilla está activada, Kaspersky Endpoint Security supervisa todos los puertos usados por las siguientes aplicaciones:

- Adobe 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 el botón **Seleccionar**.

Esto abre una lista de aplicaciones para las que Kaspersky Endpoint Security supervisa los puertos de red.

7. Utilice el interruptor en la columna **Estado** para activar o desactivar la supervisión del puerto de red.

8. Si una aplicación no está incluida en la lista, agréguela del modo siguiente:

- a. Haga clic en el botón **Añadir**.

- b. En la ventana que se abre, introduzca la ruta al archivo ejecutable de la aplicación y una breve descripción.



c. Configure el estado **Activo** o **Inactivo** para la supervisión de los puertos de red.

9. Guarde los cambios.

## Exportación e importación de listas de puertos vigilados

Kaspersky Endpoint Security utiliza las siguientes listas para supervisar los puertos de red: lista de puertos de red y lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security. Puede exportar listas de puertos vigilados a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de puertos con la misma descripción. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de las listas de puertos vigilados o para migrar las listas a un servidor diferente.

[Cómo exportar e importar listas de puertos vigilados en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Configuración de red**.
6. En la sección **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.
7. Haga clic en el botón **Configuración**.

Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos que se usan normalmente para la transmisión de correo electrónico y tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
8. 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 el botón **Exportar**.
  - c. En la ventana que se abre, introduzca el nombre del archivo XML al que desea exportar la lista de puertos de red y seleccione la carpeta en la que desea guardar este archivo.
  - d. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de puertos de red al archivo XML.
9. Para exportar la lista de aplicaciones cuyos puertos son supervisados por 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 el botón **Exportar**.
  - d. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de aplicaciones y seleccione la carpeta en la que desee guardar este archivo.
  - e. Guarde el archivo.

Kaspersky Endpoint Security exporta la lista completa de aplicaciones al archivo XML.
10. Para importar la lista de puertos de red:
  - a. En la lista de puertos de red, haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo XML del que quiera importar la lista de puertos de red.

b. Abra el archivo.

Si el equipo ya tiene una lista de puertos de red, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

11. Para importar una lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:

a. En la lista de aplicaciones, haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo XML del que quiera importar la lista de aplicaciones.

b. Abra el archivo.

Si el equipo ya tiene una lista de aplicaciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

12. Guarde los cambios.

[Cómo exportar/importar listas de puertos vigilados en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 la sección **Puertos vigilados**, seleccione **Vigilar solo los puertos de red seleccionados**.
  - b. Haga clic en el enlace **puertos N seleccionados**.  
Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos que se usan normalmente para la transmisión de correo electrónico y tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
  - c. En la lista de puertos de red, seleccione los puertos que desea exportar.
  - d. Haga clic en el botón **Exportar**.
  - e. En la ventana que se abre, introduzca el nombre del archivo XML al que desea exportar la lista de puertos de red y seleccione la carpeta en la que desea guardar este archivo.
  - f. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de puertos de red al archivo XML.
6. Para exportar la lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:
  - a. En la sección **Puertos vigilados**, seleccione la casilla de verificación **Vigilar todos los puertos de las aplicaciones especificadas**.
  - b. Haga clic en el enlace **aplicaciones N seleccionadas**.
  - c. En la lista de aplicaciones, seleccione las aplicaciones que desea exportar.
  - d. Haga clic en el botón **Exportar**.
  - e. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de aplicaciones y seleccione la carpeta en la que desee guardar este archivo.
  - f. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de aplicaciones al archivo XML.
7. Para importar la lista de puertos de red:
  - a. En la lista de puertos de red, haga clic en el botón **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que quiera importar la lista de puertos de red.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de puertos de red, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

8. Para importar una lista de aplicaciones cuyos puertos son supervisados por Kaspersky Endpoint Security:

a. En la lista de aplicaciones, haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo XML del que quiera importar la lista de aplicaciones.

b. Abra el archivo.

Si el equipo ya tiene una lista de aplicaciones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.

9. Guarde los cambios.

## Protección con contraseña

Varios usuarios con distintos niveles de conocimientos informáticos pueden usar un solo equipo. Si los usuarios cuentan con acceso ilimitado a Kaspersky Endpoint Security y su configuración, el nivel general de protección del equipo puede verse reducido. La protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).

Si el usuario que ha iniciado sesión en Windows (el *usuario de la sesión*) tiene el permiso necesario para realizar una acción, Kaspersky Endpoint Security no le solicita un nombre de usuario y contraseña o una contraseña temporal. El usuario obtiene acceso a Kaspersky Endpoint Security de conformidad con los permisos que tiene asignados.

Si el usuario de la sesión no tiene permitido realizar una acción, tiene las siguientes alternativas para obtener acceso a la aplicación:

- Introduzca un nombre de usuario y contraseña.

Este método es conveniente para las operaciones cotidianas. Para realizar una acción protegida con contraseña, se introducen las credenciales de una cuenta de dominio perteneciente a un usuario con el permiso necesario. En este caso, el equipo debe estar en ese dominio. Si el equipo no está en el dominio, puede usar la cuenta de KLAdmin.

- Introduzca una contraseña temporal.

Este método es conveniente para otorgar permisos temporales para realizar acciones bloqueadas (por ejemplo, salir de la aplicación) a usuarios fuera de la red corporativa. Cuando expira una contraseña temporal o se cierra una sesión, Kaspersky Endpoint Security revierte su configuración a su estado anterior.

Cuando un usuario intenta realizar una acción protegida con contraseña, Kaspersky Endpoint Security le solicita al usuario el nombre de usuario y la contraseña o la contraseña temporal (consulte la siguiente figura).

En la ventana de ingreso de contraseña, puede cambiar de idioma solo pulsando **ALT+SHIFT**. El uso de otros accesos directos, incluso si están configurados en el sistema operativo, no funcionan para cambiar de idioma.

The screenshot shows a Kaspersky dialog box titled "¿Seguro que desea cambiar la configuración?". It contains the following elements:

- A "Nombre de usuario:" label above a text input field. Below the field, it says "Valor predeterminado del nombre de usuario: KLAdmin."
- An "Introducir contraseña:" label above a password input field.
- A "No solicitar confirmación durante los próximos:" label above a dropdown menu currently set to "No seleccionado".
- A note at the bottom: "Para cambiar entre los idiomas de entrada, use ALT+SHIFT." followed by a small blue button labeled "ENU".
- Two buttons at the bottom: "Confirmar" (highlighted in blue) and "Cancelar".

Solicitud de contraseña de acceso a Kaspersky Endpoint Security

### Nombre de usuario y contraseña

Para acceder a Kaspersky Endpoint Security, debe introducir sus credenciales de la cuenta de dominio. La protección con contraseña admite las siguientes cuentas:

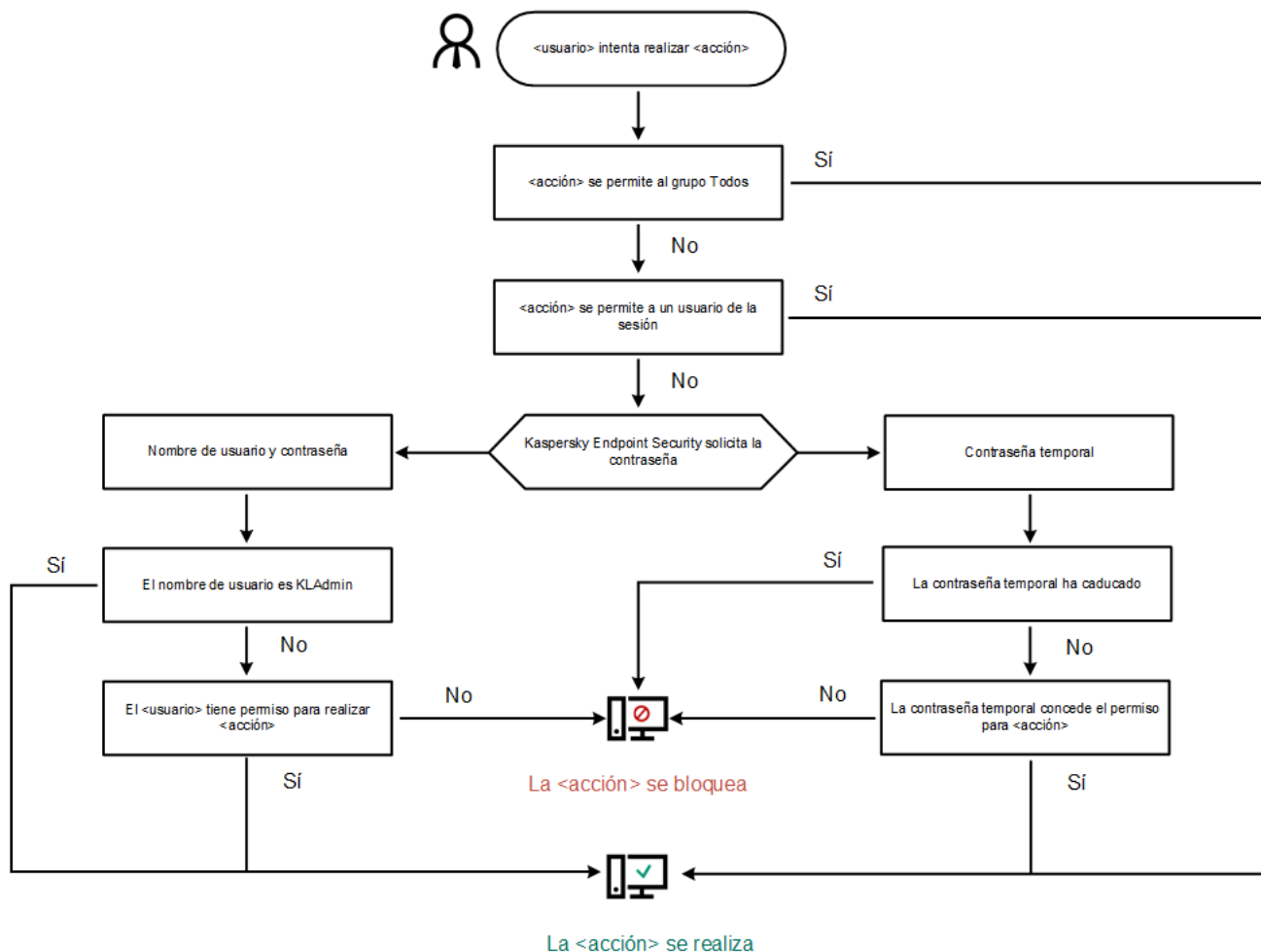
- **KLAdmin.** Una cuenta de administrado con acceso ilimitado a Kaspersky Endpoint Security. La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña. No se pueden revocar los permisos de la cuenta KLAdmin. Cuando habilita la protección con contraseña, Kaspersky Endpoint Security le solicita que configure una contraseña para la cuenta KLAdmin.
- **El grupo Todos.** Un grupo integrado de Windows que incluye a todos los usuarios dentro de la red corporativa. Los usuarios del grupo Todos pueden acceder a la aplicación según los permisos que se le otorgan.
- **Usuarios o grupos individuales.** Las cuentas de usuario para las que puede configurar permisos individuales. Por ejemplo, si se bloquea una acción para el grupo Todos, puede autorizar esta acción para un usuario o un grupo individual.
- **Usuario de sesión.** La cuenta de usuario que inició la sesión de Windows. Puede cambiar a otro usuario de sesión cuando se solicite una contraseña (la casilla **Guardar contraseña para esta sesión**). En este caso, Kaspersky Endpoint Security considera usuario de la sesión al usuario cuyas credenciales de la cuenta se introdujeron, en lugar del usuario que inició la sesión de Windows.

## Contraseña temporal

Se puede utilizar una contraseña temporal para otorgar acceso temporal a Kaspersky Endpoint Security a un equipo particular fuera de la red corporativa. El Administrador genera una contraseña temporal para un equipo particular en las propiedades del equipo de Kaspersky Security Center. El Administrador selecciona las acciones que se protegerán con la contraseña temporal y especifica el período de validez de la contraseña temporal.

## Algoritmo de funcionamiento de la protección con contraseña

Kaspersky Endpoint Security decide si se autoriza o se bloquea una acción protegida con contraseña de acuerdo al siguiente algoritmo (consulte la siguiente figura).




Algoritmo de funcionamiento de la protección con contraseña

## Activar la protección con contraseña

La protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).

Para activar la protección con contraseña:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. Utilice el interruptor **Protección con contraseña** para activar o desactivar el componente.
4. Especifique la contraseña para la cuenta de KLAdmin y confírmela.

La cuenta de KLAdmin tiene el derecho de realizar cualquier acción que esté protegida con contraseña.

Si un equipo se está ejecutando bajo una directiva, el Administrador puede restablecer la contraseña para la cuenta de KLAdmin en las propiedades de la directiva. Si el equipo no está conectado a Kaspersky Security Center y ha olvidado la contraseña de la cuenta de KLAdmin, no es posible recuperar la contraseña.

5. Configure los permisos para todos los usuarios dentro de la red corporativa:



a. En la tabla de la cuenta, haga clic en el botón **Editar** para abrir la lista de permisos para el grupo Todos.

*El grupo Todos* es un grupo integrado de Windows que incluye a todos los usuarios dentro de la red corporativa.

b. Seleccione las casillas ubicadas junto a las acciones que los usuarios podrán realizar sin introducir la contraseña.

Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLSAdmin o como un [usuario individual que tiene el permiso requerido](#), o si introduce una [contraseña temporal](#).

Los permisos de la protección con contraseña tienen algunos [aspectos importantes que se deben tener en cuenta](#). Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.

6. Guarde los cambios.

Cuando se active la protección con contraseña, la aplicación restringirá el acceso de los usuarios a Kaspersky Endpoint Security según los permisos que se le otorgaron al grupo Todos. Solo puede realizar las acciones que están bloqueadas para el grupo Todos si utiliza la cuenta de KLSAdmin, [otra cuenta que tenga los permisos requeridos](#), o si introduce una [contraseña temporal](#).

Para desactivar la protección con contraseña, deberá iniciar sesión con el usuario KLSAdmin. La protección con contraseña no puede desactivarse cuando se está usando una contraseña temporal o cualquier otra cuenta.


Durante la comprobación de contraseña, puede seleccionar la casilla **Guardar contraseña para esta sesión**. En este caso, Kaspersky Endpoint Security no solicitará una contraseña cuando un usuario intente realizar otra acción protegida con contraseña durante la sesión.

## Otorgarle permisos a usuarios o grupos individuales

Puede otorgar acceso a Kaspersky Endpoint Security a usuarios o grupos individuales. Por ejemplo, si salir de la aplicación está bloqueado para el grupo Todos, puede otorgar el permiso para **Salir de la aplicación** a un usuario particular. Por lo tanto, solo puede salir de la aplicación si ha iniciado sesión como ese usuario o como KLSAdmin.

Puede usar las credenciales de la cuenta para acceder a la aplicación solo si el equipo está en el dominio. Si el equipo no está en el dominio, puede usar la cuenta de KLSAdmin o una [contraseña temporal](#).

*Para otorgarle permisos a usuarios o grupos individuales:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En la tabla de la cuenta, haga clic en **Añadir**.
4. En la ventana que se abre, haga clic en el botón **Seleccionar usuario o grupo**.  
Se abrirá el cuadro de diálogo estándar Seleccionar usuarios o grupos.

5. Seleccione un usuario o un grupo de Active Directory y confirme su selección.

6. En la lista **Permisos**, seleccione las casillas que se encuentran junto a las acciones que el usuario o el grupo seleccionados podrán realizar sin que se les solicite una contraseña.

Si se desactiva una casilla, los usuarios no podrán realizar la acción. Por ejemplo, si se desactiva la casilla que está junto al permiso **Salir de la aplicación**, solo puede salir de la aplicación si ha iniciado sesión como KLAdmin o como un [usuario individual que tiene el permiso requerido](#), o si introduce una [contraseña temporal](#).

Los permisos de la protección con contraseña tienen algunos [aspectos importantes que se deben tener en cuenta](#). Asegúrese que se cumplan todos los requisitos para acceder a Kaspersky Endpoint Security.

7. Guarde los cambios.

Por lo tanto, si está restringido el acceso a la aplicación para el grupo Todos, los usuarios recibirán permisos para acceder a Kaspersky Endpoint Security según los permisos individuales de los usuarios.

## Utilizar una contraseña temporal para otorgar permisos

Se puede utilizar una contraseña temporal para otorgar acceso temporal a Kaspersky Endpoint Security a un equipo particular fuera de la red corporativa. Esto es necesario para permitir que el usuario realice una acción bloqueada sin obtener las credenciales de la cuenta KLAdmin. Para utilizar una contraseña temporal, se debe añadir el equipo a Kaspersky Security Center.

[Cómo permitir que un usuario realice una acción bloqueada con una contraseña temporal a través de la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Haga doble clic para abrir la ventana de propiedades del equipo.
5. En la ventana de propiedades del equipo, seleccione la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky que están instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows** y haga doble clic para abrir las propiedades de la aplicación.  
En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
7. En el bloque **Protección con contraseña**, haga clic en el botón **Configuración**.
8. En el bloque **Contraseña temporal**, haga clic en el botón **Configuración**.
9. Se abre la ventana **Crear contraseña temporal**.
10. En el campo **Fecha de caducidad**, especifique la fecha de caducidad en la que expirará la contraseña temporal.
11. En la tabla **Cobertura de la contraseña temporal**, seleccione las casillas que se encuentran junto a las acciones que estarán disponibles para el usuario después de introducir la contraseña temporal.
12. Haga clic en **Generar**.  
Se abrirá una ventana que contiene la contraseña temporal (consulte la siguiente figura).
13. Copie la contraseña y proporciónesela al usuario.

[Cómo permitir que un usuario realice una acción bloqueada con una contraseña temporal a través de Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del equipo en el que 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 **Protección con contraseña**, haga clic en el botón **Contraseña temporal**.
8. En el campo **Fecha de caducidad**, especifique la fecha de caducidad en la que expirará la contraseña temporal.
9. En la tabla **Cobertura de la contraseña temporal**, seleccione las casillas que se encuentran junto a las acciones que estarán disponibles para el usuario después de introducir la contraseña temporal.
10. Haga clic en **Generar**.  
Se abre una ventana con la contraseña temporal.
11. Copie la contraseña y proporciónese la al usuario.



### Acceso denegado

No se puede proporcionar la Dirección web solicitada.

[http://kl-test-page.avp.ru/new\\_ksn\\_samples/AVS\\_RISKWARE-KSN\\_BAD.exe](http://kl-test-page.avp.ru/new_ksn_samples/AVS_RISKWARE-KSN_BAD.exe)

**Razón:**


objeto infectado por [UDS:DangerousObject.Multi.Generic](#)

Mensaje generado: 10/5/2020 5:06:24 PM

# Aspectos especiales de los permisos de la protección con contraseña

Los permisos de la protección con contraseña tienen algunos aspectos y limitaciones importantes que se deben tener en cuenta.


## Configuración de la aplicación

Si el equipo de un usuario se está ejecutando bajo una directiva, asegúrese que toda las configuraciones requeridas de la directiva puedan modificarse (los  atributos estén abiertos).


## Salir de la aplicación

No hay consideraciones ni limitaciones especiales.

## Desactivar componentes de protección

- No se puede otorgar el permiso para desactivar los componentes de protección para el grupo "Todos". Para permitir que otros usuarios además de KLAdmin desactiven los componentes de control, [añada un usuario o un grupo](#) que tenga permiso de **Desactivar componentes de protección** en la configuración de la protección con contraseña.
- Si el equipo de un usuario se está ejecutando bajo una directiva, asegúrese que toda las configuraciones requeridas de la directiva puedan modificarse (los  atributos estén abiertos).
- Para desactivar los componentes de protección en la configuración de la aplicación, un usuario debe tener el permiso **Configurar parámetros de la aplicación**.
- Para desactivar los componentes de protección a través del menú contextual (usando el elemento de menú **Pausar la protección**), el usuario debe contar tanto con el permiso **Desactivar componentes de protección** como con el permiso **Desactivar componentes de control**.

## Desactivar componentes de control

- No se puede otorgar el permiso para desactivar los componentes de control para el grupo "Todos". Para permitir que otros usuarios además de KLAdmin desactiven los componentes de control, [añada un usuario o un grupo](#) que tenga el permiso **Desactivar componentes de control** en la configuración de la protección con contraseña.
- Si el equipo de un usuario se está ejecutando bajo una directiva, asegúrese que toda las configuraciones requeridas de la directiva puedan modificarse (los  atributos estén abiertos).
- Para desactivar los componentes de control en la configuración de la aplicación, un usuario debe tener el permiso **Configurar parámetros de la aplicación**.
- Para desactivar los componentes de control desde el menú contextual (usando el elemento del menú **Pausar la protección**), un usuario debe tener el permiso **Desactivar componentes de control** y el permiso **Desactivar componentes de protección**.

## Desactivar la directiva de Kaspersky Security Center

No es posible asignar al grupo "Everyone" el permiso para deshabilitar la directiva de Kaspersky Security Center. Para que KLAdmin no sea el único usuario autorizado a desactivar la directiva, [añada un usuario o grupo](#) que tenga el permiso **Desactivar la directiva de Kaspersky Security Center** en la configuración de la protección con contraseña.

## Quitar clave

No hay consideraciones ni limitaciones especiales.

## Eliminar/modificar/restaurar la aplicación

Si ha permitido eliminar, modificar y restaurar la aplicación para el grupo "Todos", Kaspersky Endpoint Security no solicita una contraseña cuando el usuario intenta llevar a cabo estas operaciones. Por lo tanto, cualquier usuario, incluidos aquellos usuarios fuera del dominio, puede instalar, modificar o restaurar la aplicación.

## Restaurar el acceso a los datos en las unidades cifradas

Solo puede restaurar el acceso a los datos y a las unidades cifradas si ha iniciado sesión como KLAdmin. No se le puede otorgar a ningún otro usuario el permiso para realizar esta acción.

## Ver informes

No hay consideraciones ni limitaciones especiales.

## Restaurar desde copia de seguridad

No hay consideraciones ni limitaciones especiales.

## Zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza de manera independiente y tiene en cuenta las características de los objetos que se gestionan y de las aplicaciones que se instalan en el equipo. Puede que sea necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a ellos, si está seguro de que el objeto o la aplicación son inofensivos. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza, además de la zona de confianza general en una directiva.

## Creación de una exclusión del análisis

Una *exclusión de análisis* es un conjunto de condiciones que se deben cumplir para que Kaspersky Endpoint Security no analice un objeto en busca de virus u otras amenazas.

Las exclusiones del análisis permiten utilizar de manera segura software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario. Aunque no poseen ninguna función maliciosa, dichas aplicaciones pueden ser aprovechadas por los intrusos. Para obtener más información sobre el software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos personales de un usuario, visite el [sitio web de la Enciclopedia de Kaspersky](#).

Es posible que Kaspersky Endpoint Security bloquee estas aplicaciones. Para evitar que se bloqueen, puede configurar las exclusiones del análisis para las aplicaciones en uso. Para ello, añada el nombre o la máscara de nombre que figura en la Enciclopedia de Kaspersky a la zona de confianza. Por ejemplo, a menudo se utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security identifica esta actividad como sospechosa y puede que la bloquee. Para evitar el bloqueo de la aplicación, cree una exclusión del análisis con el nombre o la máscara de nombre que se muestra en la Enciclopedia de Kaspersky.

Si la aplicación que recopila la información y la envía para procesarse se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar que esto ocurra, puede excluir la aplicación del análisis mediante la configuración de Kaspersky Endpoint Security como se describe en este documento.

Los siguientes componentes de aplicaciones y tareas que el administrador del sistema configure pueden utilizar exclusiones del análisis:

- [Detección de comportamiento.](#)
- [Prevención de exploits.](#)
- [Prevención de intrusiones en el host.](#)
- [Protección frente a amenazas en archivos.](#)
- [Protección frente a amenazas web.](#)
- [Protección frente a amenazas en el correo.](#)
- [Tareas de análisis.](#)

Kaspersky Endpoint Security no analiza un objeto si la unidad de disco o la carpeta que contiene este objeto se incluyen en la cobertura del análisis al inicio de una de las tareas de análisis. Sin embargo, no se aplica la exclusión del análisis cuando se inicia una tarea de análisis personalizado para este objeto en particular.

[Cómo crear una exclusión del análisis en la Consola de administración \(MMC\)](#) 



1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones**.
6. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
7. En la ventana abierta, seleccione la pestaña **Exclusiones de análisis**.  
Esto abre una ventana que incluye una lista de exclusiones.
8. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.
9. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.  
Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
10. Haga clic en el botón **Añadir**.
11. Para excluir un archivo o una carpeta del análisis:
  - a. En la sección **Propiedades**, seleccione la casilla de verificación **Archivo o carpeta**.
  - b. Haga clic en el enlace **Seleccionar archivo o carpeta** de la sección **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para editarlos)** para abrir la ventana **Nombre de archivo o carpeta**.
  - c. Escriba el nombre del archivo o carpeta (o la máscara de este nombre), o haga clic en **Examinar** y seleccione el archivo o carpeta en el árbol de carpetas.

Usar máscaras:

- El carácter **\*** (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\\*\\*.txt** incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
- Dos caracteres **\*\*** consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres **\** y **/** (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara **C:\Carpeta\\*\*\\*.txt** incluirá todas las rutas a archivos con la extensión TXT que se encuentren

en la carpeta llamada **Carpeta** y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada **Carpeta** que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

d. Guarde los cambios.

12. Para excluir objetos que tengan un nombre específico del análisis:

a. En la sección **Propiedades**, seleccione la casilla de verificación **Nombre de objeto**.

b. Haga clic en el enlace **Introducir un nombre de objeto** de la sección **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para editarlos)** para abrir la ventana **Nombre de objeto**.

c. Introduzca el nombre del objeto según la clasificación de la [Enciclopedia de Kaspersky](#) (por ejemplo, **Email-Worm**, **Rootkit** o **RemoteAdmin**).

Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara **Cliente\***, Kaspersky Endpoint Security excluye los objetos **Client-IRC**, **Client-P2P** y **Client-SMTP** de los análisis.

d. Guarde los cambios.

13. Si desea excluir un archivo individual de los análisis:

a. En la sección **Propiedades**, seleccione la casilla de verificación **Hash de objeto**.

b. Haga clic en el enlace de entrada de hash del objeto para abrir la ventana **Hash de objeto**.

c. Introduzca el hash del archivo o seleccione el archivo haciendo clic en el botón **Examinar**.

Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.

d. Guarde los cambios.

14. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

15. Especifique los componentes de Kaspersky Endpoint Security que van a emplearse en la exclusión del análisis:

a. Haga clic en el enlace **Cualquiera** de la sección **Descripción de la exclusión del análisis (haga clic en los elementos subrayados para editarlos)** para activar el enlace **Seleccionar componentes**.

b. Haga clic en el enlace **seleccionar los componentes** para abrir la ventana **Componentes de protección**.

c. Seleccione las casillas de verificación situadas junto a los componentes a los cuales se debe aplicar la exclusión del análisis.

d. Guarde los cambios.

Si especifica componentes en la configuración de la exclusión, esta se aplicará solo en los análisis que realicen esos componentes de Kaspersky Endpoint Security.

Si no especifica ningún componente en la configuración de la exclusión, esta se aplicará en los análisis que realicen todos los componentes de Kaspersky Endpoint Security.

16. Puede utilizar la casilla de verificación para [detener una exclusión](#) en cualquier momento.

17. Guarde los cambios.

[Cómo crear una exclusión del análisis en Web Console y Cloud Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** → **Exclusiones**.
5. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el enlace **Exclusiones del análisis**.
6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de exclusiones para todos los equipos de la empresa. Se fusionarán las listas de exclusiones en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las exclusiones de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar exclusiones de la directiva principal.
7. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.  
  
Si la casilla de verificación no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
8. Haga clic en el botón **Añadir**.
9. Seleccione cómo desea añadir la exclusión: **Archivo o carpeta**, **Nombre de objeto** o **Hash de objeto**.
10. Si desea excluir un archivo o carpeta de los análisis, seleccione el archivo o carpeta haciendo clic en el botón **Examinar**.  
  
También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres \* y ? al introducir una máscara.
  - El carácter \* (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
  - Dos caracteres \* consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\\*\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT que se encuentren en la carpeta llamada Carpeta y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara C:\\*\*\\*.txt no es válida.
  - El carácter ? (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\???.txt incluirá las rutas a todos los archivos de la carpeta llamada Carpeta que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

11. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Objeto**, introduzca el nombre del tipo de objeto de acuerdo con la clasificación de la [Enciclopedia Kaspersky](#) (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

Se pueden usar máscaras con el carácter `?` (sustituye cualquier carácter único) y el carácter `*` (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Cliente*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

12. Si desea excluir un archivo individual de los análisis, introduzca el hash del archivo en el campo **Hash del archivo**.

Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.


13. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión del análisis.

14. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

15. Puede usar el interruptor para [detener una exclusión](#) en cualquier momento.

16. Guarde los cambios.

### [Cómo crear una exclusión del análisis en la interfaz de la aplicación](#)

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.
4. Haga clic en el botón **Añadir**.
5. Si desea excluir un archivo o carpeta de los análisis, seleccione el archivo o carpeta haciendo clic en el botón **Examinar**.

También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite los caracteres \* y ? al introducir una máscara.

- El carácter \* (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
- Dos caracteres \* consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\\*\*\\*.txt incluirá todas las rutas a archivos con la extensión TXT que se encuentren en la carpeta llamada Carpeta y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara C:\\*\*\\*.txt no es válida.
- El carácter ? (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres \ y / (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara C:\Carpeta\???.txt incluirá las rutas a todos los archivos de la carpeta llamada Carpeta que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

6. Si desea excluir un tipo específico de objeto de los análisis, en el campo **Objeto**, introduzca el nombre del tipo de objeto de acuerdo con la clasificación de la [Enciclopedia Kaspersky](#) (por ejemplo, **Email-Worm**, **Rootkit** o **RemoteAdmin**).

Se pueden usar máscaras con el carácter ? (sustituye cualquier carácter único) y el carácter \* (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara **Cliente\***, Kaspersky Endpoint Security excluye los objetos **Client-IRC**, **Client-P2P** y **Client-SMTP** de los análisis.

7. Si desea excluir un archivo individual de los análisis, introduzca el hash del archivo en el campo **Hash del archivo**.

Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se añadirá a las exclusiones.

8. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión del análisis.

9. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

10. Seleccione el estado **Activo** para la exclusión.

Puede usar el interruptor para [detener una exclusión](#) en cualquier momento.

11. Guarde los cambios.

### Ejemplos de máscara de ruta:

Rutas a los archivos de cualquier carpeta:

- La máscara `*.exe` comprende las rutas a todos los archivos de extensión exe.
- La máscara `ejemplo*` comprende las rutas a todos los archivos de nombre EJEMPLO.

Rutas a los archivos de una carpeta específica:


- La máscara `C:\dir\*.*` comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
- La máscara `C:\dir\*` comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
- La máscara `C:\dir\` comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
- La máscara `C:\dir\*.exe` comprende las rutas a todos los archivos de extensión EXE almacenados en C:\dir\, pero no a los de las subcarpetas de C:\dir\.
- La máscara `C:\dir\test` comprende las rutas a todos los archivos de nombre "prueba" almacenados en C:\dir\, pero no a los almacenados en las subcarpetas de C:\dir\.
- La máscara `C:\dir\*\test` comprende las rutas a todos los archivos de nombre "prueba" almacenados en C:\dir\ y en las subcarpetas de C:\dir\.

Rutas a los archivos de cualquier carpeta que tenga un nombre específico:

- La máscara `C:\dir*\test` comprende todas las rutas a archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir*` comprende 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 "prueba" almacenados en carpetas de nombre "dir", pero no a los almacenados en subcarpetas de esas carpetas.

## Activación y desactivación de una exclusión del análisis



*Para activar o desactivar una exclusión del análisis:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.

3. En el bloque **Exclusiones**, haga clic en el enlace **Administrar exclusiones**.
4. Seleccione la exclusión que necesita en la lista de exclusiones del análisis.
5. Utilice el interruptor junto a un objeto para incluir o excluir este objeto de la cobertura del análisis.
6. Guarde los cambios.

## Selección de los tipos de objetos detectables

*Para seleccionar los tipos de objetos detectables:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En la sección **Tipos de objetos detectados**, seleccione las casillas de verificación de los tipos de objetos que desea que Kaspersky Endpoint Security detecte:
  - [Virus y gusanos](#) 



**Subcategoría:** virus y gusanos (Viruses\_and\_Worms)

**Nivel de amenaza:** alto

Los gusanos y virus tradicionales ejecutan acciones que no autoriza el usuario. Pueden crear copias de ellos mismos, que son capaces de reproducirse.

### Virus tradicionales

Cuando un virus tradicional se introduce en un equipo, lo que hace es infectar un archivo, activarse, realizar acciones maliciosas y añadir copias de sí mismo a otros archivos.

Un virus tradicional se multiplica únicamente en los recursos locales del equipo; no puede penetrar en otros equipos por sí mismo. Solo puede pasar a otro equipo si añade una copia de sí mismo a un archivo almacenado en una carpeta compartida o un CD introducido, o si el usuario reenvía un mensaje de correo electrónico con un archivo infectado como adjunto.

Un código de virus tradicional puede penetrar en varias zonas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de secuencias de scripts* y *virus de macros*.

Los virus pueden infectar los archivos a través de una gran diversidad de técnicas. *Los virus de sobrescritura* escriben su código sobre el código del archivo que se infecta, con lo que borran su contenido. El archivo infectado deja de funcionar y no se puede restaurar. *Los virus parásitos* modifican los archivos y los dejan parcial o completamente funcionales. *Los virus compañeros* no modifican los archivos, pero crean duplicados. Cuando se abre un archivo infectado, se inicia un duplicado de él (lo que es un virus en realidad). También existen los siguientes tipos de virus: *virus de vínculos*, *virus para archivos OBJ*, *virus para archivos LIB*, *virus para código fuente* y muchos otros.

### Gusano

Como ocurre con los virus tradicionales, el código de los gusanos está diseñado para infiltrarse en un equipo, activarse y realizar acciones maliciosas. La denominación de los gusanos se debe a su capacidad para "arrastrarse" de un equipo a otro y para propagar copias a través de diversos canales sin el permiso del usuario.

La principal característica que permite distinguir entre varios tipos de gusanos es la forma en que se propagan. En la siguiente tabla, se ofrece una descripción general de varios tipos de gusanos, que se clasifican por el modo en que se propagan.

Formas de propagación de los gusanos

Tipo	Nombre	Descripción
Email-Worm	Email-Worm	Se propagan a través del correo electrónico. Un mensaje de correo electrónico infectado contiene un archivo adjunto con una copia de un gusano o un enlace a un archivo que se ha cargado en un sitio que se puede haber pirateado o creado exclusivamente para dicho propósito. Al abrir el archivo adjunto, se activa el gusano. Al hacer clic en el enlace, descargar y, a continuación, abrir el archivo, el gusano también comienza a realizar sus acciones maliciosas. Después, continúa propagando copias de sí mismo y buscando otras direcciones de correo electrónico, a las que envía mensajes infectados.
Gusano de mensajería instantánea	Gusanos de cliente de MI	Se propagan a través de clientes de MI.

		<p>Por lo general, dichos gusanos envían mensajes que contienen un enlace a un archivo con una copia del gusano en un sitio web; para ello usan las listas de contactos del usuario. Cuando el usuario descarga y abre el archivo, el gusano se activa.</p>
<b>Gusano IRC</b>	Gusanos de chat de Internet	<p>Se propagan a través de Internet Relay Chats, sistemas de servicios que permiten la comunicación con otros usuarios a través de Internet en tiempo real.</p> <p>Estos gusanos publican un archivo con una copia de ellos mismos o un enlace a un archivo en un chat de Internet. Cuando el usuario descarga y abre el archivo, el gusano se activa.</p>
<b>Net-Worm</b>	Gusanos de red	<p>Estos gusanos se propagan a través de redes de equipos.</p> <p>A diferencia de otros tipos de gusanos, un gusano de red tradicional se propaga sin intervención del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red especialmente creado (exploit) que contiene el código del gusano o una parte de este. Si un equipo "vulnerable" se encuentra en la red, recibe dicho paquete de red. Cuando el gusano penetra completamente en el equipo, se activa.</p>
<b>Gusano de P2P</b>	Gusanos de redes de uso compartido de archivos	<p>Se propagan a través de las redes de uso compartido de archivos entre pares.</p> <p>Para penetrar en una red P2P, el gusano se copia en una carpeta de uso compartido de archivos, que se ubica normalmente en el equipo del usuario. La red P2P muestra información sobre este archivo para que el usuario pueda "encontrar" el archivo infectado en la red al igual que cualquier otro archivo y, a continuación, descargarlo y abrirlo.</p> <p>Los gusanos más sofisticados simulan el protocolo de red de una red P2P determinada: devuelven respuestas positivas a consultas de búsqueda y ofrecen sus copias para descargarlas.</p>
<b>Gusano</b>	Otros tipos de gusanos	<p>Entre otros tipos de gusanos, se incluyen:</p> <ul style="list-style-type: none"> <li>• Gusanos que propagan copias de sí mismos a través de recursos de red. Con las funciones del sistema operativo, pueden analizar las carpetas disponibles de la red, conectarse a equipos en Internet e intentar obtener acceso completo a sus unidades de disco. A diferencia de los tipos de gusanos descritos previamente, los otros tipos de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano.</li> <li>• Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono móvil a otro).</li> </ul>

- [Troyanos \(incluye ransomware\)](#) 

## Subcategoría: Troyanos

**Nivel de amenaza:** alto

A diferencia de los gusanos y los virus, los troyanos no se replican. Por ejemplo, se introducen en un equipo a través del correo electrónico o un navegador cuando el usuario visita una página web infectada. Los troyanos se inician con intervención del usuario. Comienzan a realizar acciones maliciosas inmediatamente después de que se inician.

Los distintos troyanos se comportan de forma diferente en los equipos infectados. Las funciones principales de los troyanos consisten en bloquear, modificar o destruir información, y desactivar equipos o redes. Los troyanos también pueden recibir o enviar archivos, ejecutarlos, mostrar mensajes en la pantalla, solicitar páginas web, descargar e instalar programas y reiniciar el equipo.

Los piratas usan conjuntos de diversos troyanos con frecuencia.

Los distintos tipos de comportamiento de los troyanos se describen en la tabla siguiente.

Tipos de comportamiento de los troyanos en un equipo infectado

Tipo	Nombre	Descripción
<b>Trojan-ArcBomb</b>	Troyanos: "archivos bomba"	Al descomprimirlos, estos archivos aumentan de tamaño de tal forma que el funcionamiento del equipo se ve afectado. Cuando el usuario intenta descomprimir un archivo de esas características, es posible que el equipo se vea ralentizado o se congele; el disco duro puede llenarse de datos "vacíos". Los "archivos bomba" son especialmente peligrosos para los servidores de correo y archivos. Si el servidor usa un sistema automático para procesar la información entrante, un "archivo bomba" puede detener el servidor.
<b>Backdoor</b>	Troyanos para administración remota	Se considera que son los troyanos más peligrosos. En sus funciones, se parecen a las aplicaciones de administración remota que se instalan en los equipos. Estos programas se instalan en un equipo sin que el usuario se dé cuenta de ello, lo que permite que el intruso administre el equipo de forma remota.
<b>Troyano</b>	Troyanos	Incluyen las siguientes aplicaciones maliciosas: <ul style="list-style-type: none"><li>• <b>Troyanos tradicionales.</b> Estos programas solo ejecutan las funciones principales de los troyanos: bloqueo, modificación o destrucción de información y desactivación de equipos o redes. No cuentan con funciones avanzadas, a diferencia de otros tipos de troyanos descritos en la tabla.</li><li>• <b>Troyanos versátiles.</b> Estos programas tienen funciones avanzadas comunes en varios tipos de troyanos.</li></ul>
<b>Trojan-Ransom</b>	Troyanos de rescate	Toman como "rehén" la información del usuario para modificarla, bloquearla o afectar al funcionamiento del equipo de modo que el usuario pierda la capacidad de usar la información. El intruso pide un rescate al usuario y le promete enviar una aplicación que restaure el rendimiento del equipo y los datos que estaban almacenados en él.
<b>Trojan-Clicker</b>	Troyanos de clic	Acceden a las páginas web desde el equipo del usuario, ya sea enviando comandos a un navegador o cambiando las

		<p>direcciones web que se especifican en los archivos del sistema operativo.</p> <p>Con estos programas, los intrusos perpetrarán ataques de red y aumentarán las visitas al sitio web mediante un mayor número de visualizaciones de anuncios publicitarios.</p>
<b>Trojan-Downloader</b>	Descargador de troyanos	<p>Acceden a la página web del intruso, descargan otras aplicaciones maliciosas desde ella y las instalan en el equipo del usuario. Pueden contener el nombre de archivo de la aplicación maliciosa que se va a descargar o recibirla desde la página web a la que se accede.</p>
<b>Trojan-Dropper</b>	Troyanos lanzadera	<p>Contienen otros troyanos que instalan en el disco duro y después se instalan.</p> <p>Los intrusos pueden usar programas del tipo Trojan Dropper para los siguientes propósitos:</p> <ul style="list-style-type: none"> <li>• Instalar una aplicación maliciosa sin que el usuario se dé cuenta: los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (pueden, por ejemplo, advertir sobre la existencia de un archivo dañado o sobre incompatibilidades con el sistema operativo).</li> <li>• Para proteger a otra aplicación maliciosa y evitar que se detecte: no todo el software antivirus puede detectar una aplicación maliciosa en una aplicación del tipo Trojan Dropper.</li> </ul>
<b>Trojan-Notifier</b>	Troyanos de notificación	<p>Le informan al atacante que el equipo infectado está accesible y le envían información: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso a través del correo electrónico o el FTP, mediante la página web del intruso o de otro modo.</p> <p>Los programas del tipo Trojan Notifier se usan normalmente como conjuntos compuestos de varios troyanos. Notifican al intruso de que se han instalado correctamente otros troyanos en el equipo del usuario.</p>
<b>Trojan-Proxy</b>	Proxies de troyanos	<p>Permiten al intruso acceder de forma anónima a las páginas web mediante el equipo del usuario; se usan normalmente para enviar correo no deseado.</p>
<b>Trojan-PSW</b>	Software de robo de contraseñas	<p>El software de robo de contraseñas es un tipo de troyano que roba cuentas de usuario, como datos de registro de software. Estos troyanos buscan datos confidenciales en los archivos del sistema y en el Registro, y los envían al "agresor" por correo electrónico, el FTP o mediante acceso a la página web del intruso, o de cualquier otro modo.</p> <p>Algunos de estos troyanos están clasificados en los distintos tipos que se describen en la tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan en Internet (Trojan-GameThief).</p>
<b>Trojan-Spy</b>	Troyanos espía	<p>Espían a los usuarios con el fin de recopilar información sobre las acciones que el usuario lleva a cabo cuando utiliza el equipo. Pueden interceptar los datos que el usuario introduce en el teclado, tomar instantáneas o recopilar listas</p>

		de aplicaciones activas. Una vez que reciben la información, la transfieren al intruso a través de correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo.
<b>Trojan-DDoS</b>	Troyanos atacantes de redes	<p>Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS). Con frecuencia, los piratas infectan diversos equipos con estos programas, de modo que puedan usar los equipos para atacar un solo servidor a la vez.</p> <p>Los programas de DoS perpetran los ataques desde un solo equipo con conocimiento del usuario. Los programas DDoS (Distributed DoS) perpetran los ataques distribuidos desde varios equipos sin que el usuario del equipo infectado lo perciba.</p>
<b>Trojan-IM</b>	Troyanos que roban información de los usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de usuarios de programas de mensajería instantánea. Transfieren los datos al intruso mediante correo electrónico o FTP, accediendo a la página web del intruso o de otro modo.
<b>Rootkit</b>	Rootkits	Enmascaran otras aplicaciones maliciosas y su actividad, con lo que prolongan la persistencia de las aplicaciones en el sistema operativo. Además, pueden ocultar archivos, procesos en la memoria infectada del equipo o claves del registro que ejecutan aplicaciones maliciosas. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones del equipo del usuario y otros equipos de la red.
<b>Trojan-SMS</b>	Troyanos con formato de mensajes SMS	Infectan teléfonos móviles a través del envío de mensajes a números de teléfono de tarificación especial.
<b>Trojan-GameThief</b>	Troyanos que roban información de los usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, para después enviar estos datos al intruso mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo.
<b>Trojan-Banker</b>	Troyanos que roban cuentas bancarias	Roban datos de cuentas bancarias o de sistemas de dinero electrónico y envían la información al hacker mediante su página web, por correo electrónico, por FTP o usando otros medios.
<b>Trojan-Mailfinder</b>	Troyanos que recopilan direcciones de correo electrónico	Recopilan direcciones de correo electrónico almacenadas en un equipo y las envían al intruso por correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado.

- [Herramientas maliciosas](#) 

## Subcategoría: Herramientas maliciosas

### Nivel de peligrosidad: medio

A diferencia de otros tipos de software malicioso (malware), las herramientas maliciosas no llevan a cabo acciones inmediatamente después de que se inicien. Se pueden almacenar e iniciar de forma segura en el equipo del usuario. Los intrusos usan con frecuencia las funciones de estos programas para crear virus, gusanos y troyanos; perpetrar ataques de red en servidores remotos; piratear equipos o llevar a cabo otras acciones maliciosas.

Varias funciones de herramientas maliciosas se agrupan por los tipos descritos en la tabla siguiente.

Funciones de herramientas maliciosas

Tipo	Nombre	Descripción
<b>Constructor</b>	Constructores	Permiten la creación de nuevos virus, gusanos y troyanos. Algunos constructores cuentan incluso con una interfaz de ventanas estándar en la que el usuario puede seleccionar el tipo de aplicación maliciosa que creará, la forma de contrarrestar los depuradores y otras funciones.
<b>DoS</b>	Ataques de red	Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS).
<b>Exploit</b>	Exploits	<p>Un exploit es un conjunto de datos o un código de programa que usa las vulnerabilidades de la aplicación en la que se procesa para llevar a cabo una acción maliciosa en un equipo. Por ejemplo, un exploit puede escribir o leer archivos, así como solicitar páginas web "infectadas".</p> <p>Los exploits utilizan las vulnerabilidades de distintas aplicaciones o servicios de red. Disfrazado como paquete de red, un exploit se transfiere a través de la red a diversos equipos. Busca equipos con servicios de red vulnerables. Un exploit en un archivo DOC usa las vulnerabilidades de un editor de textos. Puede comenzar a ejecutar las acciones preprogramadas por el pirata cuando el usuario abra el archivo infectado. Un exploit incrustado en un mensaje de correo electrónico busca vulnerabilidades en cualquier cliente de correo electrónico. Puede empezar a realizar acciones maliciosas en cuanto el usuario abra el mensaje infectado en este cliente de correo electrónico.</p> <p>Los Net-Worms se propagan por las redes mediante exploits. Los exploits <i>Nuker</i> son paquetes de red que desactivan equipos.</p>
<b>FileCryptor</b>	Cifradores	Cifran otras aplicaciones maliciosas para ocultarlas frente a las aplicaciones antivirus.
<b>Flooder</b>	Programas para contaminar redes	<p>Envían un gran número de mensajes a través de canales de red. Este tipo de herramientas incluye, por ejemplo, los programas que "contaminan" Internet Relay Chats.</p> <p>Las herramientas de tipo Flooder no incluyen programas que "contaminan" los canales que usa el correo electrónico, los clientes de MI y los sistemas de comunicación móvil. Estos programas se distinguen como los distintos tipos que se describen en esta tabla (Email-Flooder, IM-Flooder y SMS-Flooder).</p>

<b>HackTool</b>	Herramientas de pirateo	Permiten hackear el equipo en el que están instalados o atacar a otro equipo (por ejemplo, añadiendo nuevas cuentas de sistema sin el permiso del usuario o borrando los registros del sistema para ocultar los rastros de su presencia en el sistema operativo). Este tipo de herramientas incluye sniffers, que incluyen funciones maliciosas, como la interceptación de contraseñas. Los sniffers son programas que permiten la visualización del tráfico de la red.
<b>Hoax</b>	Hoaxes	Avisan al usuario con mensajes parecidos a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario que el disco se ha formateado, aunque no haya sucedido en realidad.
<b>Spoofing</b>	Herramientas de spoofing	Envían mensajes y solicitudes de red con una dirección de remitente falsa. Los intrusos usan herramientas del tipo Spoofing para pasar como los verdaderos remitentes del mensaje, por ejemplo.
<b>VirTool</b>	Herramientas que modifican aplicaciones maliciosas	Permiten la modificación de otros programas de software malicioso (malware) para ocultarlos de las aplicaciones antivirus.
<b>Email-Flooder</b>	Programas que "contaminan" direcciones de correo electrónico	Envían diversos mensajes a varias direcciones de correo electrónico y las "contaminan" de ese modo. Un gran volumen de mensajes entrantes impide a los usuarios ver los mensajes útiles en la bandeja de entrada.
<b>IM-Flooder</b>	Programas que "contaminan" el tráfico de clientes de MI	Inundan a los usuarios de clientes de MI con mensajes. El gran volumen de mensajes impide que los usuarios vean los mensajes entrantes útiles.
<b>SMS-Flooder</b>	Programas que "contaminan" el tráfico con mensajes SMS	Envían un gran número de mensajes SMS a teléfonos móviles.

- [Software publicitario](#) ⓘ:

**Subcategoría:** software publicitario (adware)

**Nivel de amenaza:** medio

El software publicitario (adware) muestra información publicitaria al usuario. El software publicitario (adware) muestra anuncios publicitarios en la interfaz de otros programas y dirige las búsquedas a páginas web de publicidad. Algunos de ellos recopilan información de marketing del usuario y la envían al desarrollador. Esta información puede incluir los nombres de los sitios web que visita el usuario o el contenido de sus búsquedas. A diferencia de los programas del tipo Trojan-Spy, el software publicitario (adware) envía esta información al desarrollador con el permiso del usuario.

- [Marcadores automáticos \(auto-dialers\)](#) ⓘ:

**Subcategoría:** Software legal que pueden utilizar los delincuentes para dañar su equipo o datos personales.

**Nivel de peligrosidad:** medio

La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de Internet para FTP, HTTP y Telnet.

No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
<b>Client-IRC</b>	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).
<b>Marcadores</b>	Marcadores automáticos (auto-dialers)	Pueden establecer conexión telefónica a través de un módem en modo oculto.
<b>Descargador</b>	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
<b>Monitor</b>	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
<b>PSWTool</b>	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
<b>RemoteAdmin</b>	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlos y gestionarlos. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos.  Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
<b>Server-FTP</b>	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
<b>Server-Proxy</b>	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>Server-Telnet</b>	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.



<b>Server-Web</b>	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
<b>RiskTool</b>	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
<b>NetTool</b>	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
<b>Client-P2P</b>	Cientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
<b>Client-SMTP</b>	Cientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>WebToolbar</b>	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
<b>FraudTool</b>	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.

- [Detectar otro software que los intrusos pueden usar para dañar su equipo o sus datos personales](#) 

**Subcategoría:** Software legal que pueden utilizar los delincuentes para dañar su equipo o datos personales.

**Nivel de peligrosidad:** medio

La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de Internet para FTP, HTTP y Telnet.

No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
<b>Client-IRC</b>	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).
<b>Marcadores</b>	Marcadores automáticos (auto-dialers)	Pueden establecer conexión telefónica a través de un módem en modo oculto.
<b>Descargador</b>	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
<b>Monitor</b>	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
<b>PSWTool</b>	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
<b>RemoteAdmin</b>	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlos y gestionarlos. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos.  Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
<b>Server-FTP</b>	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
<b>Server-Proxy</b>	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>Server-Telnet</b>	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.

<b>Server-Web</b>	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
<b>RiskTool</b>	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
<b>NetTool</b>	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
<b>Client-P2P</b>	Cientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
<b>Client-SMTP</b>	Cientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>WebToolbar</b>	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
<b>FraudTool</b>	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.

- [Objetos comprimidos cuya compresión puede usarse para proteger un código malicioso](#)

Kaspersky Endpoint Security analiza objetos comprimidos y el módulo de descompresión de los archivos SFX (autoextraíbles).

Para ocultar archivos peligrosos de las aplicaciones antivirus, los intrusos los archivan usando compresores especiales o creando archivos comprimidos varias veces.

Los analistas de virus de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

Si Kaspersky Endpoint Security detecta este tipo compresor en un archivo, es muy probable que dicho archivo contenga una aplicación maliciosa o una aplicación que los delincuentes pueden utilizar para dañar el equipo o sus datos personales.

Kaspersky Endpoint Security identifica los siguientes tipos de programas:

- *Archivos comprimidos que pueden causar daños:* se utilizan para comprimir malware, como virus, gusanos y troyanos.
- *Archivos comprimidos varias veces* (nivel de amenaza medio): han comprimido tres veces el objeto usando uno o varios programas compresores.

- [Objetos comprimidos varias veces](#)

Kaspersky Endpoint Security analiza objetos comprimidos y el módulo de descompresión de los archivos SFX (autoextraíbles).

Para ocultar archivos peligrosos de las aplicaciones antivirus, los intrusos los archivan usando compresores especiales o creando archivos comprimidos varias veces.

Los analistas de virus de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

Si Kaspersky Endpoint Security detecta este tipo de compresor en un archivo, es muy probable que dicho archivo contenga una aplicación maliciosa o una aplicación que los delincuentes pueden utilizar para dañar el equipo o sus datos personales.

Kaspersky Endpoint Security identifica los siguientes tipos de programas:

- *Archivos comprimidos que pueden causar daños*: se utilizan para comprimir malware, como virus, gusanos y troyanos.
- *Archivos comprimidos varias veces* (nivel de amenaza medio): han comprimido tres veces el objeto usando uno o varios programas compresores.

4. Guarde los cambios.

## Edición de la lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de red y archivos (incluida la actividad maliciosa), así como el acceso al registro del sistema, no supervisa Kaspersky Endpoint Security. De forma predeterminada, Kaspersky Endpoint Security analiza los objetos que el proceso de cualquier aplicación abre, ejecuta o guarda, y controla la actividad de todas las aplicaciones y el tráfico de red que generan. Sin embargo, una aplicación que se añadió a la lista de aplicaciones de confianza está excluida de los análisis de Kaspersky Endpoint Security.

Por ejemplo, si considera que los objetos que emplea el Bloc de notas estándar de Microsoft Windows son seguros sin necesidad de analizarlos, significa que confía en esta aplicación y que puede añadir el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza. Por tanto, el análisis no incluirá objetos que emplee esta aplicación.

Además, algunas acciones que Kaspersky Endpoint Security clasifica como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de diferentes aplicaciones. Por ejemplo, la interceptación de texto que se escribe mediante el teclado es un proceso rutinario para intercambiadores de disposición del teclado automáticos (como Punto Switcher). Para tener en cuenta los detalles de este tipo de aplicaciones y excluir su actividad del proceso de análisis, le recomendamos que las agregue a la lista de aplicaciones de confianza.

La exclusión de aplicaciones de confianza del proceso de análisis permite evitar conflictos de compatibilidad entre Kaspersky Endpoint Security y otros programas (por ejemplo, el problema de analizar dos veces el tráfico de red de un equipo de terceros, por parte de Kaspersky Endpoint Security y de otra aplicación antivirus) y también aumenta el rendimiento del equipo, que es fundamental cuando se emplean aplicaciones de servidor.

Al mismo tiempo, el archivo ejecutable y el proceso de la aplicación de confianza sí que se analizan en busca de virus y otro software malicioso (malware). Puede excluirse completamente una aplicación del análisis de Kaspersky Endpoint Security gracias a las exclusiones del análisis.

[Cómo añadir una aplicación a la lista de confianza en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general** → **Exclusiones**.
6. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
7. En la ventana abierta, seleccione la pestaña **Aplicaciones de confianza**.  
Esto abre una ventana que contiene una lista de aplicaciones de confianza.
8. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de aplicaciones de confianza para todos los equipos de la empresa. Se fusionarán las listas de aplicaciones de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las aplicaciones de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar aplicaciones de confianza de la directiva principal.
9. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la política. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.  
  
Si la casilla de verificación está desactivada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la política. Si se generó una lista local, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo de los análisis las aplicaciones de confianza enumeradas.
10. Haga clic en el botón **Añadir**.
11. En la ventana abierta, introduzca la ruta al archivo ejecutable de la aplicación de confianza.  
Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al introducir una máscara.  

Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Usuarios\*\Documentos\Archivo.exe`).


Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.
12. Establezca la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).
13. Puede utilizar la casilla de verificación para [excluir una aplicación de la zona de confianza](#) en cualquier momento.
14. Guarde los cambios.



1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** → **Exclusiones**.
5. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el enlace **Aplicaciones de confianza**.  
Esto abre una ventana que contiene una lista de aplicaciones de confianza.
6. Seleccione la casilla de verificación **Fusionar valores al heredar** si desea crear una lista consolidada de aplicaciones de confianza para todos los equipos de la empresa. Se fusionarán las listas de aplicaciones de confianza en las directivas principales y secundarias. Las listas se fusionarán siempre que la combinación de valores al heredar está activada. Las aplicaciones de confianza de la directiva principal se muestran en las directivas secundarias en una vista de solo lectura. No se puede cambiar o eliminar aplicaciones de confianza de la directiva principal.
7. Seleccione la casilla de verificación **Permitir el uso de aplicaciones locales de confianza** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la política. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.  
  
Si la casilla de verificación está desactivada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la política. Si se generó una lista local, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo de los análisis las aplicaciones de confianza enumeradas.
8. Haga clic en el botón **Añadir**.
9. En la ventana abierta, introduzca la ruta al archivo ejecutable de la aplicación de confianza.  
Kaspersky Endpoint Security admite variables de entorno y los caracteres **\*** y **?** al introducir una máscara.  


Kaspersky Endpoint Security no admite la variable de entorno %userprofile% al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter \* (por ejemplo, C:\Usuarios\\*\Documentos\Archivo.exe).

Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.
10. Establezca la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).
11. Puede utilizar la casilla de verificación para [excluir una aplicación de la zona de confianza](#) en cualquier momento.
12. Guarde los cambios.

## Cómo añadir una aplicación a la lista de confianza en la interfaz de la aplicación

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. Seleccione el archivo ejecutable de la aplicación de confianza.

También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres  y  al introducir una máscara.

Kaspersky Endpoint Security es compatible con variables de entorno y convierte la ruta en la interfaz local de la aplicación. En otras palabras, si introduce la ruta de archivo %userprofile%\Documents\File.exe, se añade un registro C:\Users\Fred123\Documents\File.exe en la interfaz local de la aplicación para el usuario Fred123. En consecuencia, Kaspersky Endpoint Security ignora el programa de confianza File.exe para otros usuarios. Para que la entrada se aplique a todas las cuentas de usuario, puede utilizar el carácter  (por ejemplo, C:\Usuarios\\*\Documentos\Archivo.exe).

Cuando se añade una variable de entorno nueva, se debe reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, establezca la configuración avanzada (consulte la tabla a continuación).
7. Puede usar el interruptor para [excluir una aplicación de la zona de confianza](#) en cualquier momento.
8. Guarde los cambios.


### Configuración de la aplicación de confianza

Parámetro	Descripción
<b>No analizar los archivos antes de abrirlos</b>	Todos los archivos abiertos por la aplicación quedan excluidos de los análisis de Kaspersky Endpoint Security. Por ejemplo, si utiliza aplicaciones para realizar copias de seguridad de archivos, esta función ayuda a reducir el consumo de recursos de Kaspersky Endpoint Security.
<b>No supervisar la actividad de la aplicación</b>	Kaspersky Endpoint Security no supervisará la actividad de red y archivos de la aplicación en el sistema operativo. La actividad de la aplicación se supervisa a través de los siguientes componentes: <a href="#">Detección de comportamiento</a> , <a href="#">Prevención de exploits</a> , <a href="#">Prevención de intrusiones en el host</a> , <a href="#">Motor de reparación</a> y <a href="#">Firewall</a> .
<b>No heredar restricciones del proceso principal (aplicación)</b>	Kaspersky Endpoint Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal se inicia a través de una aplicación para la que se configuran los <a href="#">derechos de aplicación</a> (Prevención de intrusiones en el host) y las <a href="#">reglas de red de la aplicación</a> (Firewall).
<b>No supervisar la actividad de</b>	Kaspersky Endpoint Security no supervisará la actividad de archivos ni redes de las aplicaciones iniciadas por esta aplicación.

las aplicaciones secundarias	
Permitir la interacción con la interfaz de la aplicación	<a href="#">Autoprotección de Kaspersky Endpoint Security</a> bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona la casilla de verificación, la aplicación de acceso remoto tiene autorización para administrar la configuración de Kaspersky Endpoint Security mediante la interfaz de Kaspersky Endpoint Security.
No bloquear la interacción con el componente de protección AMSI	Kaspersky Endpoint Security no supervisará las solicitudes de la aplicación de confianza para que el <a href="#">componente de protección AMSI</a> analice objetos.
No analizar el tráfico de red	El tráfico de red iniciado por la aplicación se excluirá de los análisis de Kaspersky Endpoint Security. Puede excluir todo el tráfico o solo el tráfico cifrado de los análisis. También puede excluir direcciones IP individuales y números de puerto de los análisis.
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: <ul style="list-style-type: none"> <li>• El estado <b>Activo</b> significa que la aplicación se encuentra en la zona de confianza.</li> <li>• El estado <b>Inactivo</b> significa que la aplicación está excluida de la zona de confianza.</li> </ul>

## Activación y desactivación de reglas de la zona de confianza para una aplicación en la lista de aplicaciones de confianza

*Para activar o desactivar la acción de las reglas de la zona de confianza aplicadas a una aplicación de la lista de aplicaciones de confianza:*


1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.
4. En la lista de aplicaciones de confianza, seleccione la aplicación de confianza necesaria.
5. Utilice el interruptor en la columna **Estado** para incluir o excluir una aplicación de confianza en la cobertura del análisis.
6. Guarde los cambios.

## Uso del almacén de certificados de confianza del sistema



El uso del almacén de certificados del sistema le permite excluir aplicaciones firmadas por una firma digital de confianza del análisis antivirus. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al Grupo de *confianza*.

*Para comenzar a utilizar el almacén de certificados de confianza del sistema:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En la lista desplegable **Almacén de confianza de certificados del sistema**, seleccione el almacén del sistema en el que debe confiar Kaspersky Endpoint Security.
4. Guarde los cambios.

## Gestión de Copia de seguridad

*Copias de seguridad* almacena copias de seguridad de los archivos que se modificaron o eliminaron durante la desinfección. Una *copia de seguridad* es una copia del archivo creada antes de que el archivo se desinfectara o se eliminara. Las copias de seguridad de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

Las copias de seguridad de los archivos se almacenan en la carpeta C:\ProgramData\Kaspersky Lab\KES\QB.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. El usuario cuya cuenta se usó para instalar la Kaspersky Endpoint Security tiene derechos de acceso limitado a esta carpeta.

Kaspersky Endpoint Security no ofrece la posibilidad de configurar permisos de acceso de usuario a copias de seguridad de los archivos.


En ocasiones no se puede mantener la integridad de los archivos durante la desinfección. Si, después de la desinfección, pierde parcial o completamente el acceso a información importante de un archivo desinfectado, puede intentar restaurarlo a su carpeta original a partir de su copia de seguridad.

Si Kaspersky Endpoint Security funciona mediante la gestión de Kaspersky Security Center, las copias de seguridad de los archivos se pueden transmitir al Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la gestión de copias de seguridad de archivos en Kaspersky Security Center, consulte el sistema de Ayuda de Kaspersky Security Center.

## Configuración del período de almacenamiento máximo de archivos en Copia de seguridad

De forma predeterminada, el período de almacenamiento máximo de copias de archivos en Copia de seguridad es de 30 días. Cuando venza el período máximo de almacenamiento, Kaspersky Endpoint Security eliminará los archivos más antiguos de Copia de seguridad.


*Para configurar el período de almacenamiento máximo para archivos en Copia de seguridad:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Informes y almacenamiento**.
3. Si desea limitar el período de almacenamiento para copias de archivos en Copia de seguridad, seleccione la casilla de verificación **Conservar objetos un máximo de N días** en el bloque **Copia de seguridad**. Escriba la duración máxima de almacenamiento de las copias de los archivos en Copia de seguridad.
4. Guarde los cambios.

## Configuración del tamaño máximo de Copia de seguridad

Puede especificar el tamaño máximo de Copia de seguridad. El tamaño de Copia de seguridad es ilimitado de forma predeterminada. Cuando se alcanza el límite máximo de almacenamiento, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos de Copia de seguridad.

Para configurar el tamaño máximo de Copia de seguridad:

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Informes y Almacenes**.
3. Si desea limitar el tamaño de la Copia de seguridad, seleccione la casilla **Limitar el tamaño de la copia de seguridad a N MB** en el bloque **Copia de seguridad**. Especifique el tamaño máximo de Copia de seguridad.
4. Guarde los cambios.

## Restauración de archivos de Copia de seguridad

Si se detecta código malicioso en un archivo, Kaspersky Endpoint Security lo bloquea, le asigna el estado *Infectado*, coloca una copia en Copia de seguridad e intenta desinfectarlo. Si se realiza la desinfección del archivo correctamente, el estado de la copia de seguridad del archivo pasará a *Desinfectado*. El archivo está disponible en su carpeta original. Si un archivo no se puede desinfectar, Kaspersky Endpoint Security lo elimina de su carpeta original. Puede restaurar el archivo de su copia de seguridad a su carpeta original.

Los archivos con el estado *Se desinfectará al reiniciar el equipo* no se pueden restaurar. Reinicie el equipo y el estado del archivo cambiará a *Desinfectado* o *Eliminado*. También puede restaurar el archivo de su copia de seguridad a su carpeta original.

Al detectar código malicioso en un archivo que forma parte de la aplicación Tienda Windows, Kaspersky Endpoint Security elimina de inmediato el archivo sin que se mueva una copia del archivo a Copia de seguridad. Puede restaurar la integridad de la aplicación de la Tienda Windows por medio de las herramientas adecuadas del sistema operativo Microsoft Windows 8 (consulte los *archivos de ayuda de Microsoft Windows 8* para obtener información detallada sobre la restauración de una aplicación de la Tienda Windows).

El conjunto de las copias de seguridad de los archivos se presenta como una tabla. Para una copia de seguridad de un archivo, se muestra la ruta a la carpeta original del archivo. La ruta a la carpeta original del archivo puede contener datos personales.

Si varios archivos con nombres idénticos y contenido diferente ubicados en la misma carpeta se mueven a Copia de seguridad, solo se podrá restaurar el archivo que se llevó allí en último lugar.

Para restaurar los archivos de Copia de seguridad, haga lo siguiente:

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Copia de seguridad**.
2. Esto abre la lista de archivos en Copia de seguridad; en esa lista, seleccione los archivos que desea restaurar y haga clic en **Restaurar**.

Kaspersky Endpoint Security restaura los archivos a partir de las copias de seguridad seleccionadas en las carpetas originales.

## Eliminación de las copias de seguridad de los archivos de Copia de seguridad

Kaspersky Endpoint Security elimina automáticamente las copias de seguridad de los archivos de Copia de seguridad (independientemente de su estado) una vez que ha vencido el período de almacenamiento establecido en la configuración de la aplicación. También puede eliminar manualmente cualquier copia de un archivo desde Copia de seguridad.

*Para eliminar las copias de seguridad de los archivos de Copia de seguridad:*

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Copia de seguridad**.
2. Esto abre la lista de archivos en Copia de seguridad; en esta lista, seleccione los archivos que desea eliminar de la copia de seguridad y haga clic en **Eliminar**.

Kaspersky Endpoint Security elimina las copias de seguridad seleccionadas de los archivos de Copia de seguridad.

## Servicio de notificaciones

Toda clase de eventos se producen durante el funcionamiento de Kaspersky Endpoint Security. Pueden ser puramente informativos o críticos. Por ejemplo, las notificaciones pueden informar de una actualización de base de datos y de módulos de aplicación exitosa o registrar errores de componentes que se necesitan remediar.

Kaspersky Endpoint Security admite el registro de información sobre eventos en el funcionamiento del registro de aplicaciones de Microsoft Windows y/o del registro de sucesos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security envía notificaciones de las siguientes formas:

- mediante notificaciones emergentes en el área de notificación de la barra de tareas de Microsoft Windows;
- por correo electrónico.


Puede configurar el envío de notificaciones de eventos. El método de envío de notificaciones se configura para cada tipo de evento.

Al usar la tabla de eventos para configurar el servicio de notificaciones, puede realizar las siguientes acciones:

- Filtre los eventos del servicio de notificaciones por valores de columnas o por condiciones de filtro personalizadas.
- Utilice la función de búsqueda para los eventos del servicio de notificaciones.
- Ordene los eventos del servicio de notificaciones.
- Cambie el orden y el conjunto de columnas que aparecen en la lista de eventos del servicio de notificaciones.

## Configuración de los parámetros de registro de eventos

*Para configurar los parámetros del registro de eventos:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En el bloque **Notificaciones**, haga clic en el botón **Configuración de notificaciones**.

Los componentes y tareas de Kaspersky Endpoint Security aparecen en la parte izquierda de la ventana. En la parte derecha de la ventana figuran los eventos generados del componente o tarea seleccionados.

Los eventos pueden contener siguientes datos de usuario:

- Rutas a archivos analizadas por Kaspersky Endpoint Security.
  - Rutas a claves del registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
  - Nombre de usuario de Microsoft Windows.
  - Direcciones de páginas web abiertas por el usuario.
4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los que desee configurar los parámetros del registro de eventos.


5. Seleccione las casillas de verificación de los eventos relevantes de las columnas **Guardar en informe local** y **Guardar en Registro de eventos de Windows**.

Los eventos cuyas casillas están seleccionadas en la columna **Guardar en informe local** se muestran en los [Registros de aplicación](#). Los eventos cuyas casillas están seleccionadas en la columna **Guardar en Registro de eventos de Windows** se muestran en los registros de Windows en el canal **Aplicación**.

6. Guarde los cambios.

## Configuración de la visualización y entrega de notificaciones

*Para configurar la visualización y entrega de notificaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En el bloque **Notificaciones**, haga clic en el botón **Configuración de notificaciones**.

Los componentes y tareas de Kaspersky Endpoint Security aparecen en la parte izquierda de la ventana. En la parte derecha de la ventana, figuran los eventos generados del componente o la tarea seleccionados.

Los eventos pueden contener siguientes datos de usuario:

- Rutas a archivos analizadas por Kaspersky Endpoint Security.
- Rutas a claves del registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
- Nombre de usuario de Microsoft Windows.
- Direcciones de páginas web abiertas por el usuario.

4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los que desee configurar el envío de notificaciones.
5. En la columna **Notificar en pantalla**, seleccione las casillas situadas junto a los eventos relevantes.

La información sobre los eventos seleccionados aparece en mensajes emergentes en pantalla en el área de notificación de la barra de tareas de Microsoft Windows.

6. En la columna **Notificar por correo electrónico**, seleccione las casillas situadas junto a los eventos relevantes.

La información sobre los eventos seleccionados se entrega por correo electrónico si se configuran los ajustes de entrega de notificaciones del correo.

7. Haga clic en **Aceptar**.

8. Si activó las notificaciones por correo electrónico, establezca la configuración para la entrega de correo electrónico:


- a. Haga clic en el botón **Parámetros de notificaciones por correo**.
- b. Seleccione la casilla de verificación **Notificar acerca de eventos** para activar el envío de notificaciones sobre los eventos de Kaspersky Endpoint Security que se seleccionan en la columna **Notificar por correo electrónico**.
- c. Especifique la configuración del envío de notificaciones por correo electrónico.



d. Haga clic en **Aceptar**.

9. Guarde los cambios.

## Configuración de la visualización de advertencias sobre el estado de la aplicación en el área de notificaciones

*Para configurar la visualización de advertencias de estado de la aplicación en el área de notificaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Interfaz**.
3. En la sección **Mostrar el estado de la aplicación en el área de notificaciones**, seleccione las casillas de verificación que hay junto a esas categorías de eventos sobre los cuales desea ver notificaciones en el área de notificaciones de Microsoft Windows.
4. Guarde los cambios.

Cuando tienen lugar eventos asociados con las categorías seleccionadas, el [icono de la aplicación](#) del área de notificaciones cambiará a  o a  según la seriedad de la advertencia.

## Mensajes entre los usuarios y el administrador

Los componentes de [Control de aplicaciones](#), [Control de dispositivos](#), [Control Web](#) y [Control de anomalías adaptativo](#) permiten que los usuarios de una red LAN con equipos que tienen Kaspersky Endpoint Security instalado envíen mensajes al administrador.

Es posible que un usuario deba enviar un mensaje al administrador de la red corporativa local en los casos siguientes:

- Control de dispositivos bloqueó el acceso al dispositivo.  
La plantilla del mensaje para una solicitud de acceso a un dispositivo bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección [Control de dispositivos](#).
- Control de aplicaciones bloqueó el inicio de una aplicación.  
La plantilla del mensaje para solicitar permiso para el inicio de una aplicación bloqueada está disponible en la interfaz de Kaspersky Endpoint Security en la sección [Control de aplicaciones](#).
- Control Web bloqueó el acceso a un recurso web.  
La plantilla del mensaje para solicitar acceso a un recurso web bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección [Control Web](#).

El método usado para enviar mensajes y la plantilla utilizada dependen de si hay una directiva activa de Kaspersky Security Center que se ejecuta en el equipo que tiene Kaspersky Endpoint Security instalado, y si hay alguna conexión con el servidor de administración de Kaspersky Security Center. Son posibles las siguientes situaciones:

- Si una directiva de Kaspersky Security Center no se está ejecutando en el equipo donde se ha instalado Kaspersky Endpoint Security, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

Los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la interfaz local de Kaspersky Endpoint Security.

- Si una directiva de Kaspersky Security Center se está ejecutando en el equipo donde se ha instalado Kaspersky Endpoint Security, el mensaje estándar se envía al servidor de administración de Kaspersky Security Center.

En este caso, los mensajes del usuario se pueden ver en el almacén de eventos de Kaspersky Security Center (consulte las instrucciones más abajo). Los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

- Si la directiva para casos en los que el equipo está fuera de la oficina de Kaspersky Security Center está ejecutándose en el equipo donde se ha instalado Kaspersky Endpoint Security, el método usado para enviar mensajes depende de si existe una conexión con Kaspersky Security Center.
  - Si se establece una conexión con Kaspersky Security Center, Kaspersky Endpoint Security envía el mensaje estándar al servidor de administración de Kaspersky Security Center.
  - Si falta una conexión con Kaspersky Security Center, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

En ambos casos, los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

*Para ver el mensaje de un usuario en el almacén de eventos de Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.

El espacio de trabajo de Kaspersky Security Center muestra todos los eventos que se producen durante el funcionamiento de Kaspersky Endpoint Security, incluidos los mensajes al administrador que se reciben de los usuarios de la red de área local.
3. Para configurar el filtro del evento, en la lista desplegable **Selecciones de eventos**, seleccione **Solicitudes de los usuarios**.
4. Seleccione el mensaje enviado al administrador.
5. Haga clic en el botón **Abrir ventana de propiedades del evento** en la parte derecha del espacio de trabajo de la consola de administración.




# Gestión de informes

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la ejecución de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se registra en informes.

Los informes se almacenan en la carpeta C:\ProgramData\Kaspersky Lab\KES\Report.

Los informes pueden contener siguientes datos de usuario:

- Rutas a archivos analizadas por Kaspersky Endpoint Security.
- Rutas a claves del registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
- Nombre de usuario de Microsoft Windows.
- Direcciones de páginas web abiertas por el usuario.

Los datos del informe se presentan en forma de tabla. Cada fila de la tabla contiene información sobre un evento independiente. Los atributos de eventos se encuentran en las columnas de la tabla. Algunas de las columnas son compuestas, que contienen columnas anidadas con atributos adicionales. Para ver atributos adicionales, haga clic en el botón  situado junto al nombre de la columna. Los eventos que se registran durante el funcionamiento de los diversos componentes o durante el rendimiento de las distintas tareas cuentan con distintos grupos de atributos.


Están disponibles los siguientes informes:

- Informe **Auditoría del sistema**. Contiene información acerca de los eventos producidos durante la interacción entre el usuario y la aplicación, y durante el funcionamiento de la aplicación en general, que no está relacionado con ningún componente o tarea de Kaspersky Endpoint Security en particular.
- Informes sobre el funcionamiento de componentes de Kaspersky Endpoint Security.
- Informes de tarea de Kaspersky Endpoint Security.
- Informe **Cifrado de datos**. Contiene información sobre eventos que tienen lugar durante el cifrado y el descifrado de datos.

Los informes usan los siguientes niveles de importancia de eventos:


 **Mensajes informativos**. Eventos de referencia que, por lo general, no contienen información importante.

 **Advertencias**. Eventos a los que se debe prestar atención porque reflejan situaciones importantes en el funcionamiento de Kaspersky Endpoint Security.

 **Eventos críticos**. Eventos de importancia fundamental que indican problemas en el funcionamiento de Kaspersky Endpoint Security o vulnerabilidades en la protección del equipo del usuario.

Para un procesamiento apropiado de los informes, puede modificar la presentación de los datos en la pantalla de los modos siguientes:

- Filtrado de la lista de eventos por diversos criterios.
- Uso de la función de búsqueda para buscar un determinado evento.
- Visualización del evento seleccionado en una sección independiente.

- Orden de las listas de eventos por cada columna del informe.
- Muestre y oculte eventos agrupados por el filtro de eventos con el botón .
- Cambio del orden y la disposición de las columnas que se muestran en el informe.

Puede guardar un informe generado en un archivo de texto, si es necesario. También puede [eliminar información de informes](#) sobre las tareas y los componentes de Kaspersky Endpoint Security que se combinan en grupos.

Si Kaspersky Endpoint Security funciona mediante la gestión de Kaspersky Security Center, la información sobre los eventos se puede transmitir al Servidor de administración de Kaspersky Security Center (para obtener más información, consulte la [Ayuda de Kaspersky Security Center](#)<sup>2</sup>).

## Ver informes

Si un usuario puede ver informes, el usuario también puede ver todos los eventos reflejados en los informes.

*Para visualizar informes:*

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Informes**.

2. En la lista de componentes y tareas, seleccione un componente o una tarea.

En la parte derecha de la ventana se muestra un informe que contiene una lista de eventos provenientes del funcionamiento del componente o la tarea seleccionados de Kaspersky Endpoint Security. Puede clasificar eventos en el informe según los valores de las celdas de una de las columnas.

3. Para ver información detallada de un evento, seleccione el evento en el informe.

En la parte inferior de la ventana se muestra una sección con el resumen de eventos.

## Configuración del período máximo de almacenamiento del informe

El período de almacenamiento máximo predeterminado de los informes sobre eventos registrados por Kaspersky Endpoint Security es de 30 días. Después de dicho período de tiempo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.

*Para modificar el plazo máximo de almacenamiento de informes:*

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

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


3. Si desea limitar el período de almacenamiento del informe, seleccione la casilla **Conservar objetos un máximo de N días** en el bloque **Informes**. Definir el período máximo de almacenamiento del informe

4. Guarde los cambios.

## Configuración del tamaño máximo del archivo del informe

Puede especificar el tamaño máximo del archivo que contiene el informe. De forma predeterminada, el tamaño máximo de archivo del informe es de 1024 MB. Para evitar superar el tamaño máximo de archivo de informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo de informe cuando se alcance el tamaño máximo en el archivo de informe.

*Para configurar el tamaño máximo del archivo del informe, haga lo siguiente:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Informes y almacenamiento**.
3. En el bloque **Informes**, seleccione la casilla **Limitar el tamaño del archivo del informe a N MB** si desea limitar el tamaño de un archivo del informe. Definir el tamaño máximo del archivo del informe
4. Guarde los cambios.

## Almacenamiento de informes en archivos

El usuario es personalmente responsable de garantizar la seguridad de información desde un informe guardado al archivo y, en particular, para controlar y restringir el acceso a esta información.

Puede guardar el informe que se genera en un archivo en formato de texto (TXT) o un archivo CSV.

Kaspersky Endpoint Security registra eventos en el informe tal y como se muestran en la pantalla, es decir, con el mismo conjunto y secuencia de atributos de eventos.


*Para guardar el informe en un archivo:*

1. En la ventana principal de la aplicación, en la sección **Supervisión**, haga clic en el mosaico **Informes**.
2. Esto abre una ventana donde debe seleccionar el componente o la tarea.  
En la parte derecha de la ventana, se muestra un informe que contiene una lista de eventos en el funcionamiento del componente o tarea seleccionado de Kaspersky Endpoint Security.
3. Si fuera necesario, puede modificar la presentación de los datos en el informe haciendo lo siguiente:
  - Filtrando eventos
  - Realizando una búsqueda de eventos
  - Reorganizando columnas
  - Ordenando eventos
4. Haga clic en el botón **Guardar informe** en la parte superior derecha de la ventana.

5. En la ventana que se abre, especifique la carpeta de destino para el archivo del informe.
6. Escriba el nombre del archivo del informe.
7. Elija el formato de archivo de informe necesario: TXT o CSV.
8. Guarde los cambios.

## Limpieza de informes

*Para quitar información de los informes:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Informes y almacenamiento**.
3. En el bloque **Informes**, haga clic en el botón **Borrar**.
4. Si la [Protección con contraseña está activada](#), Kaspersky Endpoint Security puede solicitarle las credenciales de la cuenta de usuario. La aplicación solicita las credenciales de la cuenta si el usuario no tiene el permiso necesario.

Kaspersky Endpoint Security eliminará todos los informes de todos los componentes y tareas de la aplicación.

# Autoprotección de Kaspersky Endpoint Security

Autoprotección evita que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de Kaspersky Endpoint Security y, por ejemplo, eliminar Kaspersky Endpoint Security del equipo. El conjunto de tecnologías de Autoprotección disponibles para Kaspersky Endpoint Security depende de si el sistema operativo es de 32 o 64 bits (consulte la tabla a continuación).


Tecnologías de Autoprotección de Kaspersky Endpoint Security

Tecnología	Descripción	Equipo x86	Equipo x64
<b>Mecanismo de Autoprotección</b>	La tecnología bloquea el acceso a los siguientes componentes de la aplicación: <ul style="list-style-type: none"><li>archivos en la carpeta de instalación de Kaspersky Endpoint Security y otros archivos de la aplicación;</li><li>claves de registro con informes pertenecientes a la aplicación;</li><li>procesos que la aplicación ejecuta.</li></ul>	✓	✓
<b>AM-PPL (Antimalware Protected Process Light)</b>	La tecnología protege los procesos de Kaspersky Endpoint Security frente a acciones maliciosas. Para obtener más información sobre la tecnología AM-PPL, visite el <a href="#">sitio web de Microsoft</a> .  La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019.	✓	✓
<b>Mecanismo de protección de gestión externa</b>	Esta tecnología evita que las aplicaciones de administración remota (por ejemplo, TeamViewer o RemotelyAnywhere) obtengan acceso a Kaspersky Endpoint Security.	✓	– (excepto para Windows 7)

## Activación y desactivación de Autoprotección

El mecanismo de autoprotección de Kaspersky Endpoint Security está activado de forma predeterminada.

*Para activar o desactivar Autoprotección, haga lo siguiente:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. Utilice la casilla de verificación **Activar la autoprotección** para activar o desactivar el mecanismo Autoprotección.
4. Guarde los cambios.

## Activación y desactivación de la compatibilidad con AM-PPL

Kaspersky Endpoint Security es compatible con la tecnología Antimalware Protected Process Light (en adelante también llamada "AM-PPL") de Microsoft. AM-PPL protege los procesos de Kaspersky Endpoint Security frente a acciones maliciosas (por ejemplo, la finalización de la aplicación). AM-PPL solo permite la ejecución de procesos de confianza. Los procesos de Kaspersky Endpoint Security se firman de acuerdo con los requisitos de seguridad de Windows y, por lo tanto, son de confianza. Para obtener más información sobre la tecnología AM-PPL, visite el [sitio web de Microsoft](#). La tecnología AM-PPL está activada de forma predeterminada.

Kaspersky Endpoint Security también tiene mecanismos integrados para proteger los procesos de las aplicaciones. La compatibilidad con AM-PPL le permite delegar funciones de seguridad de procesos al sistema operativo. De este modo, puede aumentar la velocidad de la aplicación y reducir el consumo de recursos informáticos.

La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019.

*Para activar o desactivar la tecnología AM-PPL:*

1. [Desactive el mecanismo Autoprotección de la aplicación.](#)

El mecanismo Autoprotección evita la modificación y eliminación de procesos de la aplicación en la memoria del equipo, incluido el cambio del estado de AM-PPL.

2. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.

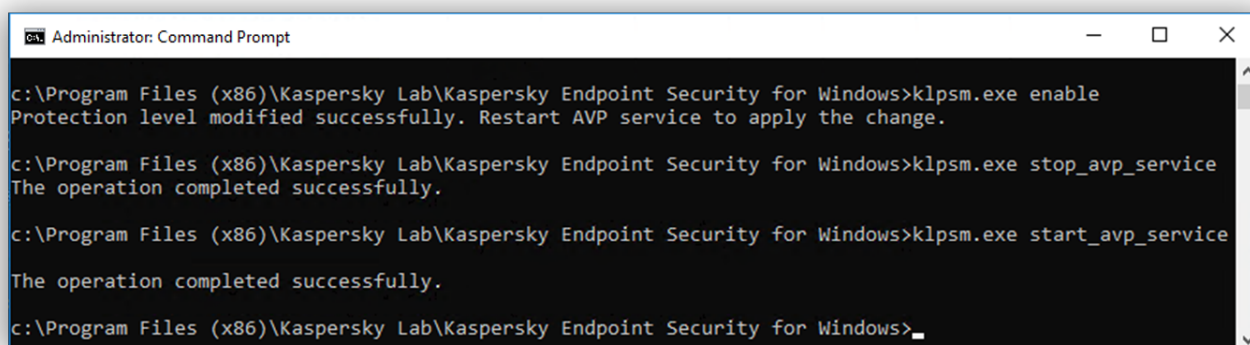
3. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

4. Introduzca lo siguiente en la línea de comandos:

- `klpsm.exe enable`. Active la compatibilidad con la tecnología AM-PPL (vea la imagen más abajo).
- `klpsm.exe disable` – Desactive la compatibilidad con la tecnología AM-PPL.

5. Reinicie Kaspersky Endpoint Security.

6. [Reanude el mecanismo Autoprotección de la aplicación.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Activación de la compatibilidad con la tecnología AM-PPL


## Activación y desactivación de protección de gestión externa

La defensa contra la administración externa evita que las aplicaciones de administración remota (por ejemplo, TeamViewer o RemotelyAnywhere) obtengan acceso a Kaspersky Endpoint Security. Esta tecnología incluye las siguientes funciones de defensa contra la administración externa:

- Protección contra la modificación de la configuración de Kaspersky Endpoint Security.
- Protección de los servicios de Kaspersky Endpoint Security (como el servicio AVP).
- Protección de los procesos de solicitud.

La protección contra la gestión externa solo está disponible para equipos que ejecuten sistemas operativos de 32 bits, excepto Windows 7. En el caso de Windows 7, la tecnología está disponible para sistemas operativos de 32 bits y 64 bits.

*Para activar o desactivar la protección contra la gestión externa:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. Utilice la casilla de verificación **Autorizar la administración de la configuración de Kaspersky Endpoint Security a través de aplicaciones de control remoto** para activar o desactivar la defensa contra la administración externa.

Si la casilla de verificación está seleccionada, puede usar aplicaciones de administración remota para configurar Kaspersky Endpoint Security y administrar sus servicios y procesos.

Si la casilla de verificación está desmarcada, la defensa contra la administración externa evita que las aplicaciones de administración remota obtengan acceso a Kaspersky Endpoint Security. Puede permitir la configuración de Kaspersky Endpoint Security mediante aplicaciones de administración remota específicas. Para hacerlo, debe [añadir la aplicación de administración remota a la lista de confianza](#). En este caso, la defensa contra la administración remota aún evitará que la aplicación de administración remota obtenga acceso a los servicios y procesos de Kaspersky Endpoint Security.

4. Utilice la casilla de verificación **Activar el control remoto de servicios** para activar o desactivar la protección de los servicios de Kaspersky Endpoint Security contra la gestión externa.

Para salir de la aplicación desde la línea de comandos, desactive la protección de los servicios de Kaspersky Endpoint Security contra la gestión externa.


5. Guarde los cambios.

Como resultado, cuando la protección contra la administración externa está activada, Kaspersky Endpoint Security evita que el puntero del ratón entre a la ventana de la aplicación. Cuando un usuario remoto intenta cerrar un servicio de aplicación, aparece una ventana del sistema con un mensaje de error.

## Soporte de las aplicaciones de administración remota

Puede que alguna que otra vez necesite usar una aplicación de administración remota mientras está activada la protección de gestión externa.

*Para activar el funcionamiento de las aplicaciones de administración remota:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el enlace **Especificar aplicaciones de confianza**.
4. En la ventana que se abre, haga clic en el botón **Añadir**.
5. Seleccione el archivo ejecutable de la aplicación de administración remota.  
También puede introducir la ruta manualmente. Kaspersky Endpoint Security admite variables de entorno y los caracteres  y  al introducir una máscara.
6. Seleccione la casilla **No supervisar la actividad de la aplicación**.
7. Guarde los cambios.



# Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones

El rendimiento de Kaspersky Endpoint Security se refiere al número de tipos de objetos que puedan dañar el equipo que son detectables, así como al consumo de energía y uso de los recursos del equipo.

## Selección de los tipos de objetos detectables

Kaspersky Endpoint Security le permite ajustar la protección de su equipo y seleccionar los [tipos de objetos](#) que la aplicación detecta durante su funcionamiento. Kaspersky Endpoint Security el sistema operativo en busca de virus, gusanos y troyanos. No puede desactivar el análisis de estos tipos de objetos. Este tipo de software malicioso (malware) puede provocar daños significativos en el equipo. Para lograr una mayor protección en su equipo, puede ampliar la gama de tipos de objetos detectables si activa el control de software legal que pueden usar los delincuentes para dañar su equipo o sus datos personales.

## Uso del modo de ahorro de energía

El consumo de energía que hacen las aplicaciones es un aspecto básico para los equipos portátiles. Por lo general, las tareas planificadas de Kaspersky Endpoint Security consumen una gran cantidad de recursos. Cuando un equipo se está ejecutando con alimentación de la batería, puede usar el modo de ahorro de energía para moderar su consumo.

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

- Tarea de actualización;
- Tarea de Análisis completo;
- Tarea de Análisis de áreas críticas;
- Tarea de análisis personalizado;
- Tarea de Comprobación de integridad.

Independientemente de si el modo de ahorro de energía está activado o no, Kaspersky Endpoint Security suspende las tareas de cifrado cuando el portátil cambia al funcionamiento con batería. La aplicación reanuda las tareas de cifrado cuando el portátil cambia del funcionamiento con batería al funcionamiento por red eléctrica.

## Concesión de recursos del equipo a otras aplicaciones

El uso que hace Kaspersky Endpoint Security de los recursos del equipo puede afectar al rendimiento de otras aplicaciones. Para solucionar el problema del funcionamiento simultáneo durante el aumento de la carga en los subsistemas del disco duro y la CPU, Kaspersky Endpoint Security puede suspender las tareas planificadas y facilitar recursos para otras aplicaciones.

No obstante, diversas aplicaciones se ejecutan inmediatamente cuando los recursos de la CPU pasan a estar disponibles y siguen funcionando en segundo plano. Para evitar que el análisis dependa del rendimiento de otras aplicaciones, es recomendable no conceder a dichas aplicaciones recursos del sistema operativo.

Si es necesario, puede iniciar dichas tareas manualmente.

## Uso de tecnología de desinfección avanzada

Las aplicaciones maliciosas actuales pueden penetrar en los niveles más bajos del sistema operativo, lo que las hace prácticamente imposibles de eliminar. Tras la detección de actividad maliciosa en el sistema operativo, Kaspersky Endpoint Security lleva a cabo un proceso de desinfección exhaustiva por medio de la tecnología de desinfección avanzada. El objetivo de *la tecnología de desinfección avanzada* consiste en eliminar del sistema operativo las aplicaciones maliciosas que ya han puesto en marcha sus procesos en la memoria RAM y que impiden que Kaspersky Endpoint Security las elimine por medio de otros métodos. Como consecuencia de ello, se neutraliza la amenaza. Cuando la desinfección avanzada está en curso, se recomienda que no ponga en marcha ningún proceso nuevo ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada emplea un número considerable de recursos del sistema operativo, lo que puede ralentizar el resto de las aplicaciones.


Después de que la desinfección avanzada haya finalizado en un equipo que ejecuta con Microsoft Windows para estaciones de trabajo, Kaspersky Endpoint Security solicita el permiso del usuario para reiniciar el equipo. Después del reinicio del sistema, Kaspersky Endpoint Security elimina los archivos de malware e inicia un "pequeño" análisis completo del equipo.

Resulta imposible que se solicite el reinicio en un equipo que se ejecuta con Microsoft Windows para servidores debido a las especificaciones de Kaspersky Endpoint Security. El reinicio de un servidor de archivos no planificado puede conllevar problemas que impliquen la no disponibilidad temporal de los datos del servidor de archivos o la pérdida de datos no guardados. Se recomienda reiniciar el servidor de archivos únicamente de acuerdo con la planificación. Esta es la razón por la cual la tecnología de desinfección avanzada está [desactivada](#) de forma predeterminada para los servidores de archivos.

Si se detecta una infección activa en un servidor de archivos, se envía a Kaspersky Security Center un evento con información que indica que se debe realizar la desinfección activa. Para desinfectar la infección activa de un servidor, active la tecnología de desinfección activa para servidores e inicie una tarea de grupo de *Análisis antivirus* en el momento que resulte adecuado para los usuarios del servidor.

## Activación o desactivación del modo de ahorro de energía

*Para activar o desactivar el modo de conservación de energía:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. En la sección **Rendimiento**, use la casilla de verificación **Posponer tareas planificadas al funcionar con batería** para activar o desactivar el modo de ahorro de energía.


Cuando se activa el modo de conservación de energía y el equipo funciona con la energía de la batería, las tareas siguientes no se ejecutan aunque estén planificadas:

- Tarea de actualización;
- Tarea de Análisis completo;
- Tarea de Análisis de áreas críticas;
- Tarea de análisis personalizado;
- Tarea de Comprobación de integridad.

4. Guarde los cambios.

## Activación o desactivación de la concesión de recursos a otras aplicaciones

*Para activar o desactivar la concesión de recursos a otras aplicaciones:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. En la sección **Rendimiento**, use la casilla de verificación **Facilitar recursos para otras aplicaciones** para activar o desactivar la concesión de recursos a otras aplicaciones.

Cuando se configura la facilitación de recursos para otras aplicaciones, Kaspersky Endpoint Security pospone las tareas planificadas que ralentizan a otras aplicaciones:

- Tarea de actualización;
- Tarea de Análisis completo;
- Tarea de Análisis de áreas críticas;
- Tarea de análisis personalizado;
- Tarea de Comprobación de integridad.

De forma predeterminada, la aplicación está configurada para facilitar recursos para otras aplicaciones.

4. Guarde los cambios.

## Prácticas recomendadas para optimizar el rendimiento de Kaspersky Endpoint Security

Al implementar Kaspersky Endpoint Security para Windows, puede utilizar las siguientes recomendaciones para configurar la protección del equipo y optimizar el rendimiento.

### General

Defina la configuración general de la aplicación de acuerdo con las siguientes recomendaciones:

1. [Actualice Kaspersky Endpoint Security a la versión más reciente.](#)

En las versiones más recientes de la aplicación se han corregido los errores, mejorado la estabilidad y optimizado en rendimiento.

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

La configuración predeterminada se considera óptima. Los expertos de Kaspersky recomiendan esta configuración. La configuración predeterminada proporciona el nivel de protección recomendado y el uso óptimo de los recursos. Si es necesario, puede [restaurar la configuración predeterminada de la aplicación](#).

3. Active las funciones de optimización del rendimiento de la aplicación.

La aplicación tiene funciones de optimización del rendimiento: [modo de conservación de energía](#) y [concesión de recursos a otras aplicaciones](#). Asegúrese de que estas opciones estén activadas.

## Análisis antivirus en estaciones de trabajo

Se recomienda activar [Análisis en segundo plano](#) para el análisis antivirus de estaciones de trabajo. El *análisis en segundo plano* es uno de los modos de análisis disponibles en Kaspersky Endpoint Security. Cuando se realiza un análisis de este tipo, la aplicación no le muestra ninguna notificación al usuario. En comparación con otros tipos de análisis, como el análisis completo, un análisis en segundo plano tiene menos impacto en los recursos del equipo. En este modo, Kaspersky Endpoint Security analiza los objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema. La configuración del análisis en segundo plano se considera óptima. Los expertos de Kaspersky recomiendan esta configuración. Por lo tanto, para realizar un análisis antivirus del equipo, puede usar solo el modo de análisis en segundo plano sin usar otras tareas de análisis.

Si el análisis en segundo plano no se adapta a sus necesidades, configure la tarea *Análisis antivirus* de acuerdo con las siguientes recomendaciones:

### 1. [Configurar el cronograma óptimo de análisis del equipo](#).

Puede configurar la tarea para que se ejecute cuando el equipo esté funcionando con una carga mínima. Por ejemplo, puede configurar la tarea para que se ejecute por la noche o los fines de semana.

Si los usuarios apagan los equipos al final del día, puede configurar la tarea de análisis de la siguiente manera:

- Active Wake-on-LAN. La función Wake-on-LAN permite encender el equipo de forma remota mediante el envío de una señal especial a través de la red local. Para utilizar esta función, debe activar Wake-on-LAN en la configuración del BIOS. También puede hacer que el equipo se apague automáticamente cuando finalice el análisis.
- Desactive la función "Ejecutar tareas perdidas". Kaspersky Endpoint Security omitirá las tareas perdidas cuando el usuario encienda el equipo. La ejecución de tareas después de encender el equipo puede incomodar al usuario, ya que el análisis requiere un gran compromiso de recursos.

Si no pudo configurar un programa de análisis óptimo, configure las tareas para que se ejecuten solo cuando el equipo esté inactivo. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o si el protector de pantalla está activado. Si ha interrumpido la ejecución de la tarea, por ejemplo, al desbloquear el equipo, Kaspersky Endpoint Security ejecuta la tarea automáticamente, continuando desde el punto en el que se interrumpió.

### 2. [Definir una cobertura del análisis](#).

Seleccione los siguientes objetos para analizar:

- Memoria del núcleo;
- Procesos en ejecución y objetos de arranque;
- Sectores de arranque;
- Unidad del sistema (% systemdrive%).

### 3. [Active las tecnologías iSwift e iChecker](#).

- Tecnología iSwift.

Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

- Tecnología iChecker.

Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

Solo puede activar las tecnologías iSwift e iChecker en la Consola de administración (MMC) y la interfaz de Kaspersky Endpoint Security. No puede activar estas tecnologías en Kaspersky Security Center Web Console.

#### 4. [Desactivar el análisis de archivos protegidos con contraseña.](#)

Si el análisis de archivos comprimidos protegidos con contraseña está activado, se muestra una solicitud de contraseña antes de analizar el archivo. Debido a que se recomienda programar la tarea fuera del horario de oficina, el usuario no puede introducir la contraseña. Puede [analizar archivos protegidos con contraseña manualmente](#).

## Análisis antivirus en servidores

Configure la tarea *Análisis antivirus* de acuerdo con las siguientes recomendaciones:

### 1. [Configurar el cronograma óptimo de análisis del equipo.](#)

Puede configurar la tarea para que se ejecute cuando el equipo esté funcionando con una carga mínima. Por ejemplo, puede configurar la tarea para que se ejecute por la noche o los fines de semana.

### 2. [Active las tecnologías iSwift e iChecker.](#)

- Tecnología iSwift.

Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

- Tecnología iChecker.

Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).

Solo puede activar las tecnologías iSwift e iChecker en la Consola de administración (MMC) y la interfaz de Kaspersky Endpoint Security. No puede activar estas tecnologías en Kaspersky Security Center Web Console.

### 3. [Desactivar el análisis de archivos protegidos con contraseña.](#)

Si el análisis de archivos comprimidos protegidos con contraseña está activado, se muestra una solicitud de contraseña antes de analizar el archivo. Debido a que se recomienda programar la tarea fuera del horario de oficina, el usuario no puede introducir la contraseña. Puede [analizar archivos protegidos con contraseña manualmente](#).

## Kaspersky Security Network

A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

*Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security podrá utilizar los servicios de KSN para conocer la categoría y la reputación de los archivos analizados u obtener información sobre la reputación de las direcciones web que se analicen.

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

#### 1. [Desactivar el modo ampliado de KSN.](#)

El *modo KSN ampliado* es un modo en el que Kaspersky Endpoint Security envía [información adicional](#) a Kaspersky.

#### 2. Configurar KSN privada.

*KSN privada.* Esta es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky Security Network y a otros datos estadísticos sin enviar datos a KSN desde sus propios equipos.

#### 3. [Activar modo nube.](#)

*Modo nube* es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky.

# Cifrado de datos

Kaspersky Endpoint Security le permite cifrar las carpetas y los archivos almacenados en las unidades locales y extraíbles, o las unidades extraíbles y los discos duros por completo. El cifrado de datos minimiza el riesgo de filtraciones de información que se puede producir en caso de pérdida o robo del equipo portátil, unidad extraíble o disco duro, o cuando usuarios y aplicaciones no autorizados acceden a los datos. Kaspersky Endpoint Security utiliza el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard").

Si la licencia ha caducado, la aplicación no cifra datos nuevos, y los datos cifrados antiguos permanecen cifrados y disponibles para su uso. En este caso, para cifrar nuevos datos se requiere activar la aplicación con una nueva licencia que permita el uso de cifrado.

Si la licencia ha caducado, si no se ha cumplido el Contrato de licencia de usuario final, si se ha eliminado la clave de licencia o los componentes de cifrado, o si se ha desinstalado Kaspersky Endpoint Security, no se garantiza que los archivos cifrados previamente se encuentren cifrados. La razón es que algunas aplicaciones, como Microsoft Office Word, crean una copia temporal de los archivos cuando se modifican. Cuando se guarda el archivo original, la copia temporal sustituye al archivo original. Por lo tanto, en un equipo que no disponga de funcionalidad de cifrado, o un equipo en la que esta funcionalidad no sea accesible, el archivo permanece sin cifrar.

Kaspersky Endpoint Security ofrece las siguientes características de protección de datos:

- **Cifrado de archivos en unidades locales del equipo.** Puede [compilar listas de archivos](#) por extensión o grupos de extensiones y listas de carpetas almacenadas en las unidades del equipo local, así como crear [reglas para el cifrado de los archivos creados por aplicaciones específicas](#). Después de aplicar una directiva, Kaspersky Endpoint Security cifra y descifra los archivos siguientes:
  - archivos añadidos individualmente a listas para su cifrado y descifrado;
  - archivos almacenados en carpetas añadidos a listas para su cifrado y descifrado;
  - Archivos creados por aplicaciones separadas.
- **Cifrado de unidades extraíbles.** Puede especificar una regla de cifrado predeterminada para que la aplicación lleve a cabo la misma acción en todas las unidades extraíbles o especificar reglas de cifrado de unidades extraíbles particulares.

La prioridad de la regla de cifrado predeterminada es más baja que la de las reglas de cifrado creadas para unidades extraíbles particulares. La prioridad de las reglas de cifrado creadas para las unidades extraíbles del modelo de dispositivo especificado es más baja que la de las reglas de cifrado creadas para las unidades extraíbles cuyo ID de dispositivo es el especificado.

Para seleccionar una regla de cifrado de los archivos de una unidad extraíble, Kaspersky Endpoint Security comprueba si se conocen el modelo de dispositivo y el ID. A continuación, la aplicación realiza una de las siguientes operaciones:

- Si se conoce el modelo de dispositivo únicamente, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles del modelo de dispositivo especificado.
- Si se conoce el ID de dispositivo únicamente, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles con el ID de dispositivo especificado.
- Si se conocen el modelo de dispositivo y el ID, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles con el ID de dispositivo especificado. Si no existe tal regla, pero sí una regla de cifrado creada para unidades extraíbles con el modelo de dispositivo específico, la aplicación aplica esta regla. Si no se especifica ninguna regla de cifrado para el ID de dispositivo específico del modelo de dispositivo concreto, la aplicación aplica la regla de cifrado predeterminada.

- Si no se conocen el modelo de dispositivo ni el ID de dispositivo, la aplicación utiliza la regla de cifrado predeterminada.

La aplicación le permite preparar una unidad extraíble para que pueda utilizar los datos cifrados que contiene en modo portátil. Una vez que active el modo portátil, puede acceder a los archivos cifrados de las unidades extraíbles conectadas al equipo sin la necesidad de disponer de la funcionalidad de cifrado.

- **Gestión de reglas de acceso de las aplicaciones a los archivos cifrados.** Para cualquier aplicación, puede crear una regla de acceso a archivos cifrados que bloquee el acceso a archivos de este tipo o lo permita solo como ciphertext, que es una secuencia de caracteres que se obtiene cuando se aplica el cifrado.
- **Creación de paquetes cifrados.** Puede crear archivos comprimidos cifrados y proteger el acceso a dichos archivos mediante una contraseña. Solo se puede acceder al contenido de los archivos comprimidos cifrados por medio de las contraseñas con las cuales se protegió el acceso a dichos archivos comprimidos. Dichos archivos comprimidos se pueden transmitir de forma segura a través de redes o por medio de unidades extraíbles.
- **Cifrado de disco completo.** Puede seleccionar una tecnología de cifrado: Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker (en adelante también llamado simplemente "BitLocker").

*BitLocker* es una tecnología que forma parte del sistema operativo Windows. Si un equipo está dotado de un módulo de plataforma segura (TPM), BitLocker lo utiliza para almacenar claves de recuperación que proporcionan acceso a un disco duro cifrado. Cuando el equipo se inicia, BitLocker solicita las claves de recuperación del disco duro desde el módulo de plataforma segura y desbloquea la unidad. Puede configurar el uso de una contraseña y un código PIN para acceder a las claves de recuperación.

Puede especificar la regla de cifrado de disco completo predeterminada y crear una lista de discos duros que se deben excluir del cifrado. Kaspersky Endpoint Security realiza un cifrado de disco completo sector por sector cuando se aplica la directiva de Kaspersky Security Center. La aplicación cifra todas las particiones lógicas de los discos duros de forma simultánea.

Después de que se hayan cifrado los discos duros del sistema, en el siguiente inicio de sesión en el equipo, el usuario debe autenticarse en el [Agente de autenticación](#) antes de que se pueda acceder a los discos duros y cargar el sistema operativo. Esto requiere la introducción de la contraseña del token o la tarjeta inteligente conectada al equipo, o bien el nombre de usuario y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local que utilice la tarea [Administrar cuentas del agente de autenticación](#). Estas cuentas se basan en las cuentas de Microsoft Windows con las que los usuarios inician sesión en el sistema operativo. También puede usar la [tecnología de inicio de sesión único \(SSO\)](#), que le permite iniciar sesión automáticamente en el sistema operativo utilizando el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

Kaspersky Endpoint Security duplica las cuentas del Agente de autenticación si crea una copia de seguridad del equipo y cifra los datos de este, y, a continuación, restaura la copia de seguridad del equipo y vuelve a cifrar dichos datos. Para eliminar las cuentas duplicadas, debe usar la herramienta klmover con la clave `dupfix`. La utilidad klmover se incluye en la compilación de Kaspersky Security Center. Puede leer más sobre su funcionamiento en la ayuda de Kaspersky Security Center.

Solo se puede acceder a discos duros cifrados en los equipos en los que se haya instalado Kaspersky Endpoint Security con la funcionalidad de cifrado de disco completo. Esta precaución minimiza el riesgo de fuga de datos de un disco duro cifrado cuando se intenta acceder a él desde el exterior de la red de área local de la compañía.

Para cifrar discos duros y unidades extraíbles, puede utilizar la función [Cifrar solo el espacio en disco utilizado](#). Se recomienda utilizar esta función solo para dispositivos nuevos que no se hayan utilizado anteriormente. Si va a aplicar cifrado a un dispositivo que ya está en uso, se recomienda que cifre el dispositivo completo. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable.



Antes comenzar el cifrado, Kaspersky Endpoint Security obtiene el mapa de los sectores del sistema de archivos. La primera oleada de cifrado incluye los sectores que están ocupados por archivos en el momento en que se inicia el cifrado. La segunda oleada de cifrado incluye los sectores que se escribieron después de que comenzara el cifrado. Una vez que el cifrado se ha completado, todos los sectores que contienen datos están cifrados.

Una vez que el cifrado se ha completado y un usuario elimina un archivo, los sectores que almacenaban el archivo eliminado vuelven a estar disponibles para almacenar nueva información a nivel del sistema de archivos, pero permanecen cifrados. Esto quiere decir que, después de un tiempo, todos los sectores de un dispositivo nuevo terminan por cifrarse, según se van guardando archivos en él, si este se cifra regularmente con la función **Cifrar solo el espacio en disco utilizado**.

El Servidor de administración de Kaspersky Security Center que haya controlado el equipo durante el cifrado proporciona los datos necesarios para descifrar archivos. Si el equipo con objetos cifrados estaba administrado por un Servidor de Administración diferente por algún motivo, puede obtener acceso a los datos cifrados de una de las siguientes maneras:

- Servidores de administración en la misma jerarquía:
  - No necesita realizar ninguna acción adicional. El usuario retendrá el acceso a los objetos cifrados. Las clave de cifrado se distribuyen a todos los Servidores de administración.
- Servidores de administración separados
  - Solicite acceso a los objetos cifrados al administrador de la red de área local.
  - Restaure los datos en los dispositivos cifrados por medio de la Utilidad de restauración.
  - Mediante una copia de seguridad, restaure la configuración del Servidor de administración de Kaspersky Security Center que haya controlado el equipo durante el cifrado y utilice esta configuración en el servidor de administración que ahora controla el equipo con los archivos cifrados.

Si no hay acceso a datos cifrados, siga las instrucciones especiales para trabajar con datos cifrados ([Restaurar el acceso a archivos cifrados](#), [Trabajar con dispositivos cifrados si no existe acceso a estos](#)).

## Limitaciones de funcionalidad del cifrado

El Cifrado de datos tiene las siguientes limitaciones:

- La aplicación crea archivos de servicio durante el cifrado. Se requiere alrededor de un 0,5 % del espacio libre no fragmentado en el disco duro para almacenarlos. Si no hay bastante espacio libre no fragmentado en el disco duro, el cifrado no comenzará hasta que se libere suficiente.
- Puede administrar todos los componentes de cifrado de datos en la Consola de administración de Kaspersky Security Center y en Kaspersky Security Center Web Console. En Kaspersky Security Center Cloud Console, solo puede administrar BitLocker.
- Cifrado de datos solo está disponible al utilizar Kaspersky Endpoint Security con el sistema de administración Kaspersky Security Center o con Kaspersky Security Center Cloud Console (solo para BitLocker). El Cifrado de datos cuando se usa Kaspersky Endpoint Security en modo sin conexión no es posible porque Kaspersky Endpoint Security almacena las claves de cifrado en Kaspersky Security Center.
- Si se instala Kaspersky Endpoint Security en un equipo en el que se ejecuta [Microsoft Windows para servidores](#), solo está disponible el cifrado de disco completo mediante tecnología de Cifrado de unidad BitLocker. Si se instala Kaspersky Endpoint Security en un equipo en el que se ejecuta Windows para estaciones de trabajo, la funcionalidad de cifrado de datos está completamente disponible.

El Cifrado de disco completo con la tecnología Cifrado de disco de Kaspersky no está disponible para los discos duros que no cumplan los requisitos de software y hardware.

No hay respaldo para la compatibilidad entre la funcionalidad de cifrado de disco completo de Kaspersky Endpoint Security y Kaspersky Anti-Virus para UEFI. Kaspersky Anti-Virus for UEFI se inicia antes de que se cargue el sistema operativo. Cuando se usa la característica de cifrado de disco completo, la aplicación detecta que no hay un sistema operativo instalado en el equipo. Esto conduce a que Kaspersky Anti-Virus for UEFI se cierre con un error. El Cifrado de archivos (FLE) no afecta el funcionamiento de Kaspersky Anti-Virus para UEFI.

Kaspersky Endpoint Security admite la siguiente configuración:

- Unidades de disco duro, SSD y USB.

La tecnología Kaspersky Disk Encryption (FDE) permite trabajar con SSD al tiempo que preserva el rendimiento y la vida útil de las unidades SSD.

- Unidades conectadas a través de bus: SCSI, ATA, IEEE1394, USB, RAID, SAS, SATA, NVME.
- Unidades no extraíbles conectadas mediante bus SD o MMC.
- Unidades con sectores de 512 bytes.
- Unidades con sectores de 4096 bytes que emulan 512 bytes.
- Unidades con el siguiente tipo de particiones: GPT, MBR y VBR (unidades extraíbles).
- Software integrado del estándar UEFI 64 y BIOS heredado.
- Software integrado del estándar UEFI con soporte de Secure Boot.

*Secure Boot* es una tecnología diseñada para verificar firmas digitales para aplicaciones y controladores de cargadores UEFI. Secure Boot bloquea el inicio de aplicaciones y controladores UEFI que no están firmados o que están firmados por editores desconocidos. Kaspersky Disk Encryption (FDE) es totalmente compatible con Secure Boot. El Agente de autenticación está firmado por un certificado de Editor de controladores UEFI de Microsoft Windows.

En algunos dispositivos (por ejemplo, Microsoft Surface Pro y Microsoft Surface Pro 2), se puede instalar una lista desactualizada de certificados de verificación de firma digital de forma predeterminada. Antes de cifrar la unidad, debe actualizar la lista de certificados.

- Software integrado del estándar UEFI con soporte Fast Boot.

*Fast Boot* es una tecnología que ayuda a que el equipo se inicie más rápido. Cuando la tecnología Fast Boot está activada, normalmente el equipo carga solo el conjunto mínimo de controladores UEFI necesarios para iniciar el sistema operativo. Cuando la tecnología Fast Boot está activada, es posible que los teclados USB, ratones, tokens USB, paneles táctiles y pantallas táctiles no funcionen mientras el Agente de autenticación se está ejecutando.

Para utilizar el Cifrado de disco de Kaspersky (FDE), se recomienda desactivar la tecnología Fast Boot. Puede utilizar la [Utilidad de prueba FDE](#) para probar el funcionamiento del Cifrado de disco de Kaspersky (FDE).

Kaspersky Endpoint Security no admite las configuraciones siguientes:

- El cargador de arranque se ubica en una unidad mientras que el sistema operativo se halla en una unidad diferente.

- El sistema contiene el software integrado del estándar UEFI 32.
- El sistema cuenta con Intel® Rapid Start Technology y unidades que constan de una partición de hibernación, incluso cuando Intel® Rapid Start Technology está desactivada.
- Unidades de disco en formato MBR con más de 10 particiones ampliadas.
- El sistema tiene un archivo de intercambio ubicado en una unidad de disco que no pertenece al sistema.
- Sistema multiarranque con varios sistemas operativos instalados simultáneamente.
- Particiones dinámicas (solo se admiten las particiones principales).
- Unidades de disco con menos del 0,5% de espacio libre en disco no fragmentado.
- Unidades de disco con un tamaño del sector distinto de 512 bytes o 4096 bytes que emulan 512 bytes.
- Unidades híbridas.
- El sistema tiene cargadores de terceros.
- Unidades con directorios NTFS comprimidos.
- La tecnología de Cifrado de disco de Kaspersky (FDE) es incompatible con otras tecnologías de cifrado de disco completo (como BitLocker, McAfee Drive Encryption y WinMagic SecureDoc).
- La tecnología Cifrado de disco de Kaspersky (FDE) es incompatible con la tecnología Express Cache.
- No se admite la creación, eliminación y modificación de particiones en una unidad cifrada. Podría perder datos.
- El formato del sistema de archivos no es compatible. Podría perder datos.

Si necesita formatear una unidad que fue cifrada con la tecnología de Cifrado de disco de Kaspersky (FDE), formatee la unidad en un equipo que no tenga Kaspersky Endpoint Security para Windows y use solo el cifrado de disco completo.

Una unidad cifrada formateada con la opción de formato rápido puede identificarse erróneamente como cifrada la próxima vez que se conecte a un equipo que tenga instalado Kaspersky Endpoint Security para Windows. Los datos del usuario no estarán disponibles.

- El agente de autenticación no admite más de 100 cuentas.
- La tecnología Single Sign-On es incompatible con otras tecnologías de desarrolladores externos.
- La tecnología de Cifrado de disco de Kaspersky (FDE) no es compatible con los siguientes modelos de dispositivos:
  - Dell Latitude E6410 (modo UEFI)
  - HP Compaq nc8430 (modo BIOS heredado)
  - Lenovo Think Center 8811 (modo BIOS heredado)
- El Agente de autenticación no admite trabajar con tokens USB cuando la compatibilidad con USB heredado está activada. Solo la autenticación basada en contraseña será posible en el equipo.
- Al cifrar una unidad en modo BIOS heredado, se recomienda activar la compatibilidad con USB heredado en los siguientes modelos de dispositivos:

- Acer Aspire 5560G
- Acer Aspire 6930
- Acer TravelMate 8572T
- Dell Inspiron 1420
- Dell Inspiron 1545
- Dell Inspiron 1750
- Dell Inspiron N4110
- Dell Latitude E4300
- Dell Studio 1537
- Dell Studio 1569
- Dell Vostro 1310
- Dell Vostro 1320
- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- HP Compaq dx2450 Microtower PC
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 100

- MSI 760GM-E51 (placa base)

## Cómo cambiar la longitud de la clave de cifrado (AES56 o AES256)

Kaspersky Endpoint Security utiliza el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard"). En Kaspersky Endpoint Security, la longitud de clave efectiva de este algoritmo puede ser de 256 bits o de 56 bits. El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: están disponibles tanto la variante de *cifrado "fuerte" (AES256)* como la de *cifrado "ligero" (AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

Cambiar la longitud de la clave de cifrado solo es posible en Kaspersky Endpoint Security 11.2.0 o posterior.

Para cambiar la longitud de la clave de cifrado, complete estos pasos:

1. Antes de cambiar la longitud de la clave de cifrado, descifre los objetos que Kaspersky Endpoint Security ya haya cifrado:
  - a. [Descifrar los discos duros.](#)
  - b. [Descifre los archivos almacenados en los discos locales.](#)
  - c. [Descifre las unidades extraíbles.](#)

Una vez que cambie la longitud de la clave de cifrado, los objetos que permanezcan cifrados dejarán de estar disponibles.

2. [Elimine Kaspersky Endpoint Security.](#)
3. [Instale Kaspersky Endpoint Security](#) con un paquete de distribución de Kaspersky Endpoint Security que contenga una biblioteca de cifrado diferente.

Otra alternativa para realizar el cambio de longitud consiste en actualizar la aplicación. Para que el cambio pueda hacerse de este modo, se deben cumplir las siguientes condiciones:

- La versión de Kaspersky Endpoint Security instalada en el equipo debe ser la 10 Service Pack 2 o posterior.
- Los componentes de cifrado de datos (Cifrado de archivos, Cifrado de disco completo) no deben estar instalados en el equipo.

De manera predeterminada, Kaspersky Endpoint Security no incluye los componentes de cifrado de datos. El componente Administración de BitLocker no afecta al cambio en la longitud de la clave de cifrado.

Para cambiar la longitud de la clave de cifrado, ejecute el archivo kes\_win.msi o setup\_kes.exe del paquete de distribución que contenga la biblioteca de cifrado necesaria. Si necesita actualizar la aplicación en forma remota, utilice el paquete de instalación.

No se puede cambiar la longitud de la clave de cifrado utilizando el paquete de distribución de la misma versión de la aplicación que está instalada en su equipo sin desinstalar primero la aplicación.

## Cifrado de disco de Kaspersky

El Cifrado de disco de Kaspersky está disponible solo para equipos con un sistema operativo Windows para estaciones de trabajo. Para los equipos con un sistema operativo Windows para servidores, use la tecnología Cifrado de unidad BitLocker.

La característica de cifrado de disco completo de Kaspersky Endpoint Security es compatible con los sistemas de archivos FAT32, NTFS y exFAT.

Antes de empezar el cifrado de disco completo, la aplicación ejecuta una serie de comprobaciones para determinar si el dispositivo se puede cifrar. Esto incluye la comprobación del disco duro del sistema para averiguar si es compatible con el Agente de autenticación o los componentes de cifrado de BitLocker. Para comprobar la compatibilidad, el equipo se debe reiniciar. Tras el reinicio, la aplicación llevará a cabo todas las comprobaciones necesarias automáticamente. Si se supera la comprobación de compatibilidad, la tarea de cifrado de disco completo comenzará después de que el sistema operativo se haya cargado y la aplicación se haya iniciado. Si se determina que el disco duro del sistema no es compatible con Agente de autenticación o con los componentes de cifrado de BitLocker, se deberá reiniciar el equipo pulsando el botón físico de reinicio. Kaspersky Endpoint Security registra información sobre la incompatibilidad. En función de esta información, la aplicación no comenzará el cifrado de disco completo cuando arranque el sistema operativo. La información sobre este evento se registra en informes de Kaspersky Security Center.

Si la configuración de hardware del equipo ha cambiado, se deberá eliminar la información de incompatibilidad registrada por la aplicación durante la comprobación anterior para averiguar la compatibilidad del disco duro del sistema con el Agente de autenticación y los componentes de cifrado de BitLocker. Para ello, escriba `avp pbatestreset` en la línea de comandos antes del cifrado de disco completo. Si el sistema operativo no se carga después de que se haya comprobado la compatibilidad del disco duro del sistema con Agente de autenticación, [debe quitar los objetos y los datos que permanecen tras la operación de prueba del Agente de autenticación](#) con la Utilidad de restauración. A continuación, inicie Kaspersky Endpoint Security y vuelva a ejecutar el comando `avp pbatestreset`.

Cuando comience el cifrado de disco completo, Kaspersky Endpoint Security cifra todos los datos escritos en los discos duros.

Si el usuario apaga o reinicia el equipo durante la tarea de cifrado de disco completo, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el Agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo cambia al modo de hibernación durante el cifrado de disco completo, el Agente de autenticación se carga cuando el sistema operativo vuelve al modo normal. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el Agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el cifrado de disco completo, Kaspersky Endpoint Security reanudará el proceso cuando el sistema operativo vuelva a encontrarse en el modo normal sin cargar el Agente de autenticación.

La autenticación de usuario en Agente de autenticación se puede realizar de dos maneras:

- Introduzca el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local con las herramientas de Kaspersky Security Center.

- Introduzca la contraseña de un token o una tarjeta inteligente conectados al equipo.

El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, no se podrá añadir el archivo del certificado electrónico al comando.

El agente de autenticación admite las distribuciones del teclado para los siguientes idiomas:

- Inglés (Reino Unido)
- Inglés (EE. UU.)
- Árabe (Argelia, Marruecos, Túnez; diseño AZERTY)
- Español (América Latina)
- Italiano
- Alemán (Alemania y Austria)
- Alemán (Suiza)
- Portugués (Brasil; diseño ABNT2)
- Ruso (para teclados IBM de 105 teclas o teclados Windows con el diseño QWERTY)
- Turco (diseño QWERTY)
- Francés (Francia)
- Francés (Suiza)
- Francés (Bélgica, diseño AZERTY)
- Japonés (para teclados de 106 teclas con el diseño QWERTY)

Hay una distribución del teclado disponible en el Agente de autenticación si esta se ha añadido en el idioma y con la configuración regional estándar del sistema operativo, y aparece disponible en la pantalla de bienvenida de Microsoft Windows.

Si el nombre de la cuenta del Agente de autenticación contiene símbolos que no pueden introducirse mediante las distribuciones del teclado disponibles en el Agente de autenticación, solo es posible acceder a los discos duros cifrados después de su restauración mediante la Utilidad de restauración o después de que [se restauren el nombre de la cuenta y la contraseña del Agente de autenticación](#).

## Características especiales del cifrado de unidades SSD

La aplicación admite el cifrado de unidades SSD, unidades SSHD híbridas y unidades con la función Intel Smart Response. La aplicación no admite el cifrado de unidades con la función Intel Rapid Start. Desactive la función Intel Rapid Start antes de cifrar dicha unidad.

El cifrado de unidades SSD tiene las siguientes características especiales:

- Si una unidad SSD es nueva y no contiene datos confidenciales, [habilite el cifrado solo del espacio ocupado](#). Esto le permite sobrescribir los sectores relevantes de la unidad.
- Si una unidad SSD está en uso y tiene datos confidenciales, seleccione una de las siguientes opciones:
  - Limpie completamente la unidad SSD (Secure Erase), instale el sistema operativo y [ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado activada](#).
  - Ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado desactivada.

El cifrado de una unidad SSD requiere de 5 a 10 GB de espacio libre. Los requerimientos de espacio libre para almacenar datos de administración de cifrado se proporcionan en la siguiente tabla.

Requerimientos de espacio libre para almacenar datos de administración de cifrado

Tamaño de la unidad SSD (GB)	Espacio libre en la partición principal de la unidad SSD (MB)	Espacio libre en la partición secundaria de la unidad SSD (MB)
128	250	64
256	250	640
512	300	128

## Cifrado de disco completo con la tecnología Cifrado de disco de Kaspersky

Antes de comenzar el cifrado de disco completo, es aconsejable asegurarse de que el equipo no esté infectado. Para ello, ejecute la tarea Análisis completo o Análisis de áreas críticas. Cifrar un disco completo en un equipo infectado con un rootkit puede provocar que el equipo se inutilice.

*Para cifrar un disco completo con la tecnología Cifrado de disco de Kaspersky:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de disco completo**.
6. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de disco de Kaspersky**.

La tecnología Cifrado de disco de Kaspersky no se puede utilizar si el equipo cuenta con discos duros cifrados por BitLocker.

7. En la lista desplegable **Modo de cifrado**, seleccione **Cifrar todos los discos duros**.



Si el equipo tiene varios sistemas operativos instalados, después de cifrar todos los discos duros solo podrá cargar el sistema operativo que tenga la aplicación instalada.

Si tiene que excluir algunos de los discos duros del cifrado, [cree una lista de estos discos duros](#).

8. Configure las reglas para añadir cuentas del Agente de autenticación durante el cifrado del disco. El agente permite a un usuario completar la autenticación para acceder a unidades cifradas y cargar el sistema operativo. Para añadir automáticamente cuentas del Agente de autenticación, configure los siguientes parámetros:

- **Crear automáticamente cuentas de Agente de Autenticación para los usuarios durante el cifrado.** Si esta casilla de verificación está seleccionada, la aplicación creará cuentas de agente de autenticación según la lista de cuentas de usuario de Windows en el equipo. De forma predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario ha iniciado sesión en el sistema operativo durante los últimos 30 días.
- **Crear automáticamente cuentas del Agente de autenticación para todos los usuarios de este equipo al iniciar sesión.** Si esta casilla de verificación está seleccionada, la aplicación verifica la información sobre las cuentas de usuario de Windows en el equipo antes de iniciar el Agente de autenticación. Si Kaspersky Endpoint Security detecta una cuenta de usuario de Windows que no tiene una cuenta de Agente de autenticación, la aplicación creará una nueva cuenta para acceder a las unidades cifradas. La nueva cuenta del Agente de autenticación tendrá la siguiente configuración predeterminada: inicio de sesión protegido con contraseña únicamente y cambio de contraseña en la primera autenticación. Por lo tanto, no es necesario [añadir manualmente cuentas del Agente de autenticación](#) mediante la tarea *Administrar cuentas del Agente de autenticación* para equipos con unidades ya cifradas.

Si desactivó la creación automática de cuentas del Agente de autenticación, puede [añadir manualmente cuentas del Agente de autenticación](#) mediante la tarea *Administrar cuentas*. También puede utilizar esta tarea para cambiar la configuración de las cuentas del Agente de autenticación que se crearon automáticamente.

9. Para comodidad del usuario, puede guardar el nombre de usuario en la memoria del Agente de autenticación para que el usuario solo tenga que introducir una contraseña la próxima vez que inicie sesión en el sistema. Para hacerlo, seleccione la casilla de verificación **Guardar el nombre de usuario introducido en el Agente de autenticación**.

10. Seleccione uno de los siguientes métodos de cifrado:

- Si desea aplicar el cifrado solo a los sectores del disco duro que están ocupados por archivos, seleccione la casilla **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)**.  
Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable. La función Cifrar solo el espacio en disco utilizado se recomienda para las unidades nuevas que no se han utilizado anteriormente.
- Si desea aplicar el cifrado al disco duro completo, desactive la casilla **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)**.

Si un dispositivo se cifró anteriormente mediante la opción **Cifrar solo el espacio en disco utilizado (reduce el tiempo de cifrado)**, después de aplicar una directiva en el modo **Cifrar todos los discos duros**, los sectores que aún no están ocupados por archivos continúan sin cifrar.

11. Si ocurre un problema de incompatibilidad de hardware durante el cifrado del equipo, puede marcar la casilla **Utilizar Legacy USB Support (no recomendado)**.

*Legacy USB Support* es una función BIOS/UEFI que le permite usar dispositivos USB (como un token de seguridad) durante la fase de inicio del equipo antes de iniciar el sistema operativo (modo BIOS). Legacy USB Support no afecta a la compatibilidad con dispositivos USB después del inicio del sistema operativo.

Cuando la función Legacy USB Support está activada, el Agente de autenticación en el modo BIOS no permite trabajar con tokens a través de USB. Se recomienda usar esta opción solo cuando existe un problema de compatibilidad de hardware y solo para los equipos en los cuales se produce el problema.

## 12. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la [ventana principal de la aplicación](#).

Si los discos duros del sistema están cifrados, el Agente de autenticación se carga antes del inicio del sistema operativo. Utilice el Agente de autenticación para completar la autenticación con el fin de obtener acceso a los discos duros cifrados del sistema y cargar el sistema operativo. Después de que se completa correctamente el procedimiento de autenticación, se carga el sistema operativo. Se repite el proceso de autenticación cada vez que el sistema operativo se reinicia.

## Creación de una lista de discos duros excluidos del cifrado

Puede crear una lista de exclusiones de cifrado solo para la tecnología Cifrado de disco de Kaspersky.

*Para crear una lista de discos duros excluidos del cifrado:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de disco completo**.
6. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de disco de Kaspersky**.

Las entradas que corresponden a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**. Esta tabla estará vacía si no ha creado previamente una lista de discos duros que se deben excluir del cifrado.

7. Para añadir discos duros a la lista de discos duros excluidos del cifrado:

- a. Haga clic en el botón **Añadir**.
- b. En la ventana que se abre, edite las configuraciones de **Nombre del dispositivo**, **Nombre del equipo**, **Tipo de disco**, **Cifrado de disco de Kaspersky**.
- c. Haga clic en el botón **Actualizar**.

d. En la columna **Nombre**, seleccione las casillas de verificación en las filas de la tabla que corresponden a los discos duros que desea añadir a la lista de discos duros excluidos del cifrado.

e. Haga clic en **Aceptar**.

Los discos duros seleccionados aparecen en la tabla **No cifrar los siguientes discos duros**.

8. Guarde los cambios.

## Exportar e importar una lista de discos duros excluidos del cifrado

Puede exportar la lista de exclusiones de cifrado del disco duro a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de exclusiones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar las exclusiones a un servidor diferente.

[Cómo exportar e importar una lista de exclusiones de cifrado del disco duro en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de disco completo**.
6. En la lista desplegable **Tecnología de cifrado**, seleccione **Cifrado de disco de Kaspersky**.  
Las entradas que corresponden a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**.
7. 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 enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
8. Para importar la lista de reglas:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
9. Guarde los cambios.

[Cómo exportar e importar una lista de exclusiones de cifrado del disco duro en Web Console.](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** y siga el enlace para ajustar la configuración.  
Se abre la configuración de cifrado.
6. Haga clic en el enlace **Exclusiones**.
7. Para exportar la lista de reglas:
  - a. Seleccione las exclusiones que desea exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las exclusiones seleccionadas o exportar la lista completa de exclusiones.
  - d. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de exclusiones y seleccione la carpeta en la que desee guardar este archivo.
  - e. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista completa de exclusiones al archivo XML.
8. Para importar la lista de reglas:
  - a. Haga clic en el botón **Importar**.
  - b. En la ventana que se abre, seleccione el archivo XML del que importar la lista de exclusiones.
  - c. Abra el archivo.  
Si el equipo ya tiene una lista de exclusiones, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
9. Guarde los cambios.

## Activación de la tecnología de inicio de sesión único (SSO)

La tecnología de inicio de sesión único (SSO) le permite iniciar sesión automáticamente en el sistema operativo utilizando las credenciales del Agente de autenticación.

Cuando se utiliza la tecnología de inicio de sesión único, el Agente de autenticación ignora los requisitos de seguridad de la contraseña especificados en Kaspersky Security Center. Puede definir los requisitos de seguridad de la contraseña en la configuración del sistema operativo.

La tecnología de inicio de sesión único es incompatible con proveedores externos de credenciales de cuentas.

### Cómo activar el uso de la tecnología de inicio de sesión único en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Configuración común de cifrado**.
6. En el bloque **Configuración de contraseña**, haga clic en el botón **Configuración**.
7. En la ventana que se abre, en la pestaña **Agente de autenticación**, seleccione la casilla de verificación **Utilizar la tecnología de inicio de sesión único (SSO)**.
8. Guarde los cambios.

Como resultado, el usuario necesita completar el procedimiento de autenticación solo una vez con el Agente. El procedimiento de autenticación no es necesario para cargar el sistema operativo. El sistema operativo se carga automáticamente.

### Cómo activar el uso del inicio de sesión único en Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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** y siga el enlace para ajustar la configuración.  
Se abre la configuración de cifrado.
6. En la sección **Configuración de contraseña**, seleccione la casilla de verificación **Utilizar la tecnología de inicio de sesión único (SSO)**.
7. Guarde los cambios.

Como resultado, el usuario necesita completar el procedimiento de autenticación solo una vez con el Agente. El procedimiento de autenticación no es necesario para cargar el sistema operativo. El sistema operativo se carga automáticamente.

Para que funcione el inicio de sesión único, la contraseña de la cuenta de Windows y la contraseña de la cuenta del Agente de autenticación deben coincidir. Si las contraseñas no coinciden, el usuario tiene que realizar el procedimiento de autenticación dos veces: en la interfaz del Agente de autenticación y antes de cargar el sistema operativo. Después de eso, Kaspersky Endpoint Security reemplaza la contraseña de la cuenta del Agente de autenticación con la de la cuenta de Windows.

## Administración de cuentas del Agente de autenticación

Se necesita un Agente de autenticación para trabajar con unidades protegidas con la tecnología Cifrado de disco de Kaspersky (FDE). Antes de que se cargue el sistema operativo, el usuario debe completar la autenticación con el Agente. La tarea *Administrar cuentas del Agente de autenticación* está diseñada para configurar los ajustes de autenticación del usuario. Puede usar tareas locales para equipos particulares, así como tareas de grupo para equipos de grupos de administración independientes o una selección de equipos.

No puede configurar una planificación para iniciar la tarea *Administrar cuentas del Agente de autenticación*. También es imposible detener una tarea por la fuerza.

[Cómo crear la tarea \*Administrar cuentas del Agente de autenticación\* en la Consola de administración \(MMC\)](#) 

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)** → **Administrar cuentas del Agente de autenticación**.

### Paso 2. Seleccionar un comando de administración de cuentas del Agente de autenticación

Genere una lista de comandos de administración de cuentas del Agente de autenticación. Los comandos de administración le permiten añadir, modificar y eliminar cuentas del Agente de autenticación (consulte las instrucciones más abajo). Solo los usuarios que tienen una cuenta de Agente de autenticación pueden completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

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

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

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

### Paso 4. Definir el nombre de la tarea

Introduzca un nombre para la tarea, por ejemplo, *Cuentas de administrador*.

### Paso 5. Conclusión de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el nuevo usuario puede completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.



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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

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

### Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

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 la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

### Paso 2. Administración de cuentas del Agente de autenticación

Genere una lista de comandos de administración de cuentas del Agente de autenticación. Los comandos de administración le permiten añadir, modificar y eliminar cuentas del Agente de autenticación (consulte las instrucciones más abajo). Solo los usuarios que tienen una cuenta de Agente de autenticación pueden completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

### Paso 3. Conclusión de la creación de tareas

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, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el nuevo usuario puede completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Para añadir una cuenta del Agente de autenticación, debe añadir un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Es conveniente utilizar una tarea de grupo, por ejemplo, para añadir una cuenta de administrador a todos los equipos.

Kaspersky Endpoint Security le permite crear automáticamente cuentas de Agente de autenticación antes de cifrar una unidad. Puede activar la creación automática de cuentas del Agente de autenticación en la [configuración de la directiva de cifrado de disco completo](#). También puede [utilizar la tecnología de inicio de sesión único \(SSO\)](#).

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de tarea, seleccione la sección **Configuración**.
3. Haga clic en **Añadir** → **Comando de adición de cuentas**.
4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows que se utilizará para crear la cuenta del Agente de autenticación.
5. Si ha introducido el nombre de una cuenta de Windows manualmente, haga clic en el botón **Autorizar** para definir el identificador de seguridad de la cuenta (SID).  
Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Autorizar**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

Es necesario definir un identificador de seguridad de la cuenta de Windows para verificar que el nombre de la cuenta de Windows se ha introducido correctamente. Si la cuenta de Windows introducida no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con error.

6. Marque la casilla **Reemplazar una cuenta existente** si desea que la cuenta del Agente de autenticación que se ha creado previamente y se reemplace por la cuenta que se está creando.

Este paso está disponible cuando añade un comando de creación de cuentas del Agente de autenticación en las propiedades de una tarea de grupo para administrar las cuentas del Agente de autenticación. Este paso no está disponible cuando añade un comando de creación de cuentas del Agente de autenticación en las propiedades de la tarea local de *Administrar cuentas del Agente de autenticación*.

7. En el campo **Nombre de usuario**, introduzca el nombre de la cuenta del Agente de autenticación que debe introducirse durante el proceso de autenticación para acceder los discos duros cifrados.
8. Seleccione la casilla de verificación **Autorizar la autenticación basada en contraseña** si desea que la aplicación solicite al usuario que introduzca la contraseña de la cuenta del Agente de autenticación durante la autenticación para acceder a los discos duros cifrados. Introduzca una contraseña para la cuenta del Agente de autenticación. Si es necesario, puede solicitar una nueva contraseña del usuario después de la primera autenticación.
9. Seleccione la casilla de verificación **Autorizar la autenticación basada en certificado** si desea que la aplicación solicite al usuario que se conecte a un token o a tarjeta inteligente conectada al equipo durante la autenticación para acceder a los discos duros cifrados. Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token.
10. En el campo **Descripción de comando**, introduzca la información de la cuenta del Agente de autenticación necesaria para administrar el comando.
11. En **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.

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

Se abre la lista de tareas.

2. Haga clic en la tarea **Administrar cuentas del Agente de autenticación** de Kaspersky Endpoint Security.

Se abre la ventana 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 **Añadir**.

Esto inicia el Asistente de administración de cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Añadir**.

6. Seleccione una cuenta de usuario. Puede seleccionar una cuenta de la lista de cuentas de dominio o introducir manualmente el nombre de la cuenta. Ir al paso siguiente.

Kaspersky Endpoint Security determina el identificador de seguridad de la cuenta (SID). Esto es necesario para verificar la cuenta. Si ha introducido el nombre de usuario de manera incorrecta, Kaspersky Endpoint Security finalizará la tarea con un error.

7. Configure los ajustes de la cuenta del Agente de autenticación.

- **Crear una nueva cuenta del Agente de autenticación para reemplazar la cuenta existente.** Kaspersky Endpoint Security analiza las cuentas existentes en el equipo. Si el ID de seguridad del usuario en el equipo y en la tarea coinciden, Kaspersky Endpoint Security cambiará la configuración de la cuenta de usuario de acuerdo con la tarea.
- **Nombre de usuario.** El nombre de usuario predeterminado de la cuenta del Agente de autenticación corresponde al nombre de dominio del usuario.
- **Autorizar la autenticación basada en contraseña.** Introduzca una contraseña para la cuenta del Agente de autenticación. Si es necesario, puede solicitar una nueva contraseña del usuario después de la primera autenticación. De esta manera, cada usuario tendrá su propia contraseña única. También puede establecer los requisitos de seguridad de la contraseña para la cuenta del Agente de autenticación en la directiva.
- **Autorizar la autenticación basada en certificado** Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token. De esta manera, el usuario deberá introducir la contraseña de la tarjeta inteligente o token.
- **Acceso de cuenta a datos cifrados.** Configure el acceso de usuario a la unidad cifrada. Por ejemplo, puede desactivar temporalmente la autenticación de usuario en lugar de eliminar la cuenta del Agente de autenticación.
- **Comentario.** Introduzca una descripción de la cuenta, si es necesario.

8. Guarde los cambios.

9. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el nuevo usuario puede completar el procedimiento de autenticación, cargar el sistema operativo y obtener acceso a la unidad cifrada.

Para cambiar la contraseña y otros ajustes de la cuenta del Agente de autenticación, debe añadir un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Es conveniente utilizar una tarea de grupo, por ejemplo, para reemplazar el certificado del token de administrador en todos los equipos.

[Cómo cambiar la cuenta del Agente de autenticación mediante la Consola de administración \(MMC\)](#) 

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de tarea, seleccione la sección **Configuración**.
3. Haga clic en **Añadir** → **Comando de modificación de cuentas**.
4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows que quiere modificar.
5. Si ha introducido el nombre de una cuenta de Windows manualmente, haga clic en el botón **Autorizar** para definir el identificador de seguridad de la cuenta (SID).  
Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Autorizar**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

Es necesario definir un identificador de seguridad de la cuenta de Windows para verificar que el nombre de la cuenta de Windows se ha introducido correctamente. Si la cuenta de Windows introducida no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con error.

6. Active la casilla de verificación **Cambiar el nombre de usuario** e introduzca un nombre de cuenta del Agente de autenticación nuevo si desea que Kaspersky Endpoint Security sustituya el nombre de usuario de todas las cuentas del Agente de autenticación que se hayan creado en función de la cuenta de Microsoft Windows que lleva el nombre que se indica en el campo **Cuenta de Windows** por el nombre introducido en el siguiente campo.
7. Seleccione la casilla de verificación **Modificar la configuración de la autenticación basada en contraseña** para poder editar los ajustes de autenticación basada en contraseña.
8. Seleccione la casilla de verificación **Autorizar la autenticación basada en contraseña** si desea que la aplicación solicite al usuario que introduzca la contraseña de la cuenta del Agente de autenticación durante la autenticación para acceder a los discos duros cifrados. Introduzca una contraseña para la cuenta del Agente de autenticación.
9. Seleccione la casilla de verificación **Editar la regla de cambio de contraseña en la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security sustituya por el siguiente valor el valor del parámetro de cambio de contraseña de todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows que lleva el nombre indicado en el campo **Cuenta de Windows**.
10. Especifique el valor del parámetro de cambio de contraseña al autenticarse en el Agente de autenticación.
11. Seleccione la casilla de verificación **Modificar la configuración de la autenticación basada en certificado** para hacer editable la configuración de la autenticación en función del certificado electrónico de un token o una tarjeta inteligente.
12. Seleccione la casilla de verificación **Autorizar la autenticación basada en certificado** si desea que la aplicación solicite al usuario la introducción de la contraseña al token o a la tarjeta inteligente conectada al equipo durante el proceso de autenticación para acceder a los discos duros cifrados. Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token.
13. Seleccione la casilla de verificación **Modificar la descripción del comando** y modifique la descripción de los comandos si desea que Kaspersky Endpoint Security cambie la descripción de los comandos de todas las cuentas del Agente de autenticación que se hayan creado con la cuenta de Microsoft Windows que lleva el nombre que se indica en el campo **Cuenta de Windows**.

14. Seleccione la casilla de verificación **Editar la regla de acceso a la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie la regla de acceso del usuario a la autenticación en el Agente de autenticación por el valor especificado más abajo para todas las cuentas del Agente de autenticación creadas con la cuenta de Microsoft Windows que lleva el nombre indicado en el campo **Cuenta de Windows**.
15. Especifique la regla para acceder al diálogo de autenticación en el Agente de autenticación.
16. Guarde los cambios.

### [Cómo cambiar la cuenta del Agente de autenticación mediante Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea **Administrar cuentas del Agente de autenticación** de Kaspersky Endpoint Security.  
Se abre la ventana 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 **Añadir**.  
Esto inicia el Asistente de administración de cuentas del Agente de autenticación.
5. Seleccione el tipo de comando **Cambiar**.
6. Seleccione una cuenta de usuario. Puede seleccionar una cuenta de la lista de cuentas de dominio o introducir manualmente el nombre de la cuenta. Ir al paso siguiente.  
Kaspersky Endpoint Security determina el identificador de seguridad de la cuenta (SID). Esto es necesario para verificar la cuenta. Si ha introducido el nombre de usuario de manera incorrecta, Kaspersky Endpoint Security finalizará la tarea con un error.
7. Seleccione las casillas de verificación que hay junto a la configuración que desea editar.
8. Configure los ajustes de la cuenta del Agente de autenticación.
  - **Crear una nueva cuenta del Agente de autenticación para reemplazar la cuenta existente.**  
Kaspersky Endpoint Security analiza las cuentas existentes en el equipo. Si el ID de seguridad del usuario en el equipo y en la tarea coinciden, Kaspersky Endpoint Security cambiará la configuración de la cuenta de usuario de acuerdo con la tarea.
  - **Nombre de usuario.** El nombre de usuario predeterminado de la cuenta del Agente de autenticación corresponde al nombre de dominio del usuario.
  - **Autorizar la autenticación basada en contraseña.** Introduzca una contraseña para la cuenta del Agente de autenticación. Si es necesario, puede solicitar una nueva contraseña del usuario después de la primera autenticación. De esta manera, cada usuario tendrá su propia contraseña única. También puede establecer los requisitos de seguridad de la contraseña para la cuenta del Agente de autenticación en la directiva.
  - **Autorizar la autenticación basada en certificado** Seleccione un archivo de certificado para la autenticación con una tarjeta inteligente o token. De esta manera, el usuario deberá introducir la contraseña de la tarjeta inteligente o token.
  - **Acceso de cuenta a datos cifrados.** Configure el acceso de usuario a la unidad cifrada. Por ejemplo, puede desactivar temporalmente la autenticación de usuario en lugar de eliminar la cuenta del Agente de autenticación.
  - **Comentario.** Introduzca una descripción de la cuenta, si es necesario.
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, debe añadir un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Es conveniente utilizar una tarea de grupo, por ejemplo, para eliminar la cuenta de un trabajador despedido.

### [Cómo eliminar una cuenta del Agente de autenticación mediante la Consola de administración \(MMC\)](#)

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de tarea, seleccione la sección **Configuración**.
3. Haga clic en **Añadir** → **Comando de eliminación de cuentas**.
4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de usuario de Windows que se utilizó para crear la cuenta del Agente de autenticación que quiere eliminar.
5. Si ha introducido el nombre de una cuenta de Windows manualmente, haga clic en el botón **Autorizar** para definir el identificador de seguridad de la cuenta (SID).  
Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Autorizar**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

Es necesario definir un identificador de seguridad de la cuenta de Windows para verificar que el nombre de la cuenta de Windows se ha introducido correctamente. Si la cuenta de Windows introducida no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con error.

6. Guarde los cambios.

### [Cómo eliminar una cuenta del Agente de autenticación mediante Web Console](#)



1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en la tarea **Administrar cuentas del Agente de autenticación** de Kaspersky Endpoint Security.  
Se abre la ventana 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 **Añadir**.  
Esto inicia el Asistente de administración de cuentas del Agente de autenticación.
5. Seleccione el tipo de comando **Eliminar**.
6. Seleccione una cuenta de usuario. Puede seleccionar una cuenta de la lista de cuentas de dominio o introducir manualmente el nombre de la cuenta.
7. Guarde los cambios.
8. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Como resultado, una vez que la tarea se ha completado al iniciar el equipo la siguiente vez, el usuario no podrá completar el procedimiento de autenticación ni cargar el sistema operativo. Kaspersky Endpoint Security denegará el acceso a los datos cifrados.

Para ver la lista de usuarios que pueden completar la autenticación con el Agente y cargar el sistema operativo, tiene que acceder a las propiedades del equipo administrado.

### [Cómo ver la lista de cuentas del Agente de autenticación mediante la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Haga doble clic para abrir la ventana de propiedades del equipo.
5. En la ventana de propiedades del equipo, seleccione la sección **Tareas**.  
Se abre la lista de tareas locales.
6. Seleccione la tarea **Administrar cuentas del Agente de autenticación**.
7. En las propiedades de tarea, seleccione la sección **Configuración**.

Como resultado, podrá acceder a una lista de las cuentas del Agente de autenticación en este equipo. Solo los usuarios de la lista pueden completar la autenticación con el Agente y cargar el sistema operativo.

### [Cómo ver una lista de cuentas del Agente de autenticación mediante Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del equipo en el que desea ver la lista de cuentas del Agente de autenticación.  
Se abren las propiedades del equipo.
3. En la ventana de propiedades del equipo, seleccione la sección **Tareas**.  
Se abre la lista de tareas locales.
4. Seleccione la tarea **Administrar cuentas del Agente de autenticación**.
5. En las propiedades del equipo, seleccione la pestaña **Configuración de la aplicación**.

Como resultado, podrá acceder a una lista de las cuentas del Agente de autenticación en este equipo. Solo los usuarios de la lista pueden completar la autenticación con el Agente y cargar el sistema operativo.

## Utilizar una tarjeta inteligente y un token con el Agente de autenticación

Se puede utilizar una tarjeta inteligente o token para la autenticación cuando se accede a discos duros cifrados. Para ello, debe añadir el archivo del certificado electrónico de una tarjeta inteligente o token a la tarea *Administrar cuentas del Agente de autenticación*.

El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, no se podrá añadir el archivo del certificado electrónico al comando.

Kaspersky Endpoint Security admite los tókenes, los lectores de tarjeta inteligente y las tarjetas inteligentes siguientes:

- SafeNet eToken PRO 64 K (4.2b);
- SafeNet eToken PRO 72 K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;

- Athena IDProtect Laser;
- SafeNet eToken PRO 72 K Java;
- Aladdin-RD JaCarta PKI.

Para añadir el archivo de un certificado electrónico de token o tarjeta inteligente al comando con el fin de crear una cuenta del agente de autenticación, debe guardar primero el archivo usando el software de terceros para gestionar certificados.

El certificado del token o tarjeta inteligente tiene que tener las propiedades siguientes:

- El certificado debe cumplir con el estándar X.509 y el archivo de certificado tiene que tener codificación DER.
- El certificado contiene una clave RSA con una longitud de al menos 1024 bits.

Si el certificado electrónico del token o de la tarjeta electrónica no cumple con este requisito, no podrá cargar el archivo de certificado en el comando para crear una cuenta del Agente de autenticación.

El parámetro KeyUsage del certificado tiene que tener el valor keyEncipherment o dataEncipherment. El parámetro KeyUsage determina el propósito del certificado. Si el parámetro tiene un valor diferente, Kaspersky Security Center descargará el archivo del certificado pero mostrará una advertencia.

Si un usuario ha perdido un token o una tarjeta inteligente, el administrador debe añadir el archivo del certificado electrónico del token o la tarjeta inteligente al comando para crear una cuenta del Agente de autenticación. Luego, el usuario debe completar el procedimiento para [obtener acceso a los dispositivos cifrados o restaurar datos de dispositivos cifrados](#).

## Descifrado de discos duros

Puede descifrar discos duros aun si no hay licencia activa que permita el cifrado de datos.

*Para descifrar discos duros:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de disco completo**.
6. En la lista desplegable **Tecnología de cifrado**, seleccione la tecnología con la que se cifraron los discos duros.
7. Realice una de las siguientes acciones:
  - En la lista desplegable **Modo de cifrado**, seleccione la opción **Descifrar todos los discos duros** para descifrar todos los discos duros cifrados.
  - Añada los discos duros cifrados que desea descifrar a la tabla **No cifrar los siguientes discos duros**.

Esta opción solo está disponible para la tecnología Cifrado de disco de Kaspersky.

## 8. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la [ventana principal de la aplicación](#).

Si el usuario apaga o reinicia el equipo durante el descifrado de discos duros que fueron cifrados mediante tecnología de cifrado de disco de Kaspersky, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el descifrado del disco duro después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo cambia al modo de hibernación mientras se descifran discos duros que fueron cifrados mediante la tecnología de cifrado de disco de Kaspersky, el Agente de autenticación se carga cuando el sistema operativo sale del modo de hibernación. Kaspersky Endpoint Security reanuda el descifrado del disco duro después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo. Después de descifrar el disco duro, no se encontrará disponible el modo de hibernación hasta que se realice un primer reinicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el descifrado del disco duro, Kaspersky Endpoint Security reanudará el descifrado del disco duro cuando el sistema operativo salga del modo de hibernación sin cargar el Agente de autenticación.

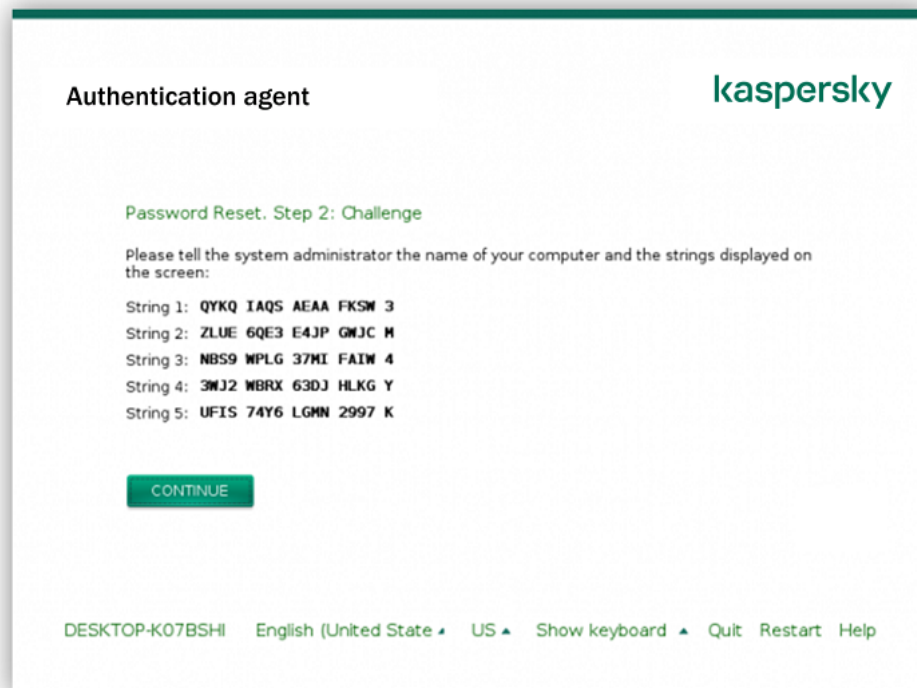
## Restauración del acceso a una unidad protegida por la tecnología Cifrado de disco de Kaspersky

Si un usuario ha olvidado la contraseña para acceder a un disco duro protegido por la tecnología Cifrado de disco de Kaspersky, tiene que iniciar el procedimiento de recuperación (solicitud-respuesta).

### Restauración del acceso al disco duro del sistema

La restauración del acceso a un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky consta de los siguientes pasos:

1. El usuario proporciona los bloques de solicitud al administrador (vea la imagen más abajo).
2. El administrador introduce los bloques de solicitud en Kaspersky Security Center, recibe los bloques de respuesta y proporciona los bloques de respuesta al usuario.
3. El usuario introduce los bloques de respuesta en la interfaz del Agente de autenticación y obtiene acceso al disco duro.



Restauración del acceso a un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky

Para comenzar el procedimiento de recuperación, el usuario tiene que hacer clic en el botón **Forgot your password** en la interfaz del Agente de autenticación.

[Cómo obtener bloques de respuesta para un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky en la Consola de administración \(MMC\)](#) <sup>2</sup>

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
6. En la ventana de diálogo que se abre, seleccione la pestaña **Agente de autenticación**.
7. En la sección **Algoritmo de cifrado en uso**, seleccione un algoritmo de cifrado: **AES56** o **AES256**.

El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: están disponibles tanto la variante de *cifrado "fuerte"* (**AES256**) como la de *cifrado "ligero"* (**AES56**). La biblioteca de cifrado AES se instala junto con la aplicación.

8. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación del usuario que solicitó la recuperación del acceso a la unidad.
9. En la lista desplegable **Disco duro**, seleccione el disco duro cifrado para el cual debe recuperar el acceso.
10. En la sección **Solicitudes de los usuarios**, introduzca los bloques de solicitud que ha establecido el usuario.

Como resultado, el contenido de los bloques de la respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de la cuenta del Agente de autenticación se mostrará en el campo **Clave de acceso**. Transmita el contenido de los bloques de respuesta al usuario.

### [Cómo obtener bloques de respuesta para un disco duro del sistema protegido por la tecnología Cifrado de disco de Kaspersky en Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuya unidad quiere restaurar el acceso.
3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione la sección **Agente de autenticación**.
5. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación creada para el usuario que está solicitando la recuperación del nombre y la contraseña de la cuenta del Agente de autenticación.
6. Introduzca los bloques de solicitud transmitidos por el usuario.

El contenido de las secciones de la respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de la cuenta del Agente de autenticación se mostrará en la parte inferior de la ventana. Transmita el contenido de los bloques de respuesta al usuario.

Tras completar el procedimiento de recuperación, el Agente de autenticación solicitará al usuario que cambie la contraseña.

## Restauración del acceso a un disco duro que no pertenece al sistema

La restauración del acceso a un disco duro que no pertenece al sistema protegido por la tecnología Cifrado de disco de Kaspersky consta de los siguientes pasos:

1. El usuario envía un archivo de solicitud de acceso al administrador.
2. El administrador añade el archivo de solicitud de acceso a Kaspersky Security Center, crea un archivo clave de acceso y lo envía al usuario.
3. El usuario añade el archivo clave de acceso a Kaspersky Endpoint Security y obtiene acceso al disco duro.

Para comenzar el procedimiento de recuperación, el usuario tiene que intentar acceder a un disco duro. Como resultado, Kaspersky Endpoint Security creará un archivo de solicitud de acceso (un archivo con la extensión KESDC), que el usuario tiene que enviar al administrador, por ejemplo, por correo electrónico.

### [Cómo obtener un archivo clave de acceso para un disco duro cifrado que no pertenece al sistema en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
6. En la ventana de diálogo que se abre, seleccione la pestaña **Cifrado de datos**.
7. En la pestaña **Cifrado de datos**, haga clic en el botón **Examinar**.
8. En la ventana para seleccionar un archivo de solicitud de acceso, especifique la ruta al archivo recibido del usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.

### [Cómo obtener un archivo clave de acceso a un disco duro cifrado que no pertenece al sistema en Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
  2. Seleccione la casilla de verificación junto al nombre del equipo a cuyos datos quiere restaurar el acceso.
  3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.
  4. Seleccione la sección **Cifrado de datos**.
  5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión KESDC).  
Web Console mostrará información sobre la solicitud. Esto incluirá el nombre del equipo en el que el usuario solicita acceso al archivo.
  6. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión KESDR).
- Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

## 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 el equipo no podrá utilizarse.

Para más información sobre la actualización segura del sistema operativo, visite la [Base de conocimientos del Soporte técnico](#)<sup>2</sup>.

La actualización automática del sistema operativo está disponible en las siguientes condiciones:

1. La actualización del sistema operativo se realiza a través de WSUS (Windows Server Update Services).
2. El equipo tiene instalado Windows 10 versión 1607 (RS1) o posterior.
3. La versión de Kaspersky Endpoint Security instalada en el equipo debe ser la 11.2.0 o posterior.

Si se cumplen todas las condiciones, puede actualizar el sistema operativo de la forma habitual.

Si está utilizando la tecnología de Cifrado de disco de Kaspersky (FDE) y Kaspersky Endpoint Security para Windows versión 11.1.0 o 11.1.1 está instalado en el equipo, no necesita descifrar los discos duros para actualizar Windows 10.

Para actualizar el sistema operativo, debe hacer lo siguiente:



1. Antes de actualizar el sistema, copie los controladores denominados cm\_km.inf, cm\_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf y klfdefsf.sys en una carpeta local. Por ejemplo, C:\fde\_drivers.
2. Ejecute la instalación de la actualización del sistema con el modificador `/ReflectDrivers` y especifique la carpeta que contiene los controladores guardados:  
`setup.exe/ReflectDrivers C:\fde_drivers`

Cuando se utiliza la tecnología de cifrado de unidad BitLocker, no es necesario descifrar los discos duros para actualizar Windows 10. Para obtener más información sobre BitLocker, visite el [sitio web de Microsoft](#).

## Eliminación de errores al actualizar la función de cifrado

El Cifrado de disco completo se actualiza cuando la versión anterior de la aplicación se actualiza a Kaspersky Endpoint Security para Windows 11.8.0.

Al iniciar la actualización de la función Cifrado de disco completo, pueden ocurrir los siguientes errores:

- No se puede iniciar la actualización.
- El dispositivo no es compatible con el Agente de autenticación.

*Para eliminar los errores que ocurrieron al iniciar el proceso de actualización de la función Cifrado de disco completo en la nueva versión de la aplicación es necesario:*

1. [Descifrar los discos duros](#).
2. [Cifrar los discos duros](#) de nuevo.

Durante la actualización de la función Cifrado de disco completo pueden ocurrir los siguientes errores:

- No se puede completar la actualización.
- La reversión de la actualización de Cifrado de disco completo se ha completado con un error.

*Para eliminar los errores que ocurrieron durante el proceso de actualización de la función Cifrado de disco completo,*

[restaure el acceso a dispositivos cifrados con la Utilidad de Restauración](#).

## Seleccionar el nivel de rastreo del Agente de autenticación

La aplicación registra información de servicio sobre el funcionamiento del Agente de autenticación e información sobre las operaciones de usuario con el Agente de autenticación en el archivo de seguimiento.

*Para seleccionar el nivel de seguimiento del Agente de autenticación:*

1. En cuanto se inicie un equipo con discos duros cifrados, pulse el botón **F3** para llamar a una ventana y configurar los ajustes del Agente de autenticación.
2. Seleccione el nivel de seguimiento en la ventana de configuración del Agente de autenticación:
  - **Disable debug logging (default)**. Si esta opción se selecciona, la aplicación no registra la información de eventos del Agente de autenticación en el archivo de seguimiento.

- **Enable debug logging.** Si se selecciona esta opción, la aplicación registra información sobre el funcionamiento del agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento.
- **Enable verbose logging.** Si se selecciona esta opción, la aplicación registra información detallada sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento.

El nivel de detalle de las entradas de esta opción es superior en comparación con el nivel de la opción **Enable debug logging**. Un nivel elevado de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.

- **Enable debug logging and select serial port.** Si se selecciona esta opción, la aplicación registra información sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento y las transmite a través del puerto COM.  
Si un equipo con discos duros cifrados está conectado a otro equipo a través del puerto COM, los eventos del Agente de autenticación se pueden examinar desde este otro equipo.
- **Enable verbose debug logging and select serial port.** Si se selecciona esta opción, la aplicación incluye entradas detalladas sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de seguimiento, y las transmite a través del puerto COM.

El nivel de detalle de las entradas de esta opción es superior en comparación con el nivel de la opción **Enable debug logging and select serial port**. Un nivel elevado de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.

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.

El archivo de seguimiento del Agente de autenticación no se envía a Kaspersky a diferencia de otros archivos de seguimiento de la aplicación. Si fuera necesario, puede enviar manualmente el archivo de seguimiento del Agente de autenticación a Kaspersky para su análisis.

## Editar los textos de ayuda del Agente de autenticación

Antes de modificar los mensajes de ayuda del Agente de autenticación, revise la lista de caracteres que pueden usarse en un entorno de prearranque (ver más abajo).

*Para editar los mensajes de ayuda del Agente de autenticación:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Configuración común de cifrado**.

6. En el bloque **Plantillas**, haga clic en el botón **Ayuda**.

7. En la ventana abierta, haga lo siguiente:

- Seleccione la pestaña **Autenticación** para editar el texto de ayuda que se muestra en la ventana Agente de autenticación cuando se introducen las credenciales de la cuenta.
- Seleccione la pestaña **Cambiar la contraseña** para editar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se cambia la contraseña de la cuenta del Agente de autenticación.
- Seleccione la pestaña **Recuperar la contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se recupera la contraseña de la cuenta del Agente de autenticación.

8. Modifique los mensajes de la ayuda.

Si quiere restaurar el texto original, haga clic en el botón **Predeterminado**.

Puede introducir texto de ayuda que contenga 16 líneas o menos. La longitud máxima de línea es 64 caracteres.

9. Guarde los cambios.

## Compatibilidad limitada con los caracteres de los mensajes de ayuda del Agente de autenticación

En un entorno anterior al arranque, se admiten los siguientes caracteres de Unicode:

- Alfabeto latino básico (0000 - 007F)
- Caracteres de Latino-1 adicionales (0080 - 00FF)
- Latino-A ampliado (0100 - 017F)
- Latino-A ampliado (0180 - 024F)
- Caracteres de ID ampliados no combinados (02B0 - 02FF)
- Marcas diacríticas combinadas (0300 - 036F)
- Alfabetos griego y copto (0370 - 03FF)
- Alfabeto cirílico (0400 - 04FF)
- Hebreo (0590 - 05FF)
- Script árabe (0600 - 06FF)
- Latino ampliado adicional (1E00 - 1EFF)
- Signos de puntuación (2000 - 206F)
- Símbolos de divisa (20A0 - 20CF)

- Símbolos parecidos a una letra (2100 - 214F)
- Cifras geométricas (25A0 - 25FF)
- Formularios de presentación de alfabeto árabe B (FE70 - FEFF)

Los caracteres que no se especifican en esta lista no se admiten en un entorno anterior al arranque. No se recomienda usar tales caracteres en mensajes de ayuda del Agente de autenticación.

## Eliminar los objetos y datos restantes después de probar el Agente de autenticación

Durante la desinstalación de la aplicación, si Kaspersky Endpoint Security detecta objetos y datos que permanecieron en el disco duro del sistema después de la operación de prueba del Agente de autenticación, la desinstalación de aplicación se interrumpe y se hace imposible hasta que esos objetos y datos se eliminan.

Solamente en casos excepcionales, los objetos y los datos pueden permanecer en el disco duro del sistema después de la operación de prueba del Agente de autenticación. Por ejemplo, esto puede suceder si el equipo no se ha reiniciado después de que se aplicara una directiva de Kaspersky Security Center con configuración de cifrado o la aplicación no puede iniciarse después de la operación de prueba del Agente de autenticación.

Puede quitar objetos y datos restantes en el disco duro del sistema después de una operación de prueba del Agente de autenticación de varias maneras:

- Mediante la directiva de Kaspersky Security Center.
- [mediante Utilidad de restauración](#).

*Para utilizar una directiva de Kaspersky Security Center con el fin de eliminar objetos y datos que permanecieron después de la operación de prueba del Agente de autenticación:*

1. Aplique al equipo una directiva de Kaspersky Security Center con la configuración definida para [descifrar](#) todos los discos duros del equipo.
2. Inicie Kaspersky Endpoint Security.

*Para eliminar la información sobre la incompatibilidad de la aplicación con Agente de autenticación,*

escriba el comando `avp pbatestreset` en la línea de comandos.

## Administración de BitLocker

*BitLocker* es una tecnología de cifrado integrada en los sistemas operativos Windows. Kaspersky Endpoint Security le permite controlar y gestionar BitLocker utilizando Kaspersky Security Center. BitLocker cifra los volúmenes lógicos. BitLocker no se puede utilizar para el cifrado de unidades extraíbles. Para obtener más detalles sobre BitLocker, consulte la [documentación de Microsoft](#).

BitLocker proporciona almacenamiento seguro de claves de acceso utilizando un módulo de plataforma segura. Un *módulo de plataforma segura (TPM)* es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del ordenador e interactúa con todos los otros componentes del sistema a través del bus de hardware. Utilizar el módulo TPM es el modo más seguro de almacenar las clave de acceso de BitLocker, ya que TPM proporciona verificación de integridad del sistema antes del inicio. Sigue pudiendo cifrar unidades en un equipo sin un módulo TPM. En este caso, la clave de acceso se cifrará con una contraseña. BitLocker utiliza los siguientes métodos de autenticación:

- TPM.
- TPM y PIN.
- Contraseña.

Después de cifrar una unidad, BitLocker crea una clave maestra. Kaspersky Endpoint Security envía la clave maestra a Kaspersky Security Center para que pueda [restaurar el acceso al disco](#), por ejemplo, si un usuario ha olvidado la contraseña.

Si un usuario cifra un disco con BitLocker, Kaspersky Endpoint Security enviará [información sobre el cifrado de disco a Kaspersky Security Center](#). Sin embargo, Kaspersky Endpoint Security no enviará la clave maestra a Kaspersky Security Center, por lo que será imposible restaurar el acceso al disco utilizando Kaspersky Security Center. Para que BitLocker funcione correctamente con Kaspersky Security Center, [descifre la unidad](#) y [vuelva a cifrarla](#) utilizando una directiva. Puede descifrar una unidad de manera local o usar una directiva.

Después de cifrar el disco duro del sistema, el usuario debe pasar por el procedimiento de autenticación de BitLocker para iniciar el sistema operativo. Después del procedimiento de autenticación, BitLocker permitirá que los usuarios inicien sesión. BitLocker no admite la tecnología Single Sign-On (SSO).

Si está utilizando directivas de grupo de Windows, desactive la administración de BitLocker en la configuración de directivas. La configuración de directivas de Windows puede entrar en conflicto con la configuración de directivas de Kaspersky Endpoint Security. Al cifrar una unidad, pueden producirse errores.

## Inicio del Cifrado de unidad BitLocker

Antes de comenzar el cifrado de disco completo, es aconsejable asegurarse de que el equipo no esté infectado. Para ello, ejecute la tarea Análisis completo o Análisis de áreas críticas. Cifrar un disco completo en un equipo infectado con un rootkit puede provocar que el equipo se inutilice.

Para usar el Cifrado de unidad BitLocker en equipos con sistemas operativos Windows para servidores, puede ser necesario instalar el componente Cifrado de unidad BitLocker. Instale el componente con las herramientas del sistema operativo (Asistente para añadir roles y componentes). Para obtener más información sobre cómo instalar el Cifrado de unidad BitLocker, consulte la [documentación de Microsoft](#).

### [Cómo ejecutar el Cifrado de unidad BitLocker mediante la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de disco completo**.
6. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **Cifrado de unidad BitLocker**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Cifrar todos los discos duros**.

Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo en el que se hizo el cifrado.

8. Configure las opciones avanzadas de Cifrado de unidad BitLocker (consulte la tabla a continuación).
9. Guarde los cambios.

### [Cómo ejecutar el Cifrado de unidad BitLocker mediante Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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. En el bloque **Control del cifrado**, seleccione **Cifrado de unidad BitLocker**.
6. Haga clic en el enlace **Cifrado de unidad BitLocker**.  
Se abrirá la ventana de configuración del Cifrado de unidad BitLocker.
7. En la lista desplegable **Modo de cifrado**, seleccione **Cifrar todos los discos duros**.

Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo en el que se hizo el cifrado.

8. Configure las opciones avanzadas de Cifrado de unidad BitLocker (consulte la tabla a continuación).
9. Guarde los cambios.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la [ventana principal de la aplicación](#).

Después de aplicar la directiva, la aplicación muestra las siguientes preguntas según la configuración de la autenticación:

- Solo TPM. No se requiere la acción del usuario. El disco se cifrará cuando se reinicie el ordenador.
- TPM + PIN/Contraseña. Si un módulo TPM está disponible, se abre una ventana para escribir el código PIN. Si un módulo TPM no está disponible, verá una ventana de contraseña para la autenticación previa al arranque.
- Solo contraseña. Verá una ventana de solicitud de contraseña para la autenticación previa al inicio.

Si el modo de compatibilidad con los Estándares federales de procesamiento de la información está habilitado para el sistema operativo del equipo, entonces en Windows 8 y versiones anteriores del sistema operativo se mostrará una solicitud para conectar un dispositivo de almacenamiento para guardar el archivo clave de recuperación. Puede guardar varios archivos de clave de recuperación en un solo dispositivo de almacenamiento.

Después de establecer una contraseña o un PIN, BitLocker le pedirá que reinicie su equipo para completar el cifrado. A continuación, el usuario debe pasar por el procedimiento de autenticación de BitLocker. Tras el procedimiento de autenticación, el usuario debe iniciar sesión en el sistema. Una vez que el sistema operativo se haya cargado, BitLocker completará el cifrado.

Si no hay acceso a claves de cifrado, el usuario puede [solicitar que el administrador de la red local le proporcione una clave de recuperación](#) (siempre que la clave de recuperación no se haya guardado anteriormente en el dispositivo USB o se haya perdido).

Configuración del componente Cifrado de unidad BitLocker

Parámetro	Descripción
<b>Activar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en tabletas</b>	<p>Esta casilla de verificación activa o desactiva el uso de la autenticación que requiere la entrada de datos en un entorno de prearranque, incluso si la plataforma no tiene la capacidad de entrada de prearranque (por ejemplo, con los teclados de la pantalla táctil de las tabletas).</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>La pantalla táctil de las tabletas no está disponible en el entorno de prearranque. Para completar la autenticación BitLocker en tabletas, el usuario debe conectar un teclado USB, por ejemplo.</p> </div> <p>Si selecciona, se permite el uso de la autenticación que requiere la entrada de prearranque en las tabletas. Se recomienda utilizar esta configuración solo en dispositivos con herramientas alternativas de entrada de datos en un entorno de prearranque, como un teclado USB, además de los teclados de la pantalla táctil.</p> <p>Si se desactiva, el Cifrado de unidad BitLocker no es posible en tabletas.</p>
<b>Utilizar cifrado de hardware (SO Windows 8 y versiones posteriores)</b>	<p>Si se selecciona, la aplicación utiliza el cifrado basado en hardware, lo que le permite aumentar la velocidad de cifrado y utilizar menos recursos del equipo.</p>
<b>Cifrar solo el espacio en disco utilizado (SO</b>	<p>Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado.</p>

**Windows 8 y versiones posteriores)**

Activar o desactivar la función **Cifrar solo el espacio en disco utilizado (SO Windows 8 y versiones posteriores)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado.

Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden.

Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente.

Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables.

Esta casilla de verificación está desactivada de forma predeterminada.

**Parámetros de autenticación**

**Usar contraseña (SO Windows 8 y versiones posteriores)**

Si se selecciona esta opción, Kaspersky Endpoint Security solicita una contraseña al usuario cada vez que este intenta acceder a la unidad cifrada.

Se puede seleccionar cuando el módulo de plataforma segura (TPM) no se está utilizando.

**Usar el módulo de plataforma segura (TPM)**

Si se selecciona esta opción, BitLocker utiliza el módulo de plataforma segura (TPM).

Un *módulo de plataforma segura (TPM)* es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del ordenador e interactúa con todos los otros componentes del sistema a través del bus de hardware.

En equipos con Windows 7 o Windows Server 2008 R2, solo es posible utilizar el cifrado con módulo TPM. El cifrado BitLocker no está disponible en equipos que no cuentan con este módulo. No es posible utilizar una contraseña en tales equipos.

Un dispositivo equipado con un módulo de plataforma segura puede crear claves de cifrado que solo con dicho dispositivo se pueden descifrar. El módulo de plataforma segura cifra las claves de cifrado con su propia clave raíz de almacenamiento. La clave raíz de almacenamiento se guarda en el módulo de plataforma segura, lo que proporciona un nivel adicional de protección contra los intentos de piratear las claves de cifrado.

Esta acción está seleccionada de forma predeterminada.

Puede establecer una capa de protección adicional para acceder a la clave de cifrado, y cifrar la clave con una contraseña o PIN:

- **Utilizar PIN para el TPM.** Si esta casilla de verificación está seleccionada, un usuario puede utilizar un código PIN para obtener acceso a una clave de cifrado almacenada en el módulo de plataforma segura (TPM). Si la casilla no está seleccionada, se prohíbe a los usuarios utilizar códigos PIN. Para acceder a la clave de cifrado, un usuario debe introducir la contraseña.



Puede permitir que el usuario utilice un PIN optimizado. El *PIN optimizado* permite utilizar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.

- **Usar el módulo de plataforma segura (TPM). Si no está disponible, use la contraseña.** Si se selecciona la casilla de verificación, el usuario podrá utilizar una contraseña para acceder a claves de cifrado cuando el módulo de plataforma segura (TPM) no esté disponible.

Si no se seleccionó la casilla de verificación y el módulo TPM no está disponible, no comenzará el cifrado de disco completo.

## Descifrado de un disco duro protegido por BitLocker

Los usuarios pueden descifrar un disco utilizando el sistema operativo (la función *Desactivar BitLocker*). Después de eso, Kaspersky Endpoint Security solicitará al usuario que vuelva a cifrar el disco. Kaspersky Endpoint Security solicitará el cifrado del disco, a menos que active el descifrado del disco en la directiva.

### [Cómo descifrar un disco duro protegido por BitLocker a través de la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de disco completo**.
6. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **Cifrado de unidad BitLocker**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Descifrar todos los discos duros**.
8. 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 **Dispositivos** → **Directivas y perfiles**.
2. 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 unidad BitLocker** y siga el enlace para ajustar la configuración.  
Se abre la configuración de cifrado.
6. En la lista desplegable **Modo de cifrado**, seleccione **Descifrar todos los discos duros**.
7. Haga clic en **Aceptar**.

Puede utilizar la herramienta Monitor de cifrado para controlar el proceso de cifrado o descifrado del disco en el equipo de un usuario. Puede ejecutar la herramienta Monitor de cifrado desde la [ventana principal de la aplicación](#).

## Restauración del acceso a una unidad protegida por BitLocker

Si un usuario ha olvidado la contraseña para acceder a un disco duro cifrado por BitLocker, tiene que iniciar el procedimiento de recuperación (solicitud-respuesta).

Si el sistema operativo del equipo tiene activado el modo de compatibilidad estándar de procesamiento de información federal (FIPS), entonces en Windows 8 y versiones anteriores, el archivo clave de recuperación se guarda en la unidad extraíble antes del cifrado. Para restaurar el acceso a la unidad, inserte la unidad extraíble y siga las instrucciones en pantalla.

La restauración del acceso a un disco duro cifrado por BitLocker consta de los siguientes pasos:

1. El usuario le dice al administrador el ID de la clave de recuperación (vea la imagen más abajo).
2. El administrador comprueba el ID de la clave de recuperación en las propiedades del equipo de Kaspersky Security Center. El ID que proporcionó el usuario debe coincidir con el ID que se muestra en las propiedades del equipo.
3. Si los ID de la clave de recuperación coinciden, el administrador proporciona al usuario la clave de recuperación o envía un archivo clave de recuperación.

Se utiliza un archivo clave de recuperación para los equipos que ejecutan los siguientes sistemas operativos:

- Windows 7;
- Windows 8;
- Windows Server 2008;
- Windows Server 2011;
- Windows Server 2012.

Para el resto de sistemas operativos, se utiliza una clave de recuperación.

4. El usuario introduce la clave de recuperación y obtiene acceso al disco duro.



Restauración del acceso a un disco duro cifrado por BitLocker

## Restauración del acceso a un disco duro

Para comenzar el procedimiento de recuperación, el usuario tiene que pulsar la tecla **Esc** en la etapa de autenticación en el prearranque.

[Cómo ver la clave de recuperación para una unidad del sistema cifrada por BitLocker en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
6. En la ventana que se abre, seleccione la pestaña **Acceso a una unidad de sistema protegida por BitLocker**.
7. Solicite al usuario el ID de la clave de recuperación indicado en la ventana de introducción de la contraseña de BitLocker y compárelo con el ID del campo **ID de clave de recuperación**.

Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

Como resultado, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá transferirse al usuario.

### [Cómo ver la clave de recuperación para una unidad del sistema cifrada por BitLocker en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuya unidad quiere restaurar el acceso.
3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione la sección **BitLocker**.
5. Compruebe el ID de clave de recuperación. El ID proporcionado por el usuario debe coincidir con el ID que se muestra en la configuración del equipo.

Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

6. Haga clic en el botón **Recibir clave**.

Como resultado, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá transferirse al usuario.

Una vez que se carga el sistema operativo, Kaspersky Endpoint Security solicita al usuario que cambie la contraseña o el código PIN. Después de establecer una nueva contraseña o código PIN, BitLocker creará una nueva clave maestra y la enviará a Kaspersky Security Center. Como resultado, se actualizarán la clave de recuperación y el archivo clave de recuperación. Si el usuario no ha cambiado la contraseña, puede usar la antigua clave de recuperación la próxima vez que se cargue el sistema operativo.

Los equipos que cuenten con el sistema operativo Windows 7 no permiten cambiar la contraseña o el código PIN. Una vez que se introduce la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no le solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, no es posible establecer un nuevo código PIN o contraseña. Este problema proviene de las particularidades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.

## Restauración del acceso a una unidad que no pertenece al sistema

Para comenzar el procedimiento de recuperación, el usuario tiene que hacer clic en el enlace **Forgot your password** en la ventana que proporciona acceso a la unidad. Después de obtener acceso a la unidad cifrada, el usuario puede activar el desbloqueo automático de la unidad durante la autenticación de Windows en la configuración de BitLocker.

### [Cómo ver la clave de recuperación para una unidad que no pertenece al sistema cifrada por BitLocker en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Protección y cifrado de datos** → **Dispositivos cifrados**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que desea crear un archivo de clave de acceso. Luego, en el menú contextual del dispositivo, haga clic en **Obtener acceso para el dispositivo en Kaspersky Endpoint Security para Windows**.
4. Solicite al usuario el ID de la clave de recuperación indicado en la ventana de introducción de la contraseña de BitLocker y compárelo con el ID del campo **ID de clave de recuperación**.

Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

5. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.

### [Cómo ver la clave de recuperación para una unidad cifrada por BitLocker que no pertenece al sistema en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Operaciones** → **Protección y cifrado de datos** → **Dispositivos cifrados**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuya unidad quiere restaurar el acceso.
3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.  
Se iniciará el Asistente para otorgar acceso a un dispositivo.
4. Siga las instrucciones del Asistente para otorgar acceso a un dispositivo:
  - a. Seleccione el complemento **Kaspersky Endpoint Security para Windows**.
  - b. Compruebe el ID de clave de recuperación. El ID proporcionado por el usuario debe coincidir con el ID que se muestra en la configuración del equipo.

Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

- c. Haga clic en el botón **Recibir clave**.

Como resultado, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá transferirse al usuario.

## Pausar la protección de BitLocker para actualizar el software

Hay una serie de consideraciones especiales para actualizar el sistema operativo, instalar paquetes de actualización para el sistema operativo o actualizar otro software con la protección BitLocker activada. La instalación de actualizaciones puede requerir el reinicio del equipo varias veces. Después de cada reinicio, el usuario debe completar la autenticación de BitLocker. Para asegurarse de que las actualizaciones se instalen correctamente, puede desactivar temporalmente la autenticación de BitLocker. En este caso, el disco permanece cifrado y el usuario tiene acceso a los datos después de iniciar sesión en el sistema. Para administrar la autenticación de BitLocker, puede usar la tarea de *Administración de la protección de BitLocker*. Puede usar esta tarea para especificar el número de reinicios del equipo que no requieren la autenticación de BitLocker. De esta forma, una vez instaladas las actualizaciones y después de que finalice la tarea de *Administración de la protección de BitLocker*, la autenticación de BitLocker se activa automáticamente. Puede activar la autenticación de BitLocker en cualquier momento.

[Cómo pausar la protección de BitLocker con la Consola de administración \(MMC\)](#) 

1. En la Consola de administración, vaya a la carpeta **Servidor de administración** → **Tareas**.

Se abre la lista de tareas.

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

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.8.0)** → **Administración de la protección de BitLocker**.

### Paso 2. Administración de la protección de BitLocker

Configure la autenticación de BitLocker. Para pausar la protección de BitLocker, seleccione **Permitir temporalmente omitir la autenticación de BitLocker** e introduzca el número de reinicios sin autenticación de BitLocker (de 1 a 15 veces). Si es necesario, introduzca una fecha y hora de caducidad para la tarea. A la hora especificada, la tarea se desactiva automáticamente y el usuario debe completar la autenticación de BitLocker cuando se reinicia el equipo.

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

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

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

### Paso 4. Definir el nombre de la tarea

Introduzca el nombre de la tarea, por ejemplo, *Actualización a Windows 10*.

### Paso 5. Conclusión de la creación de tareas

Salga del Asistente. Si es necesario, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**. Puede supervisar el progreso de la tarea en las propiedades de la tarea.

[Cómo pausar la protección de BitLocker mediante Web Console](#) 

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

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

## Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

2. En la lista desplegable **Tipo de tarea**, seleccione **Administración de la protección de BitLocker**.

3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Actualización a Windows 10*).

4. En la sección **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

## Paso 2. Administración de la protección de BitLocker

Configure la autenticación de BitLocker. Para pausar la protección de BitLocker, seleccione **Permitir temporalmente omitir la autenticación de BitLocker** e introduzca el número de reinicios sin autenticación de BitLocker (de 1 a 15 veces). Si es necesario, introduzca una fecha y hora de caducidad para la tarea. A la hora especificada, la tarea se desactiva automáticamente y el usuario debe completar la autenticación de BitLocker cuando se reinicia el equipo.

## Paso 3. Conclusión de la creación de tareas

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 la autenticación de BitLocker, Kaspersky Endpoint Security genera un evento correspondiente y registra el número de reinicios restantes. Luego, Kaspersky Endpoint Security envía el evento a Kaspersky Security Center para que lo supervise el administrador. También puede averiguar el número de reinicios restantes en las propiedades del equipo en la consola de Kaspersky Security Center.

Cuando se alcanza el número especificado de reinicios o la hora de caducidad de la tarea, la autenticación de BitLocker se activa automáticamente. Para obtener acceso a los datos, el usuario debe completar la autenticación de BitLocker.

En equipos que ejecutan Windows 7, BitLocker no puede contar los reinicios de equipos. Kaspersky Endpoint Security gestiona el recuento de reinicios en equipos con Windows 7. Por lo tanto, para activar automáticamente la autenticación de BitLocker después de cada reinicio, se debe iniciar Kaspersky Endpoint Security.



Para activar la autenticación de BitLocker antes de tiempo, abra las propiedades de la tarea de *Administración de la protección de BitLocker* y seleccione **Solicitar autenticación en cada oportunidad previa al arranque**.

## Cifrado de archivos en unidades locales del equipo

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El cifrado de archivo tiene las siguientes características especiales:

- Kaspersky Endpoint Security cifra y descifra los archivos de las carpetas predeterminadas solo para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifra ni descifra los archivos de las carpetas predeterminadas de los perfiles de usuario en itinerancia, de los perfiles de usuario obligatorio, de los perfiles de usuario temporal ni de las carpetas redirigidas.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo o aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas se encuentran en la lista de exclusiones del cifrado:
  - %WINDIR%;
  - %PROGRAMFILES% y %PROGRAMFILES(X86)%;
  - Archivos de registro de Windows.

No se puede ver ni modificar la lista de exclusiones del cifrado. Los archivos y las carpetas de la lista de exclusiones del cifrado se pueden añadir a la lista de cifrado, pero no se cifrarán durante el cifrado de archivos.

## Cifrado de los archivos de las unidades del equipo local

Kaspersky Endpoint Security no cifra los archivos que se encuentran en el almacenamiento en la nube de OneDrive o en otras carpetas que tienen OneDrive como nombre. Kaspersky Endpoint Security también bloquea la copia de archivos cifrados a carpetas de OneDrive si esos archivos no se añaden a la [regla de descifrado](#).

*Para cifrar los archivos de las unidades de disco locales:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de archivos**.

6. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.

7. En la pestaña **Cifrado**, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione uno de los elementos siguientes:

a. Seleccione el elemento **Carpetas predeterminadas** para añadir archivos desde carpetas de perfiles de usuario locales sugeridos por expertos de Kaspersky a una regla de cifrado.

- **Documentos**. Los archivos en la carpeta estándar *Documentos* del sistema operativo y sus subcarpetas.
- **Favoritos**. Los archivos en la carpeta estándar *Favoritos* del sistema operativo y sus subcarpetas.
- **Escritorio**. Los archivos en la carpeta estándar *Escritorio* del sistema operativo y sus subcarpetas.
- **Archivos temporales**. Archivos temporales relacionados con el funcionamiento de aplicaciones instaladas en el equipo. Por ejemplo, las aplicaciones de Microsoft Office crean archivos temporales que contienen copias de seguridad de documentos.
- **Archivos de Outlook**. Archivos relacionados con el funcionamiento del cliente de correo Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de libretas de direcciones sin conexión (OAB) y archivos de libretas de direcciones personales (PAB).

b. Seleccione el elemento **Carpeta personalizada** para añadir una ruta de la carpeta introducida manualmente a una regla de cifrado.

Al añadir una ruta de carpeta, cumpla las siguientes reglas:

- Use una variable de entorno (por ejemplo, %FOLDER%\UserFolder\). Puede usar una variable de entorno solo una vez y solo al comienzo de la ruta.
- No use rutas relativas. Puede usar el conjunto `\..\` (p. ej., C:\Users\..\UserFolder\). El conjunto `\..\` indica la transición a la carpeta principal.
- No utilice los caracteres `*` y `?`.
- No utilice rutas UNC.
- Utilice `;` o `,` como carácter de separación.

c. Seleccione el elemento **Archivos por extensión** para añadir extensiones de archivo individuales a una regla de cifrado. Kaspersky Endpoint Security cifra los archivos de todas las unidades de disco locales del equipo que tienen las extensiones especificadas.

d. Seleccione el elemento **Archivos por grupos de extensiones** para añadir grupos de extensiones de archivo a una regla de cifrado (por ejemplo, *Documentos de Microsoft Office*). Kaspersky Endpoint Security cifra archivos cuyas extensiones se incluyen en los grupos de extensiones de todas las unidades de disco locales del equipo.

8. Guarde los cambios.

Una vez que se aplica la directiva, Kaspersky Endpoint Security cifra los archivos incluidos en la regla de cifrado que no se incluyen en la [regla de descifrado](#).

El cifrado de archivo tiene las siguientes características especiales:

- Si se añade el mismo archivo a una regla de cifrado y a una regla de descifrado, Kaspersky Endpoint Security realiza las siguientes acciones:

- Si el archivo no está cifrado, Kaspersky Endpoint Security no cifra este archivo.
- Si el archivo está cifrado, Kaspersky Endpoint Security descifra este archivo.
- Kaspersky Endpoint Security continúa cifrando archivos nuevos si estos cumplen los criterios de la regla de cifrado. Por ejemplo, cuando cambia las propiedades de un archivo sin cifrar (ruta o extensión), el archivo cumple los criterios de la regla de cifrado. Kaspersky Endpoint Security cifra este archivo.
- Cuando el usuario crea un nuevo archivo cuyas propiedades cumplen los criterios de la regla de cifrado, Kaspersky Endpoint Security cifra el archivo en cuanto se abre.
- Kaspersky Endpoint Security pospone el cifrado de archivos abiertos hasta que se cierren.
- Si mueve un archivo cifrado a otra carpeta de la unidad local, el archivo se mantiene cifrado, sin considerar si la carpeta se incluye o no en la regla de cifrado.
- Si descifra un archivo y lo copia a otra carpeta local que no está incluida en la regla de descifrado, se puede cifrar una copia del archivo. Para evitar que el archivo copiado se cifre, cree una regla de descifrado para la carpeta de destino.

## Creación de reglas de acceso a archivos cifrados para aplicaciones

*Para crear reglas de acceso a archivos cifrados para aplicaciones:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de archivos**.
6. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.

Las reglas de acceso solo se aplican cuando se está en el modo **De acuerdo con las reglas**. Tras aplicar reglas de acceso en el modo **De acuerdo con las reglas**, si cambia al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de acceso. Todas las aplicaciones tendrán acceso a todos los archivos cifrados.

7. En la parte derecha de la ventana, seleccione la pestaña **Reglas para aplicaciones**.
8. Si desea seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.
  - a. Especifique los filtros para restringir la lista de aplicaciones de la tabla. Para ello, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período añadido**, así como todas las casillas de verificación de la sección **Grupo**.
  - b. Haga clic en el botón **Actualizar**.

- c. La tabla muestra las aplicaciones que cumplen los filtros aplicados.
- d. En la columna **Aplicaciones**, active las casillas de las aplicaciones para las que desea crear reglas de acceso a archivos cifrados.
- e. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a los archivos cifrados.
- f. En la lista desplegable **Acciones para aplicaciones seleccionadas antes**, seleccione la acción que Kaspersky Endpoint Security llevará a cabo en las reglas de acceso a archivos cifrados que se han formado previamente para dichas aplicaciones.

La información sobre las reglas de acceso a archivos cifrados para aplicaciones se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

9. Si desea seleccionar manualmente las aplicaciones, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.
  - a. En el campo de entrada, introduzca el nombre o la lista de nombres de archivos de aplicaciones ejecutables, incluidas sus extensiones.

También puede añadir nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center haciendo clic en el botón **Añadir de la lista de Kaspersky Security Center**.
  - b. Si es preciso, en el campo **Descripción**, introduzca una descripción de la lista de aplicaciones.
  - c. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a los archivos cifrados.

La información sobre las reglas de acceso a archivos cifrados para aplicaciones se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

10. Guarde los cambios.

## Cifrar archivos creados o modificados por aplicaciones específicas

Puede crear una regla según la cual Kaspersky Endpoint Security cifrará todos los archivos creados o modificados por las aplicaciones especificadas en la regla.

Los archivos que fueron creados o modificados por las aplicaciones especificadas antes de que se aplicara la regla de cifrado no se cifrarán.

*Para configurar el cifrado de archivos que se crean o modifican por aplicaciones específicas:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.

5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de archivos**.

6. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.

Las reglas de cifrado se aplican únicamente en el modo **De acuerdo con las reglas**. Después de aplicar reglas de cifrado en el modo **De acuerdo con las reglas**, si cambia al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de cifrado. Los archivos que se cifraron con anterioridad permanecerán cifrados.

7. En la parte derecha de la ventana, seleccione la pestaña **Reglas para aplicaciones**.

8. Si desea seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.

a. Especifique los filtros para restringir la lista de aplicaciones de la tabla. Para ello, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período añadido**, así como todas las casillas de verificación de la sección **Grupo**.

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

La tabla muestra las aplicaciones que cumplen los filtros aplicados.

c. En la columna **Aplicaciones**, seleccione las casillas situadas junto a las aplicaciones cuyos archivos creados quiere cifrar.

d. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

e. En la lista desplegable **Acciones para aplicaciones seleccionadas antes**, seleccione la acción que Kaspersky Endpoint Security llevará a cabo en las reglas de cifrado de archivos que se han creado previamente para las aplicaciones mencionadas.

La información sobre la regla de cifrado para archivos creados o modificados por aplicaciones seleccionadas se muestra en la tabla de la pestaña **Regla para aplicaciones**.

9. Si desea seleccionar manualmente las aplicaciones, haga clic en el botón **Añadir** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

a. En el campo de entrada, introduzca el nombre o la lista de nombres de archivos de aplicaciones ejecutables, incluidas sus extensiones.

También puede añadir nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center haciendo clic en el botón **Añadir de la lista de Kaspersky Security Center**.

b. Si es preciso, en el campo **Descripción**, introduzca una descripción de la lista de aplicaciones.

c. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

La información sobre la regla de cifrado para archivos creados o modificados por aplicaciones seleccionadas se muestra en la tabla de la pestaña **Regla para aplicaciones**.

10. Guarde los cambios.

## Generación de una regla de descifrado

Para generar una regla de descifrado:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de archivos**.
6. En la lista desplegable **Modo de cifrado**, seleccione **De acuerdo con las reglas**.
7. En la pestaña **Descifrado**, haga clic en el botón **Añadir** y en la lista desplegable seleccione uno de los elementos siguientes:
  - a. Seleccione el elemento **Carpetas predeterminadas** para añadir archivos desde carpetas de perfiles de usuario locales sugeridos por expertos de Kaspersky a una regla de descifrado.
  - b. Seleccione el elemento **Carpeta personalizada** para añadir una ruta de la carpeta introducida manualmente a una regla de descifrado.
  - c. Seleccione el elemento **Archivos por extensión** para añadir extensiones de archivo individuales a una regla de descifrado. Kaspersky Endpoint Security no cifra los archivos de todas las unidades de disco locales del equipo que tienen las extensiones especificadas.
  - d. Seleccione el elemento **Archivos por grupos de extensiones** para añadir grupos de extensiones de archivo a una regla de descifrado (por ejemplo, *Documentos de Microsoft Office*). Kaspersky Endpoint Security no cifra archivos cuyas extensiones se incluyen en los grupos de extensiones de todas las unidades de disco locales del equipo.
8. Guarde los cambios.

Si un mismo archivo se ha añadido a la regla de cifrado y a la de descifrado, Kaspersky Endpoint Security no cifra este archivo si está descifrado y descifra el archivo si está cifrado.

## Descifrado de archivos de las unidades del equipo local

Para descifrar los archivos de las unidades de disco locales:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de archivos**.

6. En la parte derecha de la ventana, seleccione la pestaña **Cifrado**.

7. Elimine los archivos y las carpetas que desea descifrar de la lista de cifrado. Para ello, seleccione los archivos y el elemento **Eliminar regla y descifrar archivos** del menú contextual del botón **Eliminar**.

Los archivos y las carpetas que se eliminan de la lista de cifrado se añaden automáticamente a la lista de descifrado.

8. [Cree una lista de descifrado de archivos](#).

9. Guarde los cambios.

En cuanto se aplique la directiva, Kaspersky Endpoint Security descifra los archivos cifrados que se añaden a la lista de descifrado.

Kaspersky Endpoint Security descifra los archivos cifrados si sus parámetros (ruta del archivo/nombre del archivo/extensión del archivo) cambian para coincidir con los parámetros de los objetos añadidos a la lista de descifrado.

Kaspersky Endpoint Security pospone el descifrado de archivos abiertos hasta que se cierren.

## Creación de paquetes cifrados

Para proteger sus datos cuando envía archivos a usuarios fuera de la red corporativa, puede usar paquetes cifrados. Los paquetes cifrados pueden resultar convenientes para transferir archivos grandes en unidades extraíbles, ya que los clientes de correo electrónico tienen restricciones de tamaño de archivo.

Antes de crear paquetes cifrados, Kaspersky Endpoint Security le pedirá al usuario una contraseña. Para proteger los datos de manera fiable, puede activar la evaluación de seguridad de la contraseña y especificar los requisitos de seguridad de la contraseña. Esto evitará que los usuarios usen contraseñas cortas y sencillas como, por ejemplo, 1234.

[Cómo activar la evaluación de seguridad de la contraseña al crear archivos comprimidos cifrados en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Configuración común de cifrado**.
6. En el bloque **Configuración de contraseña**, haga clic en el botón **Configuración**.
7. En la ventana que se abre, seleccione la ficha **Paquete cifrado**.
8. Configure los ajustes de la complejidad de la contraseña al crear paquetes cifrados.




1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos** → **Cifrado de archivos**.
5. En el bloque **Configuración de contraseña para paquetes cifrados**, configure los criterios de seguridad de la contraseña necesarios para crear paquetes cifrados.

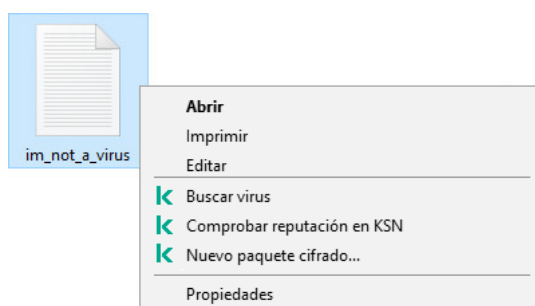
Puede crear paquetes cifrados en equipos con Kaspersky Endpoint Security instalado con Cifrado de archivos disponible.

Cuando se añade un archivo al paquete cifrado cuyo contenido reside en el almacenamiento en nube de OneDrive, Kaspersky Endpoint Security descarga el contenido del archivo y realiza el cifrado.

*Para crear un paquete cifrado:*

1. En cualquier gestor de archivos, seleccione los archivo o carpetas que desee añadir al paquete cifrado. Haga clic con el botón derecho del ratón para abrir su menú contextual.
2. En el menú contextual, seleccione **Nuevo paquete cifrado** (vea la figura a continuación).
3. En la ventana que se abre, seleccione una ubicación en una unidad extraíble para guardar el archivo cifrado → especifique el nombre del paquete y haga clic en el botón **Guardar**.
4. En la ventana que se abre, especifique la contraseña y confírmela.  
La contraseña debe cumplir los criterios de complejidad especificados en la directiva.
5. Haga clic en el botón **Crear**.

Se inicia el proceso de creación del paquete cifrado. Kaspersky Endpoint Security no comprime los archivos cuando crea un paquete cifrado. Cuando el proceso termina, se crea un paquete cifrado autoextraíble y protegido con contraseña (un archivo ejecutable con la extensión .exe – ) en la carpeta de destino seleccionada.



Creación de un paquete cifrado



Para acceder a los archivos de un paquete cifrado, haga doble clic en él para iniciar el Asistente de descompresión y, a continuación, introduzca la contraseña. Si ha olvidado o ha perdido su contraseña, no es posible recuperarla y acceder a los archivos en el paquete cifrado. Puede recrear el paquete cifrado.

## Restauración del acceso a los archivos cifrados

Cuando los archivos se cifran, Kaspersky Endpoint Security recibe una clave de cifrado para acceder directamente a los archivos cifrados. Al utilizar esta clave de cifrado, un usuario que trabaje con una cuenta de Windows que se encontrara activa durante el cifrado de archivos podrá acceder a dichos archivos directamente. Los usuarios que trabajen con cuentas de Windows que no se encontraran activas durante el cifrado de archivos deberán conectarse a Kaspersky Security Center para acceder a los archivos cifrados.

Es posible que los archivos cifrados no sean accesibles en las siguientes circunstancias:

- El equipo del usuario almacena las claves de cifrado, pero no existe conexión con Kaspersky Security Center para administrar las claves. En este caso, el usuario debe solicitar acceso a los archivos cifrados al administrador de la red de área local.

Si no existe acceso a Kaspersky Security Center, debe hacer lo siguiente:

- solicitar una clave de acceso para acceder a archivos cifrados en discos duros del equipo;
- para acceder a archivos cifrados almacenados en unidades extraíbles, deberá solicitar claves de acceso separadas para los archivos cifrados en cada unidad extraíble.
- Los componentes de cifrado se eliminan desde el equipo del usuario. En este evento, el usuario puede abrir archivos cifrados en unidades locales y extraíbles, pero el contenido de esos archivos aparecerá cifrado.

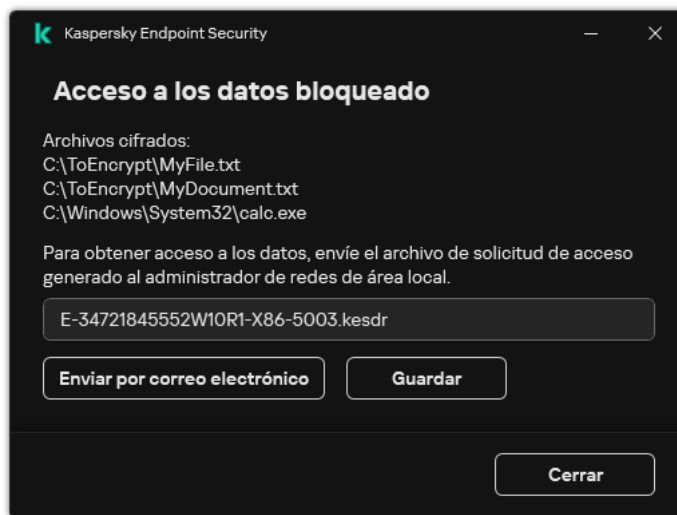
El usuario puede trabajar con archivos cifrados en las siguientes circunstancias:

- Los archivos se encuentran dentro de [paquetes cifrados](#) creados en un equipo con Kaspersky Endpoint Security.
- Los archivos se almacenan en unidades extraíbles en las cuales se permitió el [modo portátil](#).

Para obtener acceso a los archivos cifrados, el usuario tiene que comenzar el procedimiento de recuperación (solicitud-respuesta).

La recuperación del acceso a los archivos cifrados consta de los siguientes pasos:

1. El usuario envía un archivo de solicitud de acceso al administrador (vea la imagen más abajo).
2. El administrador añade el archivo de solicitud de acceso a Kaspersky Security Center, crea un archivo clave de acceso y lo envía al usuario.
3. El usuario añade el archivo clave de acceso a Kaspersky Endpoint Security y obtiene acceso a los archivos.



Restauración del acceso a los archivos cifrados

Para comenzar el procedimiento de recuperación, el usuario tiene que intentar acceder a un archivo. Como resultado, Kaspersky Endpoint Security creará un archivo de solicitud de acceso (un archivo con la extensión KESDC), que el usuario tiene que enviar al administrador, por ejemplo, por correo electrónico.

Kaspersky Endpoint Security genera un archivo de solicitud de acceso para acceder a todos los archivos cifrados almacenados en la unidad del equipo (unidad local o extraíble).

### [Cómo obtener un archivo clave de acceso a datos cifrados en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
6. En la ventana de diálogo que se abre, seleccione la pestaña **Cifrado de datos**.
7. En la pestaña **Cifrado de datos**, haga clic en el botón **Examinar**.
8. En la ventana para seleccionar un archivo de solicitud de acceso, especifique la ruta al archivo recibido del usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.

### [Cómo obtener un archivo clave de acceso a datos cifrados en Web Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
  2. Seleccione la casilla de verificación junto al nombre del equipo a cuyos datos quiere restaurar el acceso.
  3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.
  4. Seleccione la sección **Cifrado de datos**.
  5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión KESDC).  
Web Console mostrará información sobre la solicitud. Esto incluirá el nombre del equipo en el que el usuario solicita acceso al archivo.
  6. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión KESDR).
- Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

Tras recibir el archivo clave de acceso a datos cifrados, el usuario tiene que ejecutar el archivo haciendo doble clic en él. Como resultado, Kaspersky Endpoint Security concederá acceso a todos los archivos cifrados almacenados en la unidad. Para acceder a archivos cifrados almacenados en otras unidades, obtenga un archivo clave de acceso independiente para cada unidad.

## Restauración del acceso a los datos cifrados después del error del sistema operativo

Puede restaurar el acceso a los datos después del error del sistema operativo solo con el cifrado de archivos (CA). No puede restaurar el acceso a los datos si se utiliza cifrado de disco completo (CDC).

*Para restaurar el acceso a los datos cifrados después del error del sistema operativo:*

1. Vuelva a instalar el sistema operativo sin formatear el disco duro.
2. [Instale Kaspersky Endpoint Security](#).
3. Establezca una conexión entre el equipo y el Servidor de administración de Kaspersky Security Center que controló el equipo cuando se cifraron los datos.

Se concederá el acceso a los datos cifrados bajo las mismas condiciones que se aplicaban antes del error del sistema operativo.

## Modificación de plantillas de mensajes de acceso a archivos cifrados

*Para modificar las plantillas de los mensajes de acceso a archivos cifrados:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.

3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Configuración común de cifrado**.
6. En el bloque **Plantillas**, haga clic en el botón **Plantillas**.
7. En la ventana abierta, haga lo siguiente:
  - Si desea editar la plantilla del mensaje del usuario, seleccione la pestaña **Mensaje del usuario**. Se abre la ventana **Acceso a los datos bloqueado** cuando el usuario intenta acceder a un archivo cifrado y no existe ninguna clave para acceder a archivos cifrados disponible en el equipo. Al hacer clic en el botón **Enviar por correo electrónico** de la ventana **Acceso a los datos bloqueado**, se crea un mensaje de usuario de forma automática. Este mensaje se envía al administrador de la red de área local corporativa junto con el archivo de solicitud de acceso a archivos cifrados.
  - Si desea editar la plantilla del mensaje del administrador, seleccione la pestaña **Mensaje del administrador**. Este mensaje se crea automáticamente al hacer clic en el botón **Enviar por correo electrónico** de la ventana **Solicitar acceso a los archivos cifrados** y se envía al usuario después de que se le otorga acceso a los archivos cifrados.
8. Modifique las plantillas de mensajes.
9. Guarde los cambios.

## Cifrado de unidades extraíbles

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si una unidad extraíble con un sistema de archivos no compatible está conectada al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Para proteger los datos de las unidades extraíbles, puede usar los siguientes tipos de cifrado:

- Cifrado de disco completo (FDE).  
Cifrado de toda la unidad extraíble, incluido el sistema de archivos.

No se puede acceder a datos cifrados fuera de la red corporativa. También es imposible acceder a datos cifrados dentro de la red corporativa si el equipo no está conectado a Kaspersky Security Center (p. ej., en un equipo "invitado").

- Cifrado de archivos (FLE).  
Cifrado solo de los archivos en una unidad extraíble. El sistema de archivos permanece sin cambios.

El cifrado de archivos en unidades extraíbles proporciona la capacidad de acceder a datos fuera de la red corporativa mediante un modo especial llamado [modo portátil](#).

Durante el cifrado, Kaspersky Endpoint Security crea una clave maestra. Kaspersky Endpoint Security guarda la clave maestra en los siguientes repositorios:

- Kaspersky Security Center.  
La clave maestra está cifrada con la clave secreta del usuario.
- Equipo del usuario.  
La clave maestra está cifrada con la clave pública de Kaspersky Security Center.

Una vez que se completa el cifrado, se puede acceder a los datos de la unidad extraíble dentro de la red corporativa como si fuera una unidad extraíble convencional sin cifrar.

## Acceso a datos cifrados

Cuando se conecta una unidad extraíble con datos cifrados, Kaspersky Endpoint Security realiza las siguientes acciones:

1. Comprueba si hay una clave maestra en el almacenamiento local en el equipo del usuario.  
Si se encuentra la clave maestra, el usuario obtiene acceso a los datos en la unidad extraíble.  
Si la clave maestra no se encuentra, Kaspersky Endpoint Security realiza las siguientes acciones:
  - a. Envíe una solicitud a Kaspersky Security Center.  
Después de recibir la solicitud, Kaspersky Security Center envía una respuesta que contiene la clave maestra.
  - b. Kaspersky Endpoint Security guarda la clave maestra en el almacenamiento local en el equipo del usuario para operaciones posteriores con la unidad extraíble cifrada.

2. Descifre los datos.

## Características especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles tiene las siguientes características especiales:

- La directiva con la configuración preestablecida para el cifrado extraíble de la unidad se forma para un grupo específico de equipos administrados. Por lo tanto, el resultado de aplicar la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al que se conecta la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra archivos de solo lectura almacenados en las unidades extraíbles.
- Los siguientes tipos de dispositivo son compatibles como unidades extraíbles:
  - Medios de datos conectados por medio del puerto USB

- Discos duros conectados por medio de los puertos USB y FireWire
- Unidades SSD conectadas por medio de los puertos USB y FireWire

## Iniciar el cifrado de unidades extraíbles

Puede usar una directiva para descifrar una unidad extraíble. Se genera una directiva con configuraciones definidas para el cifrado de unidades extraíbles para un grupo de administración específico. Por lo tanto, el resultado del descifrado de los datos en las unidades extraíbles depende del equipo con el cual la unidad extraíble está conectada.

Kaspersky Endpoint Security admite el cifrado de los sistemas de archivos FAT32 y NTFS. Cuando se conecta una unidad extraíble con un sistema de archivos incompatible, el proceso de cifrado de la unidad finaliza con un error y Kaspersky Endpoint Security asigna estado de solo lectura a la unidad.

*Para cifrar unidades extraíbles:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de unidades extraíbles**.
6. En la lista desplegable **Modo de cifrado**, indique qué hará Kaspersky Endpoint Security por defecto con las unidades extraíbles:
  - **Cifrar toda la unidad extraíble** (FDE). Kaspersky Endpoint Security cifrará el contenido de las unidades extraíbles sector por sector. Con ello, se cifrarán no solo los archivos de las unidades, sino también sus sistemas de archivos, incluidos los nombres de los archivos y las estructuras de carpetas.
  - **Cifrar todos los archivos** (FLE). Kaspersky Endpoint Security cifrará todos los archivos que se encuentren en las unidades extraíbles. La aplicación no cifra los sistemas de archivos de las unidades extraíbles, incluidos los nombres de los archivos y las estructuras de carpetas.
  - **Cifrar solo archivos nuevos** (FLE). De los archivos de las unidades extraíbles, Kaspersky Endpoint Security cifrará únicamente aquellos que se hayan añadido o modificado desde la última aplicación de la directiva de Kaspersky Security Center.

Si una unidad extraíble ya está cifrada, Kaspersky Endpoint Security no la vuelve a cifrar.

7. Si desea que las unidades extraíbles se cifren [en modo portátil](#), active la casilla de verificación **Modo portátil**. El *modo portátil* es un modo de cifrado de archivos (FLE) para unidades extraíbles que ofrece la capacidad de acceder a los datos fuera de una red corporativa. El modo portátil también le permite trabajar con datos cifrados en equipos que no tengan instalado Kaspersky Endpoint Security.

8. Para cifrar unidades extraíbles nuevas, recomendamos activar la casilla **Cifrar solo el espacio en disco utilizado**. Si la casilla de verificación queda desactivada, Kaspersky Endpoint Security cifrará todos los archivos que encuentre en una unidad, incluidos los remanentes de archivos eliminados o modificados.
9. Si desea configurar opciones de cifrado para unidades extraíbles específicas, puede [definir reglas de cifrado](#).
10. Si desea cifrar las unidades extraíbles en modo sin conexión utilizando el cifrado de disco completo, active la casilla de verificación **Permitir el cifrado de las unidades extraíbles en modo sin conexión**.

El *modo de cifrado sin conexión* hace referencia al cifrado de unidades extraíbles (FDE) cuando no hay conexión con Kaspersky Security Center. Durante el cifrado, Kaspersky Endpoint Security guarda la clave maestra únicamente en el equipo del usuario. La clave maestra se envía a Kaspersky Security Center cuando se realiza la siguiente sincronización.

Si el equipo en el que está almacenada la clave maestra sufre un desperfecto y los datos no se transfirieron a Kaspersky Security Center, será imposible acceder a la unidad extraíble.

Si la casilla de verificación **Permitir el cifrado de las unidades extraíbles en modo sin conexión** no está activada y no hay conexión con Kaspersky Security Center, las unidades extraíbles no se podrán cifrar.

11. Guarde los cambios.

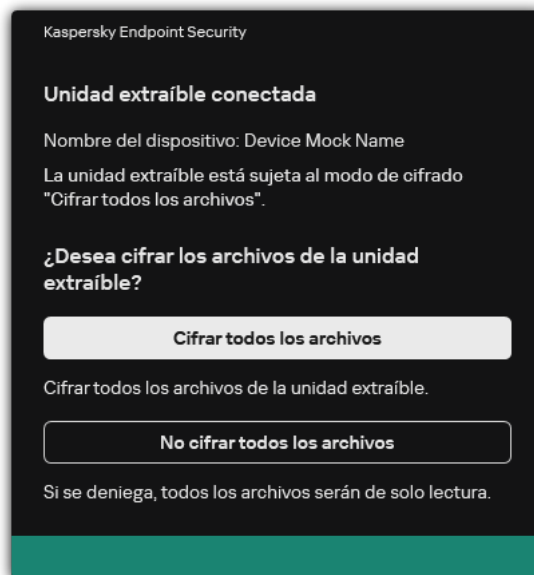
Cuando se conecte una unidad extraíble (o cuando ya haya una unidad extraíble conectada) después de que se aplique la directiva, Kaspersky Endpoint Security le solicitará al usuario que confirme la operación de cifrado (vea la imagen de más abajo).

La aplicación podrá realizar las siguientes acciones:

- Si el usuario confirma la solicitud de cifrado, Kaspersky Endpoint Security cifrará los datos.
- Si el usuario rechaza la solicitud de cifrado, Kaspersky Endpoint Security no modificará los datos y asignará acceso de solo lectura a la unidad extraíble.
- Si el usuario ignora la solicitud de cifrado, Kaspersky Endpoint Security no modificará los datos y asignará acceso de solo lectura a la unidad extraíble. La aplicación repetirá la solicitud la siguiente vez que se aplique una directiva o cuando se vuelva a conectar la misma unidad extraíble.

Si el usuario inicia la extracción segura de una unidad extraíble durante el cifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de cifrado de datos y permite la extracción de la unidad extraíble antes de que el proceso de cifrado haya finalizado. El proceso de cifrado se reanudará cuando el usuario conecte la unidad nuevamente al equipo.

Si el proceso de cifrado de una unidad extraíble falla, puede ver el informe **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Es posible que otra aplicación bloquee el acceso a los archivos. En tal caso, pruebe a desconectar la unidad extraíble del equipo y volver a conectarla.



Solicitud de cifrado para una unidad extraíble

## Añadir una regla de cifrado para unidades extraíbles

*Para añadir una regla de cifrado de unidades extraíbles:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de unidades extraíbles**.
6. Haga clic en el botón **Añadir** y, en la lista desplegable, seleccione uno de los siguientes elementos:
  - Si desea añadir reglas de cifrado para las unidades extraíbles que están en la lista de dispositivos de confianza del componente Control de dispositivos, seleccione **De una lista de dispositivos de confianza de esta directiva**.
  - Si desea añadir reglas de cifrado para las unidades extraíbles que están en la lista de Kaspersky Security Center, seleccione **De la lista de dispositivos de Kaspersky Security Center**.
7. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione la acción que Kaspersky Endpoint Security debe realizar en los archivos almacenados en las unidades extraíbles seleccionadas.
8. Seleccione la casilla de verificación **Modo portátil** si desea que Kaspersky Endpoint Security prepare las unidades extraíbles antes del cifrado, permitiendo, así, utilizar los archivos cifrados que contienen en modo portátil.

El modo portátil le permite utilizar los archivos cifrados almacenados en las unidades extraíbles conectadas a los equipos [que no disponen de la funcionalidad de cifrado](#).



9. Seleccione la casilla de verificación **Cifrar solo el espacio en disco utilizado** si desea que Kaspersky Endpoint Security cifre solo esos sectores del disco que están ocupados por archivos.

Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable. La función **Cifrar solo el espacio en disco utilizado** se recomienda para las unidades nuevas que no se han utilizado anteriormente.

Si un dispositivo se cifró anteriormente mediante la función **Cifrar solo el espacio en disco utilizado**, después de aplicar una directiva en el modo **Cifrar toda la unidad extraíble**, los sectores que aún no están ocupados por archivos no se cifrarán.

10. En la lista desplegable **Acciones para dispositivos que se seleccionaron antes**, seleccione la acción que realizará Kaspersky Endpoint Security conforme a las reglas de cifrado definidas previamente para las unidades extraíbles:

- Si desea que la regla de cifrado creada anteriormente para la unidad extraíble no sufra modificaciones, seleccione **Omitir**.
- Si desea que la regla de cifrado creada anteriormente para la unidad extraíble sea reemplazada por la regla nueva, seleccione **Actualizar**.

11. Guarde los cambios.

Las reglas de cifrado añadidas para las unidades extraíbles se aplicarán a las unidades extraíbles conectadas a cualquier equipo de la organización.

## Exportación e importación de una lista de reglas de cifrado para unidades extraíbles

Puede exportar la lista de reglas de cifrado de unidades extraíbles a un archivo XML. Luego, puede modificar el archivo para, por ejemplo, añadir una gran cantidad de reglas para el mismo tipo de unidades extraíbles. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas o para migrar las reglas a un servidor diferente.

[Cómo exportar e importar una lista de reglas de cifrado de unidades extraíbles en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de unidades extraíbles**.
6. Para exportar la lista de reglas de cifrado para unidades extraíbles:
  - a. Seleccione las reglas que quiera exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.  
Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
  - b. Haga clic en el enlace **Exportar**.
  - c. En la ventana que se abre, especifique el nombre del archivo XML al que desee exportar la lista de reglas y seleccione la carpeta en la que desee guardar este archivo.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas al archivo XML.
7. Para importar una lista de reglas de cifrado para unidades extraíbles:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.

[Cómo exportar e importar una lista de reglas de cifrado de unidades extraíbles en Web Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 enlace **Reglas de cifrado**.  
Esto abre una lista de reglas de cifrado para unidades extraíbles.
6. Para exportar la lista de reglas de cifrado para unidades extraíbles:
  - a. Seleccione las reglas que quiera exportar.
  - b. Haga clic en el botón **Exportar**.
  - c. Confirme que desea exportar solo las reglas seleccionadas o exportar la lista completa.
  - d. Guarde el archivo.  
Kaspersky Endpoint Security exporta la lista de reglas a un archivo XML en la carpeta de descargas predeterminada.
7. Para importar la lista de reglas:
  - a. Haga clic en el enlace **Importar**.  
En la ventana que se abre, seleccione el archivo XML del que desea importar la lista de reglas.
  - b. Abra el archivo.  
Si el equipo ya tiene una lista de reglas, Kaspersky Endpoint Security le pedirá que elimine la lista existente o que añada nuevas entradas desde el archivo XML.
8. Guarde los cambios.

## Modo portátil para acceder a archivos cifrados de unidades extraíbles

El *modo portátil* es un modo de cifrado de archivos (FLE) para unidades extraíbles que ofrece la capacidad de acceder a los datos fuera de una red corporativa. El modo portátil también le permite trabajar con datos cifrados en equipos que no tengan instalado Kaspersky Endpoint Security.

Resulta útil usar el modo portátil en los siguientes casos:

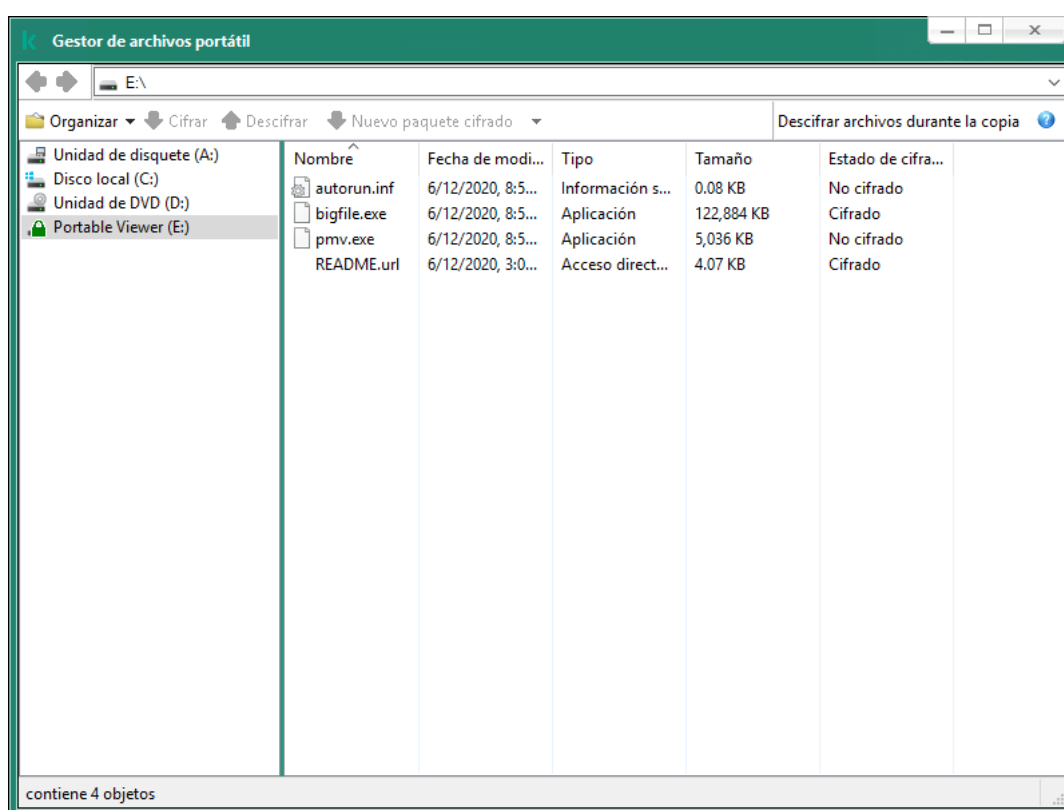
- No hay una conexión entre el equipo y el Servidor de administración de Kaspersky Security Center.
- La infraestructura ha cambiado con la modificación del Servidor de administración de Kaspersky Security Center.
- Kaspersky Endpoint Security no está instalado en el equipo.

## Administrador de archivos portátil

Para trabajar en el modo portátil, Kaspersky Endpoint Security instala un módulo de cifrado especial denominado *Gestor de archivos portátil* en una unidad extraíble. El Gestor de archivos portátil proporciona una interfaz para trabajar con datos cifrados si Kaspersky Endpoint Security no está instalado en el equipo (vea la imagen más abajo). Si Kaspersky Endpoint Security está instalado en su equipo, puede trabajar con unidades extraíbles cifradas utilizando su gestor de archivos habitual (por ejemplo, Explorador).

El Gestor de archivos portátil almacena una clave para cifrar archivos en una unidad extraíble. La clave está cifrada con la contraseña del usuario. El usuario establece una contraseña antes de cifrar archivos en una unidad extraíble.

El Gestor de archivos portátil se inicia automáticamente cuando se conecta una unidad extraíble a un equipo en el que no está instalado Kaspersky Endpoint Security. Si el inicio automático de las aplicaciones está desactivado en el equipo, inicie manualmente el Gestor de archivos portátil. Para ello, ejecute el archivo con el nombre pmv.exe que se almacena en la unidad extraíble.



Administrador de archivos portátil

## Compatibilidad con el modo portátil para trabajar con archivos cifrados

[Cómo activar la compatibilidad con el modo portátil para trabajar con archivos cifrados en unidades extraíbles en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de unidades extraíbles**.
6. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione **Cifrar solo archivos nuevos** o **Solo cifrar archivos nuevos**.

El modo portátil solo está disponible con el Cifrado de archivos (FLE). No se puede activar la compatibilidad con el modo portátil para el Cifrado de disco completo (FDE).

7. Active la casilla de verificación **Modo portátil**.
8. Si es necesario, [añada reglas de cifrado para unidades extraíbles específicas](#).
9. Guarde los cambios.
10. Después de aplicar la directiva, conecte la unidad extraíble al equipo.
11. Confirme la operación de cifrado del disco extraíble.  
Esto abre una ventana en la cual puede crear una contraseña para el Gestor de archivos portátil.
12. Especifique una contraseña que cumpla con los requisitos de resistencia y confírmela.
13. Guarde los cambios.

Kaspersky Endpoint Security cifrará los archivos en la unidad extraíble. El Gestor de archivos portátil utilizado para trabajar con archivos cifrados también se añadirá al disco extraíble. Si ya hay archivos cifrados en la unidad extraíble, Kaspersky Endpoint Security los volverá a cifrar con su propia clave. Esto permite al usuario acceder a todos los archivos de la unidad extraíble en el modo portátil.

[Cómo activar la compatibilidad con el modo portátil para trabajar con archivos cifrados en unidades extraíbles en Web Console](#) 

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.  
Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos** → **Cifrado de unidades extraíbles**.
5. Debajo de **Administrar cifrado**, seleccione **Cifrar todos los archivos** o **Cifrar solo archivos nuevos**.

El modo portátil solo está disponible con el Cifrado de archivos (FLE). No se puede activar la compatibilidad con el modo portátil para el Cifrado de disco completo (FDE).

6. Active la casilla de verificación **Modo portátil**.
7. Si es necesario, [añada reglas de cifrado para unidades extraíbles específicas](#).
8. Guarde los cambios.
9. Después de aplicar la directiva, conecte la unidad extraíble al equipo.
10. Confirme la operación de cifrado del disco extraíble.  
Esto abre una ventana en la cual puede crear una contraseña para el Gestor de archivos portátil.
11. Especifique una contraseña que cumpla con los requisitos de resistencia y confírmela.
12. Guarde los cambios.

Kaspersky Endpoint Security cifrará los archivos en la unidad extraíble. El Gestor de archivos portátil utilizado para trabajar con archivos cifrados también se añadirá al disco extraíble. Si ya hay archivos cifrados en la unidad extraíble, Kaspersky Endpoint Security los volverá a cifrar con su propia clave. Esto permite al usuario acceder a todos los archivos de la unidad extraíble en el modo portátil.

## Acceso a los archivos cifrados en una unidad extraíble

Después de cifrar los archivos en una unidad extraíble con compatibilidad con el modo portátil, están disponibles los siguientes métodos de acceso a los archivos:

- Si Kaspersky Endpoint Security no está instalado en el equipo, el Gestor de archivos portátil le solicitará que introduzca una contraseña. Deberá introducir la contraseña cada vez que reinicie el equipo o vuelva a conectar la unidad extraíble.
- Si el equipo se encuentra fuera de la red corporativa y Kaspersky Endpoint Security está instalado en el equipo, la aplicación le pedirá que introduzca la contraseña o le envíe al administrador una solicitud para acceder a los archivos. Después de obtener acceso a los archivos en una unidad extraíble, Kaspersky Endpoint Security guardará la clave secreta en el almacén de claves del equipo. Esto permitirá el acceso a los archivos en el futuro sin tener que introducir una contraseña ni pedírselo al administrador.
- Si el equipo se encuentra dentro de la red corporativa y Kaspersky Endpoint Security está instalado en el equipo, obtendrá acceso al dispositivo sin tener que introducir una contraseña. Kaspersky Endpoint Security

recibirá la clave secreta del Servidor de Administración de Kaspersky Security Center al que está conectado el equipo.

## Recuperar la contraseña para trabajar en el modo portátil

Si ha olvidado la contraseña para trabajar en el modo portátil, tiene que conectar la unidad extraíble a un equipo con Kaspersky Endpoint Security instalado dentro de la red corporativa. Obtendrá acceso a los archivos porque la clave secreta se guarda en el almacén de claves del equipo o en el Servidor de administración. Descifre y vuelva a cifrar archivos con una nueva contraseña.

## Características del modo portátil al conectar una unidad extraíble a un equipo desde otra red

Si el equipo se encuentra fuera de la red corporativa y Kaspersky Endpoint Security está instalado en el equipo, puede acceder a los archivos de las siguientes maneras:

- **Acceso basado en contraseña**

Después de introducir la contraseña, podrá ver, modificar y guardar archivos en la unidad extraíble (*acceso transparente*). Kaspersky Endpoint Security puede establecer un derecho de acceso de solo lectura para una unidad extraíble si los siguientes parámetros están definidos en la configuración de la directiva para el cifrado de unidades extraíbles:

- La compatibilidad con el modo portátil está desactivado.
- El modo **Cifrar todos los archivos** o **Cifrar solo archivos nuevos** está seleccionado.

En todos los demás casos, obtendrá acceso completo a la unidad extraíble (permiso de lectura/escritura). Podrá añadir y eliminar archivos.

Puede cambiar los permisos de acceso a la unidad extraíble incluso cuando esta está conectada al equipo. Si se cambian los permisos de acceso a la unidad extraíble, Kaspersky Endpoint Security bloqueará el acceso a los archivos y le pedirá la contraseña de nuevo.

Después de introducir la contraseña, no puede aplicar la configuración de la directiva de cifrado para la unidad extraíble. En este caso, resulta imposible descifrar o volver a cifrar archivos en la unidad extraíble.

- **Solicitar al administrador acceso a los archivos**

Si ha olvidado la contraseña para trabajar en el modo portátil, solicite al administrador acceso a los archivos. Para acceder a los archivos, el usuario debe enviar al administrador un archivo de solicitud de acceso (un archivo con la extensión KESDC). El usuario puede enviar el archivo de solicitud de acceso por correo electrónico, por ejemplo. El administrador enviará un archivo de acceso a datos cifrados (un archivo con la extensión KESDR).

Después de completar el procedimiento de recuperación de contraseña de solicitud-respuesta, recibirá acceso transparente a los archivos de la unidad extraíble y acceso completo a la unidad extraíble (permiso de lectura/escritura).

Puede aplicar una directiva de cifrado de la unidad extraíble y descifrar archivos, por ejemplo. Después de recuperar la contraseña, o cuando se actualice la directiva, Kaspersky Endpoint Security le pedirá que confirme los cambios.

[Cómo obtener un archivo de acceso a datos cifrados en la Consola de administración \(MMC\)](#) 

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a datos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione **Conceder acceso en modo sin conexión**.
6. En la ventana de diálogo que se abre, seleccione la pestaña **Cifrado de datos**.
7. En la pestaña **Cifrado de datos**, haga clic en el botón **Examinar**.
8. En la ventana para seleccionar un archivo de solicitud de acceso, especifique la ruta al archivo recibido del usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.

### [Cómo obtener un archivo de acceso a datos cifrados en Web Console <sup>?</sup>](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Seleccione la casilla de verificación junto al nombre del equipo a cuyos datos quiere restaurar el acceso.
3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.
4. Seleccione la sección **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión KESDC).  
Web Console mostrará información sobre la solicitud. Esto incluirá el nombre del equipo en el que el usuario solicita acceso al archivo.
6. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión KESDR).

Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

## Descifrado de unidades extraíbles

Puede usar una directiva para descifrar una unidad extraíble. Se genera una directiva con configuraciones definidas para el cifrado de unidades extraíbles para un grupo de administración específico. Por lo tanto, el resultado del descifrado de los datos en las unidades extraíbles depende del equipo con el cual la unidad extraíble está conectada.



Para descifrar unidades extraíbles:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Cifrado de datos** → **Cifrado de unidades extraíbles**.
6. Si desea descifrar todos los archivos cifrados almacenados en las unidades extraíbles, en la lista desplegable **Modo de cifrado**, seleccione **Descifrar toda la unidad extraíble**.
7. Para descifrar los datos que se almacenan en unidades extraíbles individuales, modifique las reglas de cifrado de las unidades extraíbles cuyos datos desea descifrar. Para ello:
  - a. En la lista de unidades extraíbles para las cuales se han configurado reglas de cifrado, seleccione la entrada correspondiente a la unidad extraíble pertinente.
  - b. Haga clic en el botón **Establecer una regla** para modificar la regla de cifrado de la unidad extraíble seleccionada.
  - c. En el menú contextual del botón **Establecer una regla**, haga clic en **Descifrar toda la unidad extraíble**.
8. Guarde los cambios.

Como resultado, si un usuario conecta una unidad extraíble o si ya está conectada, Kaspersky Endpoint Security descifra la unidad extraíble. La aplicación advierte al usuario de que el proceso de descifrado puede tardar un tiempo. Si el usuario inicia la extracción segura de una unidad extraíble durante el descifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de descifrado de datos y permite la extracción de la unidad extraíble antes de que la operación de descifrado haya finalizado. El proceso de descifrado se reanuda cuando el usuario conecte la unidad nuevamente al equipo.

Si el proceso de descifrado de una unidad extraíble falla, puede ver el informe **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Es posible que otra aplicación bloquee el acceso a los archivos. En tal caso, pruebe a desconectar la unidad extraíble del equipo y volver a conectarla.

## Visualización de los detalles del cifrado de datos

Mientras que las tareas de cifrado y descifrado están en curso, Kaspersky Endpoint Security envía a Kaspersky Security Center información sobre el estado de los parámetros del cifrado aplicados a los equipos cliente.

Se pueden dar los siguientes valores del estado del cifrado:

- *Directiva de cifrado no definida*. No se ha definido una directiva de cifrado de Kaspersky Security Center para el equipo.
- *Aplicar directiva*. El cifrado y el descifrado de datos está en curso en el equipo.

- *Error*. Se ha producido un error durante el cifrado o descifrado de datos del equipo.
- *Reinicio necesario*. El sistema operativo tiene que ser reanudado para iniciar o acabar el cifrado o el descifrado de los datos en el equipo.
- *De conformidad con la directiva*. El cifrado de datos en el equipo se ha terminado usando la configuración de cifrado especificada en la directiva de Kaspersky Security Center aplicada al equipo.
- *Cancelada por el usuario*. El usuario ha rechazado confirmar la operación de cifrado del archivo en la unidad extraíble.

## Ver el estado de cifrado

*Para ver el estado del cifrado de los datos del equipo:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos** del espacio de trabajo, mueva la barra de desplazamiento hacia la derecha.
5. Si la columna **Estado de cifrado** no se muestra:
  - a. Haga clic con el botón derecho del ratón para abrir el menú contextual del encabezamiento de la tabla.
  - b. En el menú contextual, en la lista desplegable **Ver**, seleccione **Añadir/Quitar columnas**.
  - c. En la ventana que se abre, marque la casilla **Estado de cifrado**.
  - d. Haga clic en **Aceptar**.

La columna **Estado de cifrado** muestra el estado del cifrado de los datos de los equipos que pertenecen al grupo de administración seleccionado. Este estado se forma según la información sobre el cifrado del archivo en unidades de disco locales del equipo y sobre el cifrado de disco completo.

## Ver las estadísticas del cifrado en los paneles de Kaspersky Security Center

*Para ver el estado del cifrado en los paneles de Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione el nodo **Servidor de administración**.
3. En el espacio de trabajo situado a la derecha del árbol de la consola de administración, seleccione la pestaña **Estadísticas**.
4. Cree una nueva página con paneles de información que contengan estadísticas de cifrado de datos. Para ello:
  - a. En la pestaña **Estadísticas**, haga clic en el botón **Personalizar vista**.

- b. En la ventana abierta, haga clic en el botón **Añadir**.
- c. En la ventana que se abre, en la sección **General**, escriba el nombre de la página.
- d. En la sección **Paneles de información**, haga clic en el botón **Añadir**.
- e. En la ventana abierta, en el grupo **Estado de la protección**, seleccione el elemento **Cifrado de dispositivos**.
- f. Haga clic en **Aceptar**.
- g. Si es necesario, edite la configuración del panel de detalles. Para esto, utilice las secciones **Ver** y **Dispositivos**.
- h. Haga clic en **Aceptar**.
- i. Repita los pasos d-h del proceso, seleccionando el elemento **Cifrado de unidades extraíbles** en la sección **Estado de la protección**.  
Los paneles de detalles añadidos aparecen en la lista de **Paneles de información**.
- j. Haga clic en **Aceptar**.  
El nombre de la página con los paneles de detalles creados en los pasos anteriores aparece en la lista **Páginas**.
- k. Haga clic en el botón **Cerrar**.

5. En la pestaña **Estadísticas**, abra la página que se creó en los pasos anteriores de las instrucciones.

Aparecen los paneles de información que muestran el estado del cifrado de los equipos y de las unidades extraíbles.

## Ver errores de cifrado de archivos en unidades del equipo local

*Para ver los errores del cifrado del archivo en unidades del equipo local:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el nombre del equipo en la lista y haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual del equipo, seleccione el elemento **Propiedades**. En la ventana que se abre, seleccione la sección **Protección**.
6. Haga clic en el enlace **Ver errores de cifrado de datos** para abrir la ventana **Errores de cifrado de datos**.

Esta ventana muestra la información de los errores de cifrado de archivos de las unidades del equipo local. Cuando se corrige un error, Kaspersky Security Center elimina la información del error de la ventana **Errores de cifrado de datos**.

## Visualización del informe del cifrado de datos

Para ver el informe del cifrado de datos:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.  
Se inicia el Asistente de nueva plantilla de informe.
4. Siga los pasos del Asistente de plantillas de informe. En la ventana **Selección del tipo de plantilla de informe** de la sección **Otro**, seleccione uno de los siguientes elementos:
  - **Informe sobre el estado del cifrado de los dispositivos administrados.**
  - **Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo.**
  - **Informe sobre errores en el cifrado de archivos.**
  - **Informe sobre el bloqueo del acceso a archivos cifrados.**

Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.

5. Seleccione la plantilla del informe que se creó en los pasos anteriores de las instrucciones.
6. En el menú contextual de la plantilla, seleccione **Mostrar informe**.

Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

## Trabajar con dispositivos cifrados cuando no hay acceso a estos

### Obtener acceso a los dispositivos cifrados

Es posible que se requiera a un usuario solicitar acceso a dispositivos cifrados en los siguientes casos:

- El disco duro se cifró en un equipo diferente.
- La clave de cifrado para un dispositivo no está en el equipo (por ejemplo, después del primer intento de acceder a la unidad extraíble cifrada en el equipo), y el equipo no está conectado a Kaspersky Security Center.  
Después de que el usuario ha aplicado la clave de acceso al dispositivo cifrado, Kaspersky Endpoint Security guarda la clave de cifrado en el equipo del usuario y permite el acceso a este dispositivo después de sucesivos intentos de acceso, incluso si no hay conexión con Kaspersky Security Center.

El acceso a dispositivos cifrados se puede obtener de la siguiente manera:

1. El usuario usa la interfaz de aplicación Kaspersky Endpoint Security para crear un archivo de solicitud de acceso con la extensión kesdc y lo envía al administrador de la red de área local corporativa.

2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo clave de acceso con la extensión kesdr y lo envía al usuario.
3. El usuario aplica la clave de acceso.

## Restauración de datos de dispositivos cifrados

Un usuario puede usar la [Utilidad de restauración de dispositivos cifrados](#) (denominada en lo sucesivo la Utilidad de restauración) para trabajar con dispositivos cifrados. Esto se puede requerir en los siguientes casos:

- Falló el procedimiento para usar una clave de acceso para obtener acceso.
- Los componentes de cifrado no se han instalado en el equipo con el dispositivo cifrado.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración permanecen durante un tiempo sin cifrar en la memoria del equipo del usuario. Para reducir el riesgo de acceso no autorizado a estos datos, se aconseja restaurar el acceso a dispositivos cifrados en equipos de confianza.

Los datos en dispositivos cifrados se pueden restaurar de la siguiente manera:

1. El usuario usa la Utilidad de restauración para crear un archivo de solicitud de acceso con la extensión fdertc y lo envía al administrador de la red de área local corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo clave de acceso con la extensión fdertr y lo envía al usuario.
3. El usuario aplica la clave de acceso.

Para restaurar datos de discos duros de sistemas cifrados, el usuario también puede especificar las credenciales de la cuenta del Agente de autenticación en la Utilidad de restauración. Si los metadatos de la cuenta del Agente de autenticación están dañados, el usuario debe completar el procedimiento de restauración con un archivo de solicitud de acceso.

Antes de restaurar los datos en los dispositivos cifrados, se recomienda cancelar la directiva de Kaspersky Security Center o desactivar el cifrado en la configuración de la directiva de Kaspersky Security Center en el equipo donde el procedimiento se realizará. Esto evita que el dispositivo vuelva a cifrarse.

## Recuperación de datos mediante la Utilidad de restauración FDERT

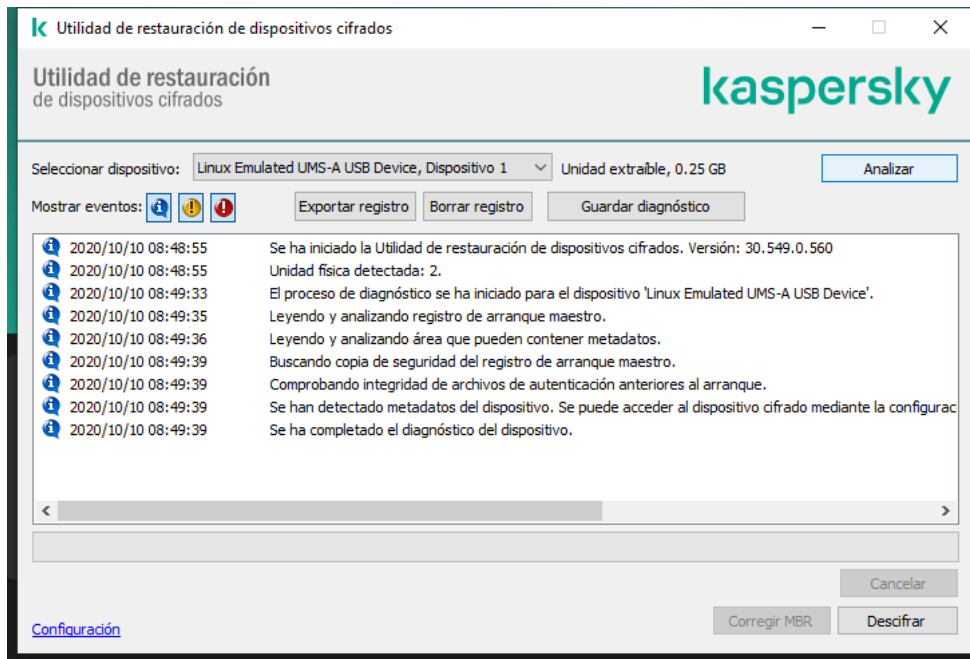
Si el disco duro falla, el sistema de archivos podría estar dañado. Si es así, los datos protegidos por la tecnología Cifrado de disco de Kaspersky no estará disponible. Puede descifrar los datos y copiarlos a una nueva unidad.

La recuperación de datos de un disco duro protegido por la tecnología Cifrado de disco de Kaspersky consta de los siguientes pasos:

1. Cree una Utilidad de restauración independiente (vea la imagen más abajo).
2. Conecte una unidad a un equipo que no tenga instalados los componentes de cifrado de Kaspersky Endpoint Security.

3. Ejecute la Utilidad de restauración y diagnostique el disco duro.


4. Acceda a los datos del disco. Para hacerlo, introduzca las credenciales del Agente de autenticación o inicie el procedimiento de recuperación (solicitud-respuesta).



Utilidad de restauración FDERT

## Creación de una Utilidad de restauración independiente

*Para crear el archivo ejecutable de la Utilidad de restauración:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Restaurar dispositivo cifrado**.  
Se ejecuta la Utilidad de restauración de dispositivos cifrados.
3. Haga clic en el botón **Crear Utilidad de restauración independiente** de la ventana de la Utilidad de restauración.
4. Guarde la Utilidad de restauración independiente en la memoria del equipo.

Como resultado, el archivo ejecutable de la Utilidad de restauración (fdert.exe) se guardará en la carpeta especificada. Copie la Utilidad de restauración a un equipo que no tenga los componentes de cifrado de Kaspersky Endpoint Security. Esto evita que la unidad vuelva a cifrarse.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración permanecen durante un tiempo sin cifrar en la memoria del equipo del usuario. Para reducir el riesgo de acceso no autorizado a estos datos, se aconseja restaurar el acceso a dispositivos cifrados en equipos de confianza.

## Recuperación de los datos de un disco duro

*Para restaurar el acceso a un dispositivo cifrado por medio de la Utilidad de restauración:*

1. Ejecute el archivo con el nombre `fdert.exe`, que es el archivo ejecutable de la Utilidad de restauración. Kaspersky Endpoint Security crea este archivo.

2. En la ventana Utilidad de restauración, seleccione el dispositivo cifrado al que desea restaurar el acceso.

3. Haga clic en el botón **Analizar** para permitir a la utilidad definir qué acciones se deben llevar a cabo en el dispositivo: si se debe desbloquear o descifrar.

Si el equipo tiene acceso a la funcionalidad de cifrado de Kaspersky Endpoint Security, la Utilidad de restauración le pedirá a usted que desbloquee el dispositivo. Aunque el desbloqueo de un dispositivo no lo descifra, puede accederse a este directamente como consecuencia de estar desbloqueado. Si el equipo no tiene acceso a la funcionalidad de cifrado de Kaspersky Endpoint Security, la Utilidad de restauración le pedirá a usted que descifre el dispositivo.

4. Si desea importar información de diagnóstico, haga clic en el botón **Guardar diagnóstico**.

La utilidad guardará un archivo comprimido con los archivos que contienen la información de diagnóstico.

5. Haga clic en el botón **Corregir MBR** si el diagnóstico del disco duro del sistema cifrado ha devuelto un mensaje acerca de que hay problemas relacionados con el registro de arranque principal (MBR) del dispositivo.

Reparar el registro de arranque maestro puede reducir el tiempo que requiere obtener la información necesaria para desbloquear o descifrar el dispositivo.

6. Haga clic en el botón **Desbloquear** o **Descifrar**, según los resultados del diagnóstico.

7. Si desea restaurar los datos utilizando una cuenta del Agente de autenticación, seleccione la opción **Utilizar la configuración de la cuenta del Agente de autenticación** e introduzca las credenciales del Agente de autenticación.

Este método solo es posible al restaurar datos en un disco duro del sistema. Si el disco duro del sistema está dañado y los datos de la cuenta del Agente de autenticación se han perdido, debe obtener una clave de acceso del administrador de la red de área local corporativa para restaurar datos en un dispositivo cifrado.

8. Si desea comenzar el procedimiento de recuperación, haga lo siguiente:

a. Seleccione la opción **Especificar la clave de acceso al dispositivo manualmente**.

b. Haga clic en el botón **Recibir la clave de acceso** y guarde el archivo de solicitud de acceso en la memoria del equipo (un archivo con la extensión `FDERTC`).

c. Envíe el archivo de solicitud de acceso al administrador de la red de área local corporativa.

No cierre la ventana **Recibir clave de acceso al dispositivo** hasta que haya recibido la clave de acceso. Si esta ventana se abre de nuevo, no podrá aplicar la clave de acceso que el administrador había creado anteriormente.

d. Reciba y guarde el archivo de acceso (un archivo con la extensión `FDERTR`) que creó y le proporcionó el administrador de la red de área local corporativa (consulte las instrucciones más abajo).

e. Descargue el archivo de acceso en la ventana **Recibir clave de acceso al dispositivo**.

9. Si está descifrando un dispositivo, debe configurar ajustes de descifrado adicionales.

- Especificar el área que se debe descifrar:

- Si desea descifrar el dispositivo completo, seleccione la opción **Descifrar todo el dispositivo**.

- Si desea descifrar una parte de los datos de un dispositivo, seleccione la opción **Descifrar áreas individuales del dispositivo** y especifique los límites de la parte que se va a descifrar.
- Seleccione la ubicación para escribir los datos descifrados:
  - Si desea que los datos del dispositivo original se vuelvan a escribir con los datos descifrados, anule la selección de la casilla de selección **Descifrar en un archivo de imagen de disco**.
  - Si desea guardar los datos descifrados por separado de los datos cifrados originales, seleccione la casilla de selección **Descifrar en un archivo de imagen de disco** y el botón **Examinar** para especificar la ruta donde desea guardar el archivo VHD.

10. Haga clic en **Aceptar**.

Comienza el proceso de descifrado o desbloqueo.

### [Cómo crear un archivo de acceso a datos cifrados en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Protección y cifrado de datos** → **Dispositivos cifrados**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que desea crear un archivo de clave de acceso. Luego, en el menú contextual del dispositivo, haga clic en **Obtener acceso para el dispositivo en Kaspersky Endpoint Security para Windows**.

Si no está seguro de para qué equipo se generó el archivo de solicitud de acceso, en el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Protección y cifrado de datos** y, en el espacio de trabajo, haga clic en el enlace **Obtener clave de cifrado del dispositivo en Kaspersky Endpoint Security para Windows**.

4. En la ventana de diálogo que se abre, seleccione el algoritmo de cifrado que quiere usar: **AES256** o **AES56**.

El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: están disponibles tanto la variante de *cifrado "fuerte"* (**AES256**) como la de *cifrado "ligero"* (**AES56**). La biblioteca de cifrado AES se instala junto con la aplicación.

5. Haga clic en **Examinar** para abrir una ventana. En esta ventana, especifique la ruta al archivo de solicitud con la extensión **fdertc** que se recibió del usuario.
6. Haga clic en el botón **Abrir**.

Verá información sobre la solicitud del usuario. Kaspersky Security Center genera un archivo clave. Envíe el archivo clave de acceso a datos cifrados generado al usuario por correo electrónico. O guarde el archivo de acceso y utilice cualquier método disponible para transferir el archivo.

### [Cómo crear un archivo de acceso a datos cifrados en Web Console](#)



1. En la ventana principal de Web Console, seleccione **Operaciones** → **Protección y cifrado de datos** → **Dispositivos cifrados**.
  2. Seleccione la casilla de verificación junto al nombre del equipo del que quiere recuperar los datos.
  3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.  
Se iniciará el Asistente para otorgar acceso a un dispositivo.
  4. Siga las instrucciones del Asistente para otorgar acceso a un dispositivo:
    - a. Seleccione el complemento **Kaspersky Endpoint Security para Windows**.
    - b. Seleccione el algoritmo de cifrado que quiere usar: **AES256** o **AES56**.  
El algoritmo de cifrado de datos depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución: están disponibles tanto la variante de *cifrado "fuerte"* (**AES256**) como la de *cifrado "ligero"* (**AES56**). La biblioteca de cifrado AES se instala junto con la aplicación.
    - c. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que recibió del usuario (un archivo con la extensión FDERTC).
    - d. Haga clic en el botón **Guardar clave** y seleccione una carpeta para guardar el archivo clave de acceso a datos cifrados (un archivo con la extensión FDERTR).
- Como resultado, podrá obtener la clave de acceso a datos cifrados, que tendrá que transferir al usuario.

## Creación de un disco de rescate del sistema operativo

El disco de rescate del sistema operativo puede ser útil cuando no se puede acceder a un disco duro cifrado por alguna razón y el sistema operativo no se puede cargar.

Puede cargar una imagen del sistema operativo Windows por medio del disco de rescate y restaurar el acceso al disco duro cifrado por medio de la Utilidad de restauración incluida en la imagen del sistema operativo.

*Para crear un disco de rescate del sistema operativo:*

1. [Cree un archivo ejecutable para la Utilidad de restauración de dispositivos cifrados](#).
2. Cree una imagen personalizada del entorno de prearranque de Windows. Mientras tanto, añada el archivo ejecutable de la Utilidad de restauración a la imagen.
3. Guardar la imagen personalizada del entorno de preinstalación de Windows en medios de arranque como, por ejemplo, un lector de CD o una unidad extraíble.

Consulte los archivos de ayuda de Microsoft para recibir instrucciones sobre la creación de una imagen personalizada del entorno de prearranque de Windows (por ejemplo, en el [recurso Microsoft TechNet](#)).

## Componentes de Detection and Response.

Kaspersky Endpoint Security admite soluciones de Detection and Response usando un agente integrado. Para utilizar Detection and Response, debe habilitar la integración con estas soluciones al instalar la aplicación. El agente integrado es compatible con:

- Kaspersky Managed Detection and Response (MDR);
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum);
- Kaspersky Endpoint Detection and Response Expert (EDR Expert);
- Kaspersky Sandbox 2.0.

Kaspersky Endpoint Security también incluye el kit de distribución de Kaspersky Endpoint Agent. Kaspersky Endpoint Agent es compatible con Kaspersky Anti Targeted Attack Platform (el componente Endpoint Detection and Response Expert [KATA EDR]). Para instalar Kaspersky Endpoint Agent, debe seleccionar el componente Endpoint Agent al instalar la aplicación.

No puede seleccionar el agente incorporado y el Agente Kaspersky Endpoint Agent al instalar la aplicación. Si necesita instalar tanto el agente incorporado como Kaspersky Endpoint Agent, instale Kaspersky Endpoint Agent por separado.

Puede utilizar la solución Kaspersky Endpoint Security with Detection and Response en diferentes configuraciones, por ejemplo, [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

## Kaspersky Endpoint Agent

*Kaspersky Endpoint Agent* admite la interacción entre la aplicación y otras soluciones de Kaspersky para detectar amenazas avanzadas (por ejemplo Kaspersky Sandbox). Las soluciones de Kaspersky son compatibles con versiones determinadas de Kaspersky Endpoint Agent.

Para utilizar Kaspersky Endpoint Agent como parte de las soluciones de Kaspersky, debe activar dichas soluciones con la correspondiente clave de licencia.

Para obtener información completa sobre Kaspersky Endpoint Agent para Windows incluido en la solución de software que está utilizando y para obtener información completa sobre la solución independiente, consulte la Guía de ayuda del producto correspondiente:

- *Ayuda de la plataforma Kaspersky Anti Targeted Attack*
- *Ayuda de Kaspersky Sandbox*
- *Ayuda de Kaspersky Endpoint Detection and Response Optimum*
- *Ayuda de Kaspersky Managed Detection and Response*

Kaspersky Endpoint Agent se incluye en el [Kit de distribución de Kaspersky Endpoint Security](#). Puede instalar Kaspersky Endpoint Agent durante la instalación de Kaspersky Endpoint Security. Para ello, debe seleccionar el componente Endpoint Agent durante la instalación de la aplicación (por ejemplo, en el [paquete de instalación](#)). Después de instalar la aplicación con Endpoint Agent, Kaspersky Endpoint Security y Kaspersky Endpoint Agent se añadirán a la lista de aplicaciones instaladas. Después de desinstalar Kaspersky Endpoint Security, Kaspersky Endpoint Agent también se desinstalará automáticamente.

El kit de distribución del Agente de Kaspersky Endpoint forma parte del kit de distribución de Kaspersky Endpoint Security para Windows.

Correspondencia de las versiones KES y KEA

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

## Migración de directivas y tareas para Kaspersky Endpoint Agent

Ahora, Kaspersky Endpoint Security 11.7.0 cuenta con un agente para la migración desde Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Puede migrar la configuración de directivas y tareas para las siguientes soluciones:

- Kaspersky Sandbox.
- Kaspersky Endpoint Detection and Response (EDR);
- Kaspersky Managed Detection and Response (MDR).

Se recomienda comenzar con la migración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security en un solo ordenador, luego, en un grupo de ordenadores y después completar la migración en todos los ordenadores de la organización.

*Para migrar la configuración de directivas y tareas de Kaspersky Endpoint Agent a Kaspersky Endpoint Security, haga lo siguiente:*

En la ventana principal de Web Console, seleccione **Operaciones** → **Migración desde Kaspersky Endpoint Agent**.

Esto ejecuta el Asistente de migración de directivas y tareas. Siga las instrucciones del Asistente.

### Paso 1. Migración de directivas

El Asistente de migración crea una directiva nueva que combina las configuraciones de las directivas de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. En la lista de directivas, seleccione las directivas de Kaspersky Endpoint Agent cuyas configuraciones desee unir con la directiva de Kaspersky Endpoint Security. Haga clic en una directiva de Kaspersky Endpoint Agent para seleccionar la directiva de Kaspersky Endpoint Security con la que desea unir la configuración. Asegúrese de que haya seleccionado las directivas correctas y vaya al siguiente paso.

## Paso 2. Migración de tareas

El Asistente de migración crea tareas nuevas para Kaspersky Endpoint Security. En la lista de tareas, seleccione las tareas de Kaspersky Endpoint Agent que desee crear para la directiva de Kaspersky Endpoint Security. El asistente admite tareas para Kaspersky Endpoint Detection and Response y Kaspersky Sandbox. Ir al paso siguiente.

## Paso 3: Fin del asistente

Salga del Asistente. Como resultado, el asistente realiza lo siguiente:

- Crea una directiva de Kaspersky Endpoint Security.

La directiva une la configuración de Kaspersky Endpoint Security y Kaspersky Endpoint Agent. La directiva se denomina *<nombre de la directiva de Kaspersky Endpoint Security>* y *<nombre de la directiva de Kaspersky Endpoint Agent>*. La directiva nueva tiene el estado *Inactivo*. Para continuar, cambie los estados de las directivas de Kaspersky Endpoint Agent y Kaspersky Endpoint Security a *Inactivo* y active la directiva nueva y combinada.

Después de realizar la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, asegúrese de que la directiva nueva tenga configurada [la funcionalidad para la transferencia de datos al Servidor de administración](#) (datos del archivo en cuarentena y datos de la cadena de desarrollo de la amenaza). Los valores de parámetros de la transferencia de datos no se migran desde una directiva de Kaspersky Endpoint Agent.

- Se crean tareas nuevas de Kaspersky Endpoint Security.

Las tareas nuevas son copias de las tareas de Kaspersky Endpoint Agent para Kaspersky Endpoint Detection and Response y Kaspersky Sandbox. Al mismo tiempo, el Asistente deja las tareas de Kaspersky Endpoint Agent sin cambios.

## Migrar la configuración [KES + KEA] a la configuración [KES + agente incorporado]

Ahora Kaspersky Endpoint Security 11.7.0 tiene agentes integrados para las soluciones Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) y Kaspersky Sandbox 2.0. Ya no necesita una aplicación diferente de Kaspersky Endpoint Agent para trabajar con estas soluciones. Cuando actualiza Kaspersky Endpoint Security a la versión 11.7.0, las soluciones EDR Optimum y Kaspersky Sandbox continúan trabajando con Kaspersky Endpoint Security. Asimismo, Kaspersky Endpoint Agent se elimina del ordenador.

La migración de la configuración de [KES + KEA] a [KES + agente incorporado] implica los siguientes pasos:

### 1 Actualizar Kaspersky Security Center

Actualizar todos los componentes de Kaspersky Security Center a la versión 13.2, incluidos el Agente de administración en ordenadores de usuarios y Web Console.

## 2 Actualizar el complemento web de Kaspersky Endpoint Security

En Kaspersky Security Center Web Console, actualizar el complemento web de Kaspersky Endpoint Security a la versión 11.7.0. Para administrar los componentes EDR Optimum y Kaspersky Sandbox, debe usar Web Console.

## 3 Migrar las directivas y tareas

Use el [Asistente de migración de directivas y tareas de Kaspersky Endpoint Agent](#) para migrar la configuración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows.

Esto crea una nueva directiva de Kaspersky Endpoint Security. La directiva nueva tiene el estado *Inactivo*. Para aplicar la directiva, abra las propiedades de la directiva, acepte la Declaración de Kaspersky Security Network y configure el estado a *Activo*.

## 4 Funcionalidad de licencias

Si utiliza una licencia común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Agent, la funcionalidad EDR Optimum se activa de manera automática después de actualizar la aplicación a la versión 11.7.0. No necesita realizar ninguna otra acción.

Si utiliza una licencia independiente adicional de Kaspersky Endpoint Detection and Response Optimum para activar la funcionalidad EDR Optimum, debe asegurarse de que la clave de EDR Optimum se añada al repositorio de Kaspersky Security Center y de que [la funcionalidad de distribución automática de claves de licencia esté activada](#). Después de actualizar la aplicación a la versión 11.7.0, la funcionalidad EDR Optimum se activa de manera automática.

Si utiliza una licencia de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security para activar Kaspersky Endpoint Agent, y una licencia diferente para activar Kaspersky Endpoint Security para Windows, debe reemplazar la clave para Kaspersky Endpoint Security para Windows con la clave común de Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. Puede reemplazar la clave con la tarea [Añadir clave](#).

No necesita activar la funcionalidad Kaspersky Sandbox. Kaspersky Sandbox estará disponible de forma inmediata después de actualizar y activar Kaspersky Endpoint Security para Windows.

## 5 Actualizar la aplicación de Kaspersky Endpoint Security

Para actualizar la aplicación y migrar las funcionalidades EDR Optimum y Kaspersky Sandbox, se recomienda usar una [tarea de instalación remota](#).

Para actualizar la aplicación mediante una tarea de instalación remota, debe modificar las siguientes configuraciones:

- Seleccione los componentes Endpoint Detection and Response Optimum o Kaspersky Sandbox en la configuración del paquete de instalación.
- Excluya el componente Kaspersky Endpoint Agent en la configuración del paquete de instalación.

También puede actualizar la aplicación con los siguientes métodos:

- Utilizando el servicio de actualización de Kaspersky (Seamless Update - SMU).
- De forma local, utilizando el Asistente de instalación.

En este caso, debe revisar la configuración de Kaspersky Endpoint Agent que se encuentra instalada en el ordenador. Si el Kaspersky Endpoint Agent instalado incluye el componente Endpoint Detection and Response Expert (KATA EDR), elimine el componente antes de actualizar la aplicación. Si no puede eliminar el componente Endpoint Detection and Response Expert (KATA EDR), Kaspersky Endpoint Security no incluirá los componentes EDR Optimum ni Kaspersky Sandbox al actualizar la aplicación. Puede instalar componentes con la tarea [Cambiar componentes de la aplicación](#) después de actualizar la aplicación.

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 activas de las soluciones de Kaspersky. Por lo tanto, si el equipo tiene, por ejemplo, Kaspersky Endpoint Agent instalado y la solución EDR Optimum activada, el instalador de Kaspersky Endpoint Security configura automáticamente el conjunto de componentes y selecciona el componente EDR Optimum. Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina el Agente de Kaspersky Endpoint. La ejecución del instalador MSI con la cuenta del sistema (SYSTEM) se realiza normalmente cuando se actualiza a través del servicio de actualización de Kaspersky (SMU) o cuando se despliega un paquete de instalación a través de Kaspersky Security Center.

Si está actualizando Kaspersky Endpoint Security con un archivo MSI en una cuenta de usuario sin privilegios, Kaspersky Endpoint Security no tendrá acceso a las licencias activas de las soluciones de Kaspersky. En este caso, Kaspersky Endpoint Security selecciona automáticamente los componentes según la configuración del Agente de Kaspersky Endpoint de la siguiente manera:

- Si el componente Endpoint Detection and Response Expert (KATA EDR) está instalado, Kaspersky Endpoint Security selecciona el componente Endpoint Agent. Kaspersky Endpoint Security selecciona solo el componente Endpoint Agent, incluso si Kaspersky Endpoint Agent tiene otros componentes instalados, por ejemplo la configuración [KATA EDR + KSB].
- Si el componente Kaspersky Sandbox, EDR Optimum o la configuración [Kaspersky Sandbox + EDR Optimum] está instalado, Kaspersky Endpoint Security selecciona los componentes correspondientes. Esto hace que Kaspersky Endpoint Security pase a utilizar el agente incorporado y elimina el Agente de Kaspersky Endpoint.

## 6 Reinicio del equipo

Reinicie el equipo para terminar de actualizar la aplicación con el agente incorporado. Al actualizar la aplicación, el instalador elimina Kaspersky Endpoint Agent antes de reiniciar el equipo. Después de reiniciar el equipo, el instalador añade el agente incorporado. Esto significa que Kaspersky Endpoint Security no realiza las funciones de EDR y Kaspersky Sandbox hasta que no se reinicia el equipo.

## 7 Revisar el estado de Kaspersky Endpoint Detection and Response Optimum y Kaspersky Sandbox

Si, después de la actualización, el ordenador tiene el estado *Crítico* en la consola de Kaspersky Security Center, haga lo siguiente:

- Asegúrese de que el ordenador tenga el Agente de administración 13.2 instalado.
- Verifique el estado de funcionamiento de los componentes EDR Optimum y Kaspersky Sandbox en el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No instalado*, instale los componentes con la tarea [Cambiar los componentes de la aplicación](#).
- Asegúrese de aceptar la Declaración de Kaspersky Security Network en la directiva nueva de Kaspersky Endpoint Security para Windows.

Asegúrese de que la funcionalidad EDR Optimum esté activada, mediante el *Informe sobre el estado de los componentes de la aplicación*. Si un componente tiene el estado *No cubierto por una licencia*, asegúrese de que [la funcionalidad de distribución automática de claves de licencia de EDR Optimum esté activada](#).

## Actualización de la aplicación como parte de KATA EDR

Si tiene Kaspersky Endpoint Agent instalado para la integración con Kaspersky Anti Targeted Attack Platform (el componente de Endpoint Detection and Response Expert [KATA EDR]), puede actualizar Kaspersky Endpoint Security para Windows de las siguientes maneras:

- Con una tarea de instalación remota.

Para hacerlo, debe modificar las siguientes configuraciones:

- Excluir los componentes Endpoint Detection and Response Optimum y Kaspersky Sandbox en la configuración del paquete de instalación.
- Seleccionar el componente Kaspersky Endpoint Agent en la configuración del paquete de instalación. Si el ordenador ya tiene Kaspersky Endpoint Agent instalado, la aplicación se actualiza a la versión 3.11.
- Usando el servicio de actualización de Kaspersky (SMU).  
Para hacerlo, debe confirmar la actualización de la aplicación. Kaspersky Endpoint Security excluye Endpoint Detection and Response Optimum y Kaspersky Sandbox de la instalación. No se admite la actualización de Kaspersky Endpoint Agent. Puede actualizar Kaspersky Endpoint Agent manualmente.
- De forma local, utilizando el Asistente de instalación.  
Kaspersky Endpoint Security excluye Endpoint Detection and Response Optimum y Kaspersky Sandbox de la instalación. Si el ordenador ya tiene Kaspersky Endpoint Agent instalado, la aplicación se actualiza a la versión 3.11.

## Managed Detection and Response



Kaspersky Endpoint Security 11.6.0 presenta el agente integrado para la solución Managed Detection and Response. La solución *Kaspersky Managed Detection and Response (MDR)* detecta y analiza automáticamente los incidentes de seguridad en su infraestructura. Para hacerlo, MDR utiliza datos de telemetría recibidos de endpoints y aprendizaje automático. MDR envía datos de incidentes a los expertos de Kaspersky. Luego, los expertos pueden procesar el incidente y, por ejemplo, añadir una nueva entrada a las bases de datos antivirus. De manera alternativa, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aisle el equipo de la red. Para obtener información detallada sobre cómo funciona la solución, consulte la [Ayuda de Kaspersky Managed Detection and Response](#).

## Integración con MDR

Para configurar la integración con Kaspersky Managed Detection and Response, debe activar el componente Managed Detection and Response y configurar Kaspersky Endpoint Security.

El componente Managed Detection and Response no es compatible con el componente Endpoint Detection and Response Expert.

Debe activar los siguientes componentes para que Managed Detection and Response funcione:

- [Kaspersky Security Network \(modo ampliado\)](#).
- [Detección de comportamiento](#).

La activación de estos componentes no es opcional. De lo contrario, Kaspersky Managed Detection and Response no puede funcionar porque no recibe los datos de telemetría necesarios.

Además, Kaspersky Managed Detection and Response usa datos recibidos de otros componentes de la aplicación. La activación de estos componentes es opcional. Los componentes que proporcionan datos adicionales incluyen los siguientes:

- [Protección frente a amenazas web.](#)
- [Protección frente a amenazas en el correo.](#)
- [Firewall.](#)

Para que Kaspersky Managed Detection and Response funcione con el Servidor de administración a través de Kaspersky Security Center Web Console, también debe establecer una conexión nueva y segura, una *conexión en segundo plano*. Kaspersky Managed Detection and Response le solicita que establezca una conexión en segundo plano cuando despliega la solución. Asegúrese de que la conexión en segundo plano esté establecida. Para obtener información acerca de la integración de Kaspersky Security Center con otras soluciones de Kaspersky, consulte la [Ayuda de Kaspersky Security Center](#).

La integración con Kaspersky Managed Detection and Response consta de los siguientes pasos:

### 1 Configuración de Kaspersky Security Network privada

Omita este paso si utiliza Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configura automáticamente la instancia local de Kaspersky Security Network al instalar el complemento MDR.

KSN privada admite intercambio de datos entre equipos y servidores dedicados de Kaspersky Security Network, no así KSN global.

Cargue el archivo de configuración de Kaspersky Security Network en las propiedades del Servidor de administración. El archivo de configuración de Kaspersky Security Network se encuentra dentro del archivo comprimido ZIP del archivo de configuración de MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener detalles sobre la configuración de Kaspersky Security Network privada, consulte la [Ayuda de Kaspersky Security Center](#). También puede cargar un archivo de configuración de Kaspersky Security Network en el equipo desde la línea de comandos (consulte las instrucciones a continuación).

#### [Cómo configurar Kaspersky Security Network privada desde la línea de comandos](#)

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

```
avp.com KSN /private <nombre del archivo>
```

donde <nombre del archivo> es el nombre del archivo de configuración que contiene la configuración de KSN privada (formato de archivo PKCS7 o PEM).

Ejemplo:

```
avp.com KSN/privado C:/kpsn_config.pkcs7
```

Como resultado, Kaspersky Endpoint Security utilizará KSN privada para determinar la reputación de archivos, aplicaciones y sitios web. La configuración de política en la sección **Kaspersky Security Network** mostrará el siguiente estado de funcionamiento: *Red KSN: KSN privada*.

Debe [activar el modo de KSN ampliado](#) para que funcione Managed Detection and Response.

### 2 Active Managed Detection and Response



Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (consulte las instrucciones a continuación). El archivo BLOB contiene el ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra dentro del archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener información detallada sobre un archivo BLOB, consulte la [Ayuda de Kaspersky Managed Detection and Response](#).

### [Cómo activar Managed Detection and Response en la Consola de administración \(MMC\)](#)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Detection and Response** → **Managed Detection and Response**.
6. Seleccione la casilla de verificación **Managed Detection and Response**.
7. En el bloque **Configuración**, haga clic en **Importar** y seleccione el archivo BLOB recibido en Kaspersky Managed Detection and Response Console. El archivo tiene la extensión P7.
8. Guarde los cambios.

### [Cómo activar Managed Detection and Response en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Detection and Response** → **Managed Detection and Response**.
5. Active la opción **Managed Detection and Response**.
6. Haga clic en **Importar** y seleccione el archivo BLOB que se obtuvo en Kaspersky Managed Detection and Response Console. El archivo tiene la extensión P7.
7. Guarde los cambios.

### [Cómo activar Managed Detection and Response desde la línea de comandos](#)

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:  

```
avp.com MDRLICENSE /ADD <nombre del archivo> /login=<nombre de usuario>  
/password=<contraseña>
```

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Configurar parámetros de la aplicación**.

Como resultado, Kaspersky Endpoint Security realizará una comprobación del archivo BLOB. La verificación del archivo BLOB incluye la verificación de la firma digital y el período de licencia. Si el archivo BLOB se verifica correctamente, Kaspersky Endpoint Security lo cargará y enviará al equipo durante la próxima sincronización con Kaspersky Security Center. Consulte *informe de estado de los componentes de la aplicación* para verificar el estado operativo del componente. También puede ver el estado operativo de un componente en informes de la interfaz local de Kaspersky Endpoint Security. El componente **Managed Detection and Response** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

## Migración desde Kaspersky Endpoint Agent

Kaspersky Endpoint Security versión 11 y posteriores son compatibles con la solución MDR. Kaspersky Endpoint Security versiones 11-11.5.0 solo envían datos de telemetría a Kaspersky Managed Detection and Response para activar 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 11-11.5.0, debe actualizar las bases de datos a la versión más reciente para trabajar con la solución MDR. También debe instalar Kaspersky Endpoint Agent.

Si utiliza Kaspersky Endpoint Security 11.6.0 o posterior, debe seleccionar el componente Managed Detection and Response cuando instale la aplicación para trabajar con la solución MDR. En este caso, no es necesario instalar Kaspersky Endpoint Agent.

Para migrar de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows:

1. Configure la integración con Kaspersky Managed Detection and Response en la directiva de Kaspersky Endpoint Security.
2. Desactive el componente Managed Detection and Response en la directiva de Kaspersky Endpoint Agent.

Si la directiva de Kaspersky Endpoint Security también se 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.

## Endpoint Detection and Response



Kaspersky Endpoint Security 11.7.0 ahora tiene un agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante también "EDR Optimum"). Kaspersky Endpoint Security 11.8.0 ahora tiene un agente integrado para la solución Kaspersky Endpoint Detection and Response Expert (en adelante también "EDR Expert"). *Kaspersky Endpoint Detection and Response* es una variedad de soluciones para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de las soluciones combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware y ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre las soluciones, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) <sup>2</sup> y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#) <sup>2</sup>.

Kaspersky Endpoint Detection and Response examina y analiza el desarrollo de amenazas e informa al *personal de seguridad* o al *Administrador* del posible ataque, para permitir una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana separada. *Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) <sup>2</sup> y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#) <sup>2</sup>.

Kaspersky Endpoint Detection and Response usa las siguientes herramientas de Inteligencia contra amenazas:

- La infraestructura de servicios de nube de Kaspersky Security Network (en lo sucesivo también denominada "KSN"), que proporciona acceso a información de reputación de software, sitios web y archivos en tiempo real de la base de conocimientos de Kaspersky. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de las aplicaciones de Kaspersky ante amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Kaspersky Endpoint Detection and Response usa la solución Kaspersky Private Security Network (KPSN), que envía los datos a los servidores regionales sin enviar datos desde los dispositivos a KSN.
- Integración con el [portal Kaspersky Threat Intelligence Portal](#) <sup>2</sup>, que contiene y muestra información sobre la reputación de los archivos y las direcciones web.
- Base de datos de [amenazas de Kaspersky](#) <sup>2</sup>.

## Integración con Kaspersky Endpoint Detection and Response

Para integrar con Kaspersky Endpoint Detection and Response, debe añadir el componente Endpoint Detection and Response Optimum (EDR Optimum) o el componente Endpoint Detection and Response Expert (EDR Expert) y configurar Kaspersky Endpoint Security.

Los componentes EDR Optimum y EDR Expert no son compatibles. Además, el componente EDR Expert no es compatible con el componente Managed Detection and Response.

Se deben cumplir con las siguientes condiciones para que Endpoint Detection and Response funcione:

- Kaspersky Security Center 13.2. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de Endpoint Detection and Response.
- EDR Optimum se puede administrar en Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console. EDR Expert solo se puede administrar mediante Kaspersky Security Center Cloud Console. No puede administrar esta funcionalidad mediante el uso de la Consola de administración (MMC).

- La aplicación está activada y la funcionalidad se incluye en la licencia.
- El componente Endpoint Detection and Response está activado.
- Los componentes de la aplicación de los que depende Endpoint Detection and Response están activados y en funcionamiento. Endpoint Detection and Response depende de los siguientes componentes:
  - [Protección frente a amenazas en archivos.](#)
  - [Protección frente a amenazas web.](#)
  - [Protección frente a amenazas en el correo.](#)
  - [Prevención de exploits.](#)
  - [Detección de comportamiento.](#)
  - [Prevención de intrusiones en el host.](#)
  - [Motor de reparación.](#)
  - [Control de anomalías adaptativo.](#)

El proceso de integración con Kaspersky Endpoint Detection and Response incluye los siguientes pasos:

### 1 Instalar los componentes de Endpoint Detection and Response

Puede seleccionar el componente EDR Optimum o EDR Expert durante la [instalación](#) o la [actualización](#), además de utilizar la tarea de [Cambiar componentes de la aplicación](#). Debe reiniciar el equipo para terminar de actualizar la aplicación con los componentes nuevos.

Después de la ejecución de la tarea *Cambiar componentes de la aplicación*, el estado de la tarea se muestra de manera incorrecta. En lugar de *Completada correctamente*, la tarea tiene el estado *Programada*. Aun así, la tarea puede completarse correctamente. Asegúrese de que el componente nuevo esté instalado en las propiedades del ordenador de la consola de Kaspersky Security Center (**Aplicaciones** → **Kaspersky Endpoint Security para Windows** → **Componentes**) o en la interfaz de la aplicación local.

### 2 Activar Kaspersky Endpoint Detection and Response

Puede comprar una licencia para uso de Kaspersky Endpoint Detection and Response de las siguientes maneras:

- La funcionalidad de Endpoint Detection and Response está incluida en la licencia de Kaspersky Endpoint Security para Windows.

La funcionalidad estará disponible inmediatamente después de la [activación de Kaspersky Endpoint Security para Windows](#).

- Extensión de licencia para el uso de EDR Optimum o EDR Expert (complemento de Kaspersky Endpoint Detection and Response).

La funcionalidad estará disponible una vez que añade una clave diferente para Kaspersky Endpoint Detection and Response. Como resultado, se instalan dos claves en el equipo: una para Kaspersky Endpoint Security y una para Kaspersky Endpoint Detection and Response.

La licencia para la funcionalidad independiente de Endpoint Detection and Response es la misma que la de Kaspersky Endpoint Security.

Asegúrese de que la funcionalidad EDR Optimum o EDR Expert esté incluida en la licencia y en ejecución en la [interfaz local de la aplicación](#).

### 3 Activación de los componentes de Endpoint Detection and Response

Puede activar o desactivar el componente en la configuración de directivas de Kaspersky Endpoint Security para Windows.

#### [Cómo activar o desactivar el componente Endpoint Detection and Response en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Detection and Response** → **Endpoint Detection and Response**.
5. Active la opción **Endpoint Detection and Response**.
6. Guarde los cambios.

El componente Kaspersky Endpoint Detection and Response está activado. Consulte *informe de estado de los componentes de la aplicación* para verificar el estado operativo del componente. También puede ver el estado operativo de un componente en los [informes](#) de la interfaz local de Kaspersky Endpoint Security. El componente **Endpoint Detection and Response Optimum** o **Endpoint Detection and Response Expert** se añade a la lista de componentes de Kaspersky Endpoint Security.

### 4 Activar la transferencia de datos al Servidor de administración

Para activar todas las funcionalidades de Endpoint Detection and Response, se debe activar la transferencia de los datos de los siguientes tipos de datos:

- Datos de archivos en cuarentena.

Los datos se requieren para obtener información acerca de los archivos en cuarentena en un equipo a través de Web Console y Cloud Console. Por ejemplo, puede descargar un archivo desde Cuarentena para analizarlo en Web Console y Cloud Console.

- Datos de la cadena de desarrollo de la amenaza.

Los 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 tomar acciones de respuesta en Web Console y Cloud Console.

#### [Cómo activar la transferencia de datos al Servidor de administración en Web Console y Cloud Console](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 almacenes**.
5. Seleccione las siguientes casillas en el bloque **Transferencia de datos al Servidor de administración**:
  - **Acerca de los archivos en Cuarentena.**
  - **Acerca de una cadena de desarrollo de la amenaza.**
6. Guarde los cambios.

## Migración desde Kaspersky Endpoint Agent

Si está utilizando Kaspersky Endpoint Security 11.7.0 o una versión más reciente con el componente EDR Optimum (agente incorporado) instalado, el soporte de la integración con la solución Kaspersky Endpoint Detection and Response Optimum está disponible inmediatamente después de la instalación. El componente EDR Optimum no es compatible con Kaspersky Endpoint Agent. Si Kaspersky Endpoint Agent está instalado en el equipo, cuando Kaspersky Endpoint Security se actualiza a la versión 11.7.0, Kaspersky Endpoint Detection and Response Optimum continúa trabajando con Kaspersky Endpoint Security ([migrando la configuración de \[KES + KEA\] a \[KES + agente incorporado\]](#)). Además, Kaspersky Endpoint Agent se eliminará del ordenador. Para completar la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, debe transferir la configuración de directivas y tareas mediante el [Asistente de migración](#).

Si utiliza Kaspersky Endpoint Security 11.4.0–11.6.0 para la interoperabilidad con Kaspersky Endpoint Detection and Response Optimum, la aplicación incluye Kaspersky Endpoint Agent. Puede instalar Kaspersky Endpoint Agent junto con Kaspersky Endpoint Security.

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).

El componente EDR Optimum, como parte de Kaspersky Endpoint Security, admite la interacción con la solución Kaspersky Endpoint Detection and Response Optimum 2.0. La interacción con Kaspersky Endpoint Detection and Response Optimum versión 1.0 no es compatible.

## Analizar en busca de indicadores de compromiso (tarea estándar)

Un *Indicador de compromiso (IOC)* es un conjunto de datos sobre un objeto o actividad que indica el acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. Las tareas de *Análisis de IOC* permiten encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta a la amenaza.

Kaspersky Endpoint Security busca indicadores de compromiso utilizando archivos IOC. Los *archivos IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos IOC deben cumplir con el [estándar OpenIOC](#).

## Modo de ejecución de 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. La *tarea de análisis de IOC estándar* es una tarea grupal o local que se crea y configura manualmente en Web Console. Las tareas se ejecutan mediante archivos IOC preparados por el usuario. Si desea añadir un indicador de compromiso de forma manual, lea los [requerimientos para archivos de IOC](#).

El archivo que puede descargar al hacer clic en el enlace a continuación contiene una tabla con la lista completa de términos de IOC del estándar de OpenIOC.



[DESCARGAR EL ARCHIVO IOC TERMS.XLSX](#)

## Crear una tarea de análisis de IOC

Puede crear tareas de *análisis de IOC* manualmente:

- En los detalles de la alerta.

*Detalles de la alerta* es una herramienta para ver la totalidad de la información recolectada sobre una amenaza detectada y administrar las acciones de respuesta. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

- Utilizar el Asistente de tareas.

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, haga lo siguiente:*

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

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 **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Ir al paso siguiente.
5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Ir al paso siguiente.

De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

La cuenta del sistema (SYSTEM) no tiene permiso para ejecutar la tarea de *análisis de IOC* en las unidades de red. Si desea ejecutar la tarea para una unidad de red, seleccione la cuenta de un usuario que tenga acceso a esa unidad.

Para ejecutar tareas de análisis de IOC independientes en unidades de red, debe elegir manualmente la cuenta de usuario que tiene acceso a esa unidad en las propiedades de la tarea.

6. Salga del Asistente.

La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

Se abre la ventana propiedades de la tarea.

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

9. Vaya a la sección **Configuración del análisis de IOC**.

10. Cargue los archivos IOC para buscar indicadores de compromiso.

Después de cargar los archivos IOC, puede ver la lista de indicadores de los archivos IOC.

No se recomienda añadir ni eliminar archivos IOC después de ejecutar la tarea. Esto puede hacer que los resultados del análisis de IOC se muestren incorrectamente para ejecuciones anteriores de la tarea. Para buscar indicadores de compromiso por nuevos archivos IOC, se recomienda añadir nuevas tareas.

11. Configure acciones al detectar un IOC:

- **Aísle el equipo de la red.** Si se selecciona esta opción, Kaspersky Endpoint Security aísla el equipo de la red para evitar que la amenaza se propague. Puede configurar la duración del aislamiento en [la configuración del componente Endpoint Detection and Response](#).
- **Mover la copia a la cuarentena, eliminar objeto.** Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.
- **Ejecutar análisis de áreas críticas.** Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea [Análisis de áreas críticas](#). De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.



12. Vaya a la sección **Avanzado**.

13. Seleccione los tipos de datos (documentos del IOC) que se deben analizar como parte de la tarea.

Kaspersky Endpoint Security selecciona tipos de datos (documentos de IOC) de manera automática para la tarea de *análisis de IOC*, de acuerdo con el contenido de los archivos de IOC cargados. No se recomienda deseleccionar tipos de datos.

También puede configurar coberturas de análisis para los siguientes tipos de datos:

- **Archivos FileItem.** Configure una cobertura de análisis de IOC en el ordenador mediante coberturas preconfiguradas.  
De forma predeterminada, Kaspersky Endpoint Security analiza en busca de IOC solo en áreas importantes del equipo, como la carpeta de Descargas, el escritorio, la carpeta de archivos temporales del sistema operativo, etc. También puede añadir la cobertura del análisis de forma manual.
- **Registro de eventos de Windows EventLogItem.** Introduzca el período en el cual se registran los eventos. También puede elegir qué registros de eventos de Windows se deben utilizar para realizar el análisis de IOC. De manera predeterminada, están seleccionados los siguientes registros de eventos: registro de eventos de la aplicación, registro de eventos del sistema y registro de eventos de seguridad.

Para el tipo de datos **Registro de Windows RegistryItem**, Kaspersky Endpoint Security analiza [un conjunto de claves de registro](#).

14. Guarde los cambios.

15. Active la casilla ubicada junto a la tarea.

16. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security ejecuta la búsqueda de indicadores de compromiso en el equipo. Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**. Puede ver la información acerca de los indicadores de compromiso detectados en las propiedades de la tarea: **Configuración de la aplicación** → **Resultados del análisis de IOC**.

Los resultados del análisis de IOC se conservan durante 30 días. Después de dicho período, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

## Mover archivo a la cuarentena

Al reaccionar ante amenazas, Kaspersky Endpoint Detection and Response Optimum puede crear tareas de *Mover archivo a Cuarentena*. La *cuarentena* es un almacén local especial en el equipo donde se envían los archivos infectados por virus o los archivos no desinfectables. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la cuarentena solo cuando trabaja con las soluciones Kaspersky Sandbox y Kaspersky Endpoint 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](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

Puede crear tareas de *Mover archivo a Cuarentena* de las siguientes formas:

- En detalles de la alerta (solo para EDR Optimum).

*Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

- Utilizar el Asistente de tareas.

Debe introducir la ruta del archivo o el hash (SHA256 o MD5), o tanto la ruta del archivo como el hash del archivo.

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 Mover archivo a la cuarentena, haga lo siguiente:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en el botón **Añadir**.  
El Asistente de tareas comienza.
3. Configure los parámetros de la tarea:
  - a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.
  - b. En la lista desplegable **Tipo de tarea**, seleccione **Mover archivo a Cuarentena**.
  - c. En el campo **Nombre de la tarea**, escriba una descripción breve.
  - d. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.
5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.  
La nueva tarea aparecerá en la lista de tareas.
7. Haga clic en nueva tarea.  
Se abre la ventana propiedades de la tarea.
8. Seleccione la ficha **Configuración de la aplicación**.

9. En la lista de archivos, haga clic en **Añadir**.

Se inicia el asistente de adición de archivos.

10. Para añadir el archivo, debe introducir la ruta completa al mismo, o tanto el hash como la ruta.

Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se encuentra el archivo*.

11. Haga clic en el botón **Guardar**.

12. Active la casilla ubicada junto a la tarea.

13. Haga clic en el botón **Ejecutar**.

Como resultado, 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 de *Mover archivo a Cuarentena* puede finalizar con el error *Acceso denegado* si está intentando poner en cuarentena un archivo ejecutable que se está ejecutando actualmente. [Cree una tarea de terminar proceso](#) para el archivo y vuelva a intentarlo.

La tarea de *Mover archivo a Cuarentena* puede fallar con el error *No hay espacio suficiente en el almacenamiento de la Cuarentena*, si intenta poner un archivo demasiado grande en cuarentena. Vacíe la Cuarentena o [aumente el tamaño de la Cuarentena](#). Luego, vuelva a intentarlo.

Puede restaurar un archivo de la cuarentena o vaciar la cuarentena mediante Web Console. Puede restaurar objetos localmente en el equipo mediante la [línea de comandos](#).

## Obtener archivo

Puede obtener archivos de los equipos de los usuarios. Por ejemplo, puede configurar la obtención de un archivo de registro de eventos creado por una aplicación de terceros. Para obtener el archivo, debe crear una tarea dedicada. Como resultado de la ejecución de la tarea, el archivo se guarda en Cuarentena. Puede descargar este archivo de la cuarentena a su equipo mediante Web Console. En el 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, haga lo siguiente:*

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

- a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.
- 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 **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.

La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

Se abre la ventana propiedades de la tarea.

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

9. En la lista de archivos, haga clic en **Añadir**.

Se inicia el asistente de adición de archivos.

10. Para añadir el archivo, debe introducir la ruta completa al mismo, o tanto el hash como la ruta.

Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se encuentra el archivo*.

11. Haga clic en el botón **Guardar**.

12. Active la casilla ubicada junto a la tarea.

13. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security crea una copia del archivo y mueve esa copia a la Cuarentena. Puede descargar el archivo de la cuarentena en Web Console.

## Eliminar el archivo

Puede eliminar archivos de forma remota mediante la tarea *Eliminar archivo*. Por ejemplo, puede eliminar un archivo de forma remota al responder a amenazas.

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 Eliminar el archivo, haga lo siguiente:

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

b. En la lista desplegable **Tipo de tarea**, seleccione **Eliminar el archivo**.

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

d. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.

5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.

La nueva tarea aparecerá en la lista de tareas.

7. Haga clic en nueva tarea.

Se abre la ventana propiedades de la tarea.

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

9. En la lista de archivos, haga clic en **Añadir**.

Se inicia el asistente de adición de archivos.

10. Para añadir el archivo, debe introducir la ruta completa al mismo, o tanto el hash como la ruta.

Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se encuentra el archivo*.

11. Haga clic en el botón **Guardar**.

12. Active la casilla ubicada junto a la tarea.

13. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security elimina el archivo del equipo. Si el archivo está bloqueado por un proceso diferente, la tarea se muestra como *Completada*, pero el archivo en sí se elimina solo después de reiniciar el equipo. Después de reiniciar el equipo, confirme que se eliminó el archivo.

La tarea de *Eliminar el archivo* puede finalizar con el error *Acceso denegado* si está intentando eliminar un archivo ejecutable que se está ejecutando actualmente. [Cree una tarea de terminar proceso](#) para el archivo y vuelva a intentarlo.

## Inicio del proceso

Puede ejecutar archivos de forma remota utilizando la tarea de *Inicio del proceso*. Por ejemplo, puede ejecutar de forma remota una utilidad que crea el archivo de configuración del equipo. Luego, puede utilizar la [tarea \*Obtener archivo\*](#) para recibir el archivo creado en Kaspersky Security Center Web Console.

Puede configurar la tarea para EDR Optimum en Web Console y Cloud Console. La configuración de la tarea para EDR Expert está disponible solo en Cloud Console.

Para crear una tarea de inicio del proceso, haga lo siguiente:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Haga clic en el botón **Añadir**.  
El Asistente de tareas comienza.
3. Configure los parámetros de la tarea:
  - a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.
  - b. En la lista desplegable **Tipo de tarea**, seleccione **Inicio del proceso**.
  - c. En el campo **Nombre de la tarea**, escriba una descripción breve.
  - d. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.
5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

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

8. Se abre la ventana propiedades de la tarea.

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

10. Introduzca el comando de inicio del proceso.

Por ejemplo, si desea ejecutar una utilidad (`utility.exe`) que guarda la información sobre la configuración del equipo en un archivo llamado `conf.txt`, debe introducir los siguientes valores:

- **Comando ejecutable** – `utility.exe`
- **Argumentos de la línea de comandos** – `/R conf.txt`
- **Ruta de acceso a la carpeta de trabajo** – `C:\Users\admin\Diagnostic\`

De forma alternativa, en el campo **Comando ejecutable**, puede introducir `C:\Users\admin\Diagnostic\utility.exe /R conf.txt`. En este caso, no es necesario que introduzca el resto de la configuración.

11. Haga clic en el botón **Guardar**.

12. Active la casilla ubicada junto a la tarea.

13. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security ejecuta el comando en modo silencioso e inicia el proceso. Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**.

## Terminar proceso

Puede finalizar procesos de forma remota mediante la tarea *Terminar proceso*. Por ejemplo, puede finalizar de forma remota una utilidad de prueba de velocidad de Internet que se inició con la tarea de [Inicio del proceso](#).

Si desea prohibir la ejecución de un archivo, puede configurar el [componente de Prevención de ejecución](#). Puede prohibir la ejecución de archivos ejecutables, scripts, archivos de formato Office.

La tarea *Terminar proceso* tiene las siguientes limitaciones:

- Los procesos de System Critical Objects (SCO) no se pueden terminar. 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 Terminar proceso, haga lo siguiente:*

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

Se abre la lista de tareas.

2. Haga clic en el botón **Añadir**.

El Asistente de tareas comienza.

3. Configure los parámetros de la tarea:

- a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.8.0)**.

- b. En la lista desplegable **Tipo de tarea**, seleccione **Finalización de procesos**.
  - c. En el campo **Nombre de la tarea**, escriba una descripción breve.
  - d. En el bloque **Seleccionar a qué dispositivos se asignará la tarea**, elija el alcance de la tarea.
4. Seleccione los dispositivos según la opción seleccionada de alcance de tarea. Haga clic en **Siguiente**.
  5. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea utilizar para ejecutar la tarea. Haga clic en **Siguiente**.

De forma predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (SYSTEM).

6. Finalice el asistente haciendo clic en el botón **Finalizar**.  
La nueva tarea aparecerá en la lista de tareas.
7. Haga clic en nueva tarea.  
Se abre la ventana propiedades de la tarea.
8. Seleccione la ficha **Configuración de la aplicación**.
9. Para completar el proceso, debe seleccionar el archivo que desea terminar. Puede seleccionar el archivo de una de las siguientes formas:
  - Introduzca el nombre completo del archivo.
  - Introduzca el hash del archivo y la ruta al archivo.
  - Introduzca el PID del proceso (solo para tareas locales).

Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, puede obtener un error de *No se encuentra el archivo*.

10. En la ventana de propiedades de la tarea, elija 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 el botón **Guardar**.
13. Active la casilla ubicada junto a la tarea.
14. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security finaliza el proceso en el ordenador. Por ejemplo, si una aplicación "GAME" está en ejecución y finaliza el proceso game.exe, la aplicación se cierra sin guardar los datos. Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**.



## Prevención de ejecución

La prevención de ejecución permite administrar la ejecución de archivos ejecutables y scripts, así como abrir archivos de formato Office. De esta manera, puede, por ejemplo, prevenir la ejecución de aplicaciones que considere inseguras. La prevención de ejecución es compatible con [un conjunto de extensiones de archivos](#) y [un conjunto de intérpretes de script](#).

### Regla de prevención de ejecución

La prevención de ejecución administra el acceso de usuarios a archivos con reglas de prevención de ejecución. Una *regla de prevención de ejecución* es un conjunto de criterios que se consideran al realizar bloqueos. La aplicación identifica archivos por sus rutas o sumas de comprobación calculadas mediante algoritmos hash MD5 y SHA256.

Puede crear Reglas de prevención de ejecución:

- En detalles de la alerta (solo para EDR Optimum).

*Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) <sup>2</sup> y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#) <sup>2</sup>.

- Uso de una directiva de grupo o configuración de la aplicación local.

Debe introducir la ruta del archivo o el hash (SHA256 o MD5), o tanto la ruta del archivo como el hash del archivo.

También puede administrar la prevención de ejecución de forma local, mediante la [línea de comandos](#).

No se recomienda crear más de 5000 reglas de prevención de ejecución, ya que esto puede provocar inestabilidad en el sistema.

Las reglas de prevención no incluyen archivos en CD ni imágenes ISO. La aplicación no bloquea la ejecución ni apertura de estos archivos.

### Modos de regla de prevención de ejecución

El componente de prevención de ejecución puede funcionar en 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 registro de eventos de Kaspersky Security Center.

## Administración de la prevención de ejecución

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 prevenir la ejecución, haga lo siguiente:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Detection and Response** → **Endpoint Detection and Response**.
5. Utilice el interruptor **Prevención de ejecución** para activar o desactivar el componente.
6. En el bloque **Acción al ejecutar o abrir un objeto prohibido**, seleccione el modo de funcionamiento del componente:
  - **Bloquear y escribirlo en el informe.** En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Windows y en el registro de eventos de Kaspersky Security Center.
  - **Solo eventos del registro.** 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.
7. Crear una lista de reglas de prevención de ejecución:
  - a. Haga clic en el botón **Añadir**.
  - b. Esto abre una ventana; en esta ventana, introduzca el nombre de la regla de prevención de ejecución (por ejemplo, *Aplicación A*).
  - c. En la lista desplegable de **Tipo**, seleccione el objeto de que desee bloquear: **Archivo ejecutable**, **Script**, **Documento de Microsoft Office**.  
Si selecciona un tipo equivocado, Kaspersky Endpoint Security no bloquea el archivo ni el script.
  - d. Para añadir el archivo, debe introducir el hash del archivo (SHA256 o MD5), la ruta completa al archivo o tanto el hash como la ruta.

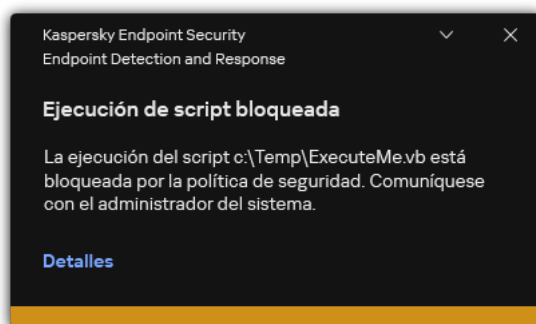
Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo que comienza con `\\`, y no la letra de unidad. Por ejemplo, `\\server\shared_folder\file.exe`. Si la ruta del archivo contiene una letra de unidad de red, Kaspersky Endpoint Security no bloquea el archivo ni el script.

La prevención de ejecución es compatible con [un conjunto de extensiones de archivos](#) y [un conjunto de intérpretes de script](#).

e. Haga clic en **Aceptar**.

8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security bloquea la ejecución de objetos: ejecución de archivos ejecutables y scripts, apertura de archivos de formato Office. Sin embargo, puede abrir un archivo de script en un editor de textos, incluso si no se puede ejecutar el script. Cuando se bloquea la ejecución de un objeto, Kaspersky Endpoint Security muestra una notificación estándar (ver la figura a continuación), si las notificaciones [están habilitadas en la configuración de la aplicación](#).



Notificación de prevención de ejecución

## Aislamiento de equipos de la red

El aislamiento de red del ordenador permite aislar automáticamente un ordenador de la red en respuesta a la detección de un indicador de compromiso (IOC).

Cuando el Aislamiento de red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones de red TCP/IP nuevas en el equipo, excepto las siguientes conexiones:

- Conexiones enumeradas en exclusiones de aislamiento de red.
- Conexiones iniciadas por los servicios de Kaspersky Endpoint Security.
- Conexiones iniciadas por el agente de administración de Kaspersky Security Center.

### Administrar el aislamiento de red

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.

Puede configurar el Aislamiento de red para que se encienda de manera automática en respuesta a una detección de IOC. También puede encender y apagar el Aislamiento de red de forma manual.

Puede encender el Aislamiento de red de la siguiente manera:

- En detalles de la alerta (solo para EDR Optimum).

*Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) <sup>2</sup> y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#) <sup>2</sup>.

- Uso de los ajustes locales de la aplicación.

### [Cómo configurar el Aislamiento de red para que se encienda de forma automática en respuesta a una detección de IOC](#) <sup>2</sup>

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

Se abre la lista de tareas.

2. Seleccione la tarea **Análisis de IOC** de Kaspersky Endpoint Security.

Se abre la ventana propiedades de la tarea.

De ser necesario, cree una tarea de [Análisis de IOC](#).

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

4. En el bloque **Acción al detectar una IOC**, seleccione las casillas de verificación **Tomar medidas de respuesta después de encontrar un IOC** y **Aislar el equipo de la red**.

5. Guarde los cambios.

Como resultado, cuando se detecta un IOC, la aplicación aísla el ordenador de la red para prevenir que la amenaza se propague.

### [Cómo encender el Aislamiento de red de un ordenador de forma manual](#) <sup>2</sup>

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
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 red**, haga clic en **Aislar el equipo de la red**.

Puede configurar el Aislamiento de red para que se apague de forma automática cuando se cumpla un límite de tiempo especificado. De manera predeterminada, la aplicación apaga el Aislamiento de red cuando transcurren 8 horas desde que se encendió. También puede apagar el Aislamiento de red de forma manual. Después de apagar el Aislamiento de red, el ordenador puede usar la red sin restricciones.

#### [Cómo configurar el plazo para apagar el Aislamiento de red de un ordenador de forma automática](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Detection and Response** → **Endpoint Detection and Response**.
5. En el bloque **Aislamiento de red**, haga clic en **Configure los ajustes de desbloqueo de equipos**.
6. Esto abre una ventana: aquí debe seleccionar la casilla de verificación **Desbloquear automáticamente el ordenador aislado en N horas** e introducir el plazo para apagar el Aislamiento de red de forma automática.
7. Guarde los cambios.

#### [Cómo apagar el Aislamiento de red de un ordenador de forma manual](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
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 red**, haga clic en **Desbloquee el aislamiento del equipo de la red**.

También puede desactivar el Aislamiento de red de forma local mediante la [línea de comandos](#).

## Exclusiones de aislamiento de red

Puede configurar Exclusiones de aislamiento de red. Las conexiones de red que coinciden con las reglas no se bloquean en el ordenador cuando el aislamiento de red está activado.

Para configurar las Exclusiones de aislamiento de red, puede usar una lista de *perfiles de red estándar*. De forma predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones de forma manual (ver las instrucciones a continuación).

Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si el aislamiento de red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center o en los detalles de la alerta.

Una directiva activa no evita que se apliquen exclusiones al Aislamiento de red configurado en las propiedades del ordenador, porque estos parámetros tienen situaciones de uso diferentes.

### [Cómo añadir una Exclusión de aislamiento de red](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Detection and Response** → **Endpoint Detection and Response**.
5. En el bloque **Exclusiones de aislamiento de red**, haga clic en **Exclusiones**.
6. Esto abre una ventana: aquí debe hacer clic en **Añadir desde el perfil** y seleccionar los perfiles de red estándar para configurar las exclusiones.  
Las exclusiones del aislamiento de red desde el perfil se añaden a la lista de Exclusiones de aislamiento de red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de conexiones de red.
7. Si es necesario, añada una Exclusión de aislamiento de red de forma manual. Para hacerlo, en la ventana de la lista de exclusiones, haga clic en **Añadir** y modifique la configuración de conexiones de red de forma manual.
8. Guarde los cambios.

También puede ver la lista de Exclusiones de aislamiento de red de forma local mediante la [línea de comandos](#). Para usar esta opción, es necesario que el equipo esté aislado.

## Apéndice 1. Extensiones de archivos compatibles con la Prevención de ejecución

Kaspersky Endpoint Security es compatible con la prevención de la apertura de archivos en formato Office en ciertas aplicaciones. La información acerca de las extensiones de archivos y aplicaciones compatibles se enumera en la siguiente tabla.

Extensiones de archivos compatibles con la Prevención de ejecución

Nombre de aplicación	Archivo ejecutable	Extensión del archivo
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt

		xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Navegador Tor	acro32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

## Apéndice 2. Intérpretes de scripts compatibles

La Prevención de ejecución es compatible con los siguientes intérpretes de script:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe



- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msixexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacyelevated.exe
- wscript.exe
- wwaahost.exe

La Prevención de ejecución admite el funcionamiento con aplicaciones de Java en el entorno de tiempo de ejecución de Java (procesos de java.exe y javaw.exe).

## Apéndice 3. Cobertura de análisis de IOC en el registro (RegistryItem)

Cuando añade el tipo de datos RegistryItem a la cobertura de análisis de IOC, Kaspersky Endpoint Security analiza las siguientes claves de registro:

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 4. Requisitos de los archivos de IOC

Al crear tareas de análisis de IOC, considere los siguientes requerimientos y limitaciones de los [archivos de IOC](#):

- La aplicación es compatible con archivos IOC con extensiones IOC y XML en el estándar abierto OpenIOC versiones 1.0 y 1.1 para describir indicadores de compromiso.
- Si, al crear una tarea de Análisis de IOC en la línea de comandos, carga archivos de IOC y algunos no son compatibles, la aplicación utiliza solo los archivos de IOC compatibles cuando se ejecuta la tarea. Si, al crear una tarea de Análisis de IOC en la línea de comandos, ninguno de los archivos de IOC que carga resulta ser compatible, la tarea puede ejecutarse de todos modos. Sin embargo, no detectará ningún indicador de riesgo. No es posible cargar archivos de IOC no compatibles a través de Web Console o Cloud Console.
- Los errores semánticos y los términos y etiquetas de IOC no compatibles en archivos de IOC no hacen que falle la ejecución de la tarea. En dichas secciones de archivos de IOC, la aplicación no detecta una coincidencia.
- [Los identificadores de todos los archivos de IOC](#) utilizados en una sola tarea de análisis de IOC deben ser únicos. Si hay archivos de IOC con el mismo identificador, esto puede afectar los resultados de la ejecución de la tarea.
- Un solo archivo de IOC no debe superar los 2 MB de tamaño. Usar archivos más grandes hará que las tareas de análisis de IOC finalicen con un error. Dicho esto, el tamaño total de todos los archivos agregados a la colección IOC puede superar los 2 MB.
- Se recomienda crear un archivo de IOC por amenaza. Esto facilita el análisis de los resultados de la tarea de análisis de IOC.

El archivo que puede descargar al hacer clic en el enlace a continuación contiene una tabla con la lista completa de términos de IOC del estándar de OpenIOC.

 [DESCARGAR EL ARCHIVO IOC\\_TERMS.XLSX](#)

Las funcionalidades y limitaciones en la compatibilidad de la aplicación con el estándar OpenIOC se enumeran en la siguiente tabla.

Funcionalidades y limitaciones en la compatibilidad con OpenIOC versiones 1.0 y 1.1.

Condiciones compatibles	OpenIOC 1.0:  <code>is</code> <code>isnot</code> (como una excepción del grupo) <code>contains</code> <code>containsnot</code> (como una excepción del grupo) OpenIOC 1.1:  <code>is</code> <code>contains</code> <code>starts-with</code>
-------------------------	--

	ends-with matches greater-than less-than
Atributos de la condición compatibles	OpenIOC 1.1:  preserve-case negate
Operadores compatibles	AND OR
Tipos de datos compatibles	"date": fecha (condiciones aplicables: is, greater-than, less-than)  "int": número entero (condiciones aplicables is, greater-than, less-than)  "string": serie (condiciones aplicables: is, contains, matches, starts-with, ends-with)  "duration": duración en segundos (condiciones aplicables: is, greater-than, less-than)
Funcionalidades de interpretación de tipos de datos	Los tipos de datos "boolean string", "restricted string", "md5", "IP", "sha256" y "base64Binary" se interpretan como series.  La aplicación es compatible con la interpretación de la configuración de Content para los tipos de datos int y date cuando se establecen en forma de intervalos:  OpenIOC 1.0: Usar el operador T0 en el campo Content: <Content type="int">49600 T0 50700</Content> <Content type="date">2009-04-28T10:00:00Z T0 2009-04-28T16:00:00Z</Content> <Content type="int">[154192 T0 154192]</Content> OpenIOC 1.1: Usar las condiciones greater-than y less-than Usar el operador T0 en el campo Content La aplicación es compatible con la interpretación de los tipos de datos date y duration siempre que los indicadores estén configurados en formato ISO 8601, Zulu Time Zone, UTC.

## Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 ahora tiene un agente incorporado para la integración con la solución Kaspersky Sandbox. *La solución Kaspersky Sandbox* detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Kaspersky 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. Kaspersky Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Kaspersky Sandbox). Para obtener más información acerca de la solución, consulte la [Ayuda de Kaspersky Sandbox](#).

Las siguientes configuraciones son posibles para la solución Kaspersky Sandbox:

## Kaspersky Sandbox 2.0

Kaspersky Sandbox 2.0 soporta la configuración [KES + agente incorporado].

Requisitos mínimos:

- Kaspersky Endpoint Security 11.7.0 for Windows o versiones posteriores.
- No se requiere el Agente de Kaspersky Endpoint.
- Kaspersky Security Center 13.2.

## Kaspersky Sandbox 1.0

Kaspersky Sandbox 1.0 soporta la configuración [KES + KEA].

Requisitos mínimos:

- Kaspersky Endpoint Security 11.2.0 a 11.6.0 for Windows.
- Kaspersky Endpoint Agent 3.8.  
Puede instalar el Agente de Kaspersky Endpoint desde el kit de distribución de Kaspersky Endpoint Security para Windows.
- Kaspersky Security Center 11.

## Integración con Kaspersky Sandbox

Es necesario añadir el componente Kaspersky Sandbox para la integración con el componente Kaspersky Sandbox. Puede seleccionar el componente Kaspersky Sandbox durante la [instalación](#) o [actualización](#), además de utilizar la tarea [Cambiar componentes de la aplicación](#).

Después de la ejecución de la tarea *Cambiar componentes de la aplicación*, el estado de la tarea se muestra de manera incorrecta. En lugar de *Completada correctamente*, la tarea tiene el estado *Programada*. Aun así, la tarea puede completarse correctamente. Asegúrese de que el componente nuevo esté instalado en las propiedades del ordenador de la consola de Kaspersky Security Center (**Aplicaciones** → **Kaspersky Endpoint Security para Windows** → **Componentes**) o en la interfaz de la aplicación local.

Para utilizar el componente, se deben cumplir las siguientes condiciones:

- Kaspersky Security Center 13.2. Las versiones anteriores de Kaspersky Security Center no permiten crear tareas de análisis de IOC independientes para la respuesta a la amenaza.
- El componente solo se puede administrar mediante Web Console. No puede administrar este componente mediante la Consola de administración (MMC).
- La aplicación está activada y la funcionalidad se incluye en la licencia.
- La transferencia de datos al Servidor de administración está activada.

Para utilizar todas las funcionalidades de Kaspersky Sandbox, asegúrese de que la transferencia de datos de archivos en cuarentena esté activada. Los datos se requieren para obtener información acerca de los archivos en cuarentena en un ordenador a través de Web Console. Por ejemplo, puede descargar un archivo desde la cuarentena para analizarlo en Web Console.

### Cómo activar la transferencia de datos al Servidor de administración en Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 almacenes**.
5. En el bloque **Transferencia de datos al Servidor de administración**, seleccione la casilla de verificación **Acerca de los archivos en Cuarentena**.
6. Guarde los cambios.

- Se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración

Para que Kaspersky Sandbox trabaje con el Servidor de administración mediante Kaspersky Security Center Web Console, debe establecer una nueva conexión segura, una *conexión en segundo plano*. Para obtener información acerca de la integración de Kaspersky Security Center con otras soluciones de Kaspersky, consulte la [Ayuda de Kaspersky Security Center](#).

### Establecer una conexión en segundo plano en Web Console

1. En la ventana principal de Web Console, seleccione **Configuración de la consola** → **Integración**.
2. Vaya a la sección **Integración entre servicios**.
3. Active el interruptor **Establecer una conexión en segundo plano para la integración entre servicios**.
4. Guarde los cambios.

Si no se establece una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración, las tareas independientes de análisis de IOC no se pueden crear como parte de la Respuesta a la amenaza.

- El componente Kaspersky Sandbox está activado.

Puede activar o desactivar la integración con Kaspersky Sandbox en Web Console o localmente a través de la [línea de comandos](#).

*Para activar o desactivar la integración con Kaspersky Sandbox, haga lo siguiente:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 **Detection and Response** → **Kaspersky Sandbox**.
5. Utilizar el interruptor de **Integración con Kaspersky Sandbox** para activar o desactivar el componente.
6. Guarde los cambios.

Como resultado, el componente Kaspersky Sandbox se activa. Consulte el *Informe de estado de los componentes de la aplicación* para verificar el estado operativo del componente. También puede ver el estado operativo de un componente en los [informes](#) de la interfaz local de Kaspersky Endpoint Security. El componente **Kaspersky Sandbox** se añadirá a la lista de componentes de Kaspersky Endpoint Security.

Kaspersky Endpoint Security guarda información sobre el funcionamiento del componente Kaspersky Sandbox en un informe. El informe también contiene información sobre errores. Si recibe un mensaje de error con un formato de descripción Código de error: XXX (por ejemplo, 0xa67b01f4), póngase en contacto con el [Soporte técnico](#).

## Migración desde Kaspersky Endpoint Agent

Si está utilizando Kaspersky Endpoint Security 11.7.0 o una versión más reciente con el componente Kaspersky Sandbox (agente integrado) instalado, la interoperabilidad con la solución Kaspersky Sandbox está disponible inmediatamente después de la instalación. El componente Kaspersky Sandbox no es compatible con Kaspersky Endpoint Agent. Si Kaspersky Endpoint Agent está instalado en el equipo, cuando Kaspersky Endpoint Security se actualiza a la versión 11.7.0, Kaspersky Sandbox continúa trabajando con Kaspersky Endpoint Security ([migración de la configuración de \[KES+KEA\] a \[KES + agente incorporado\]](#)). Además, Kaspersky Endpoint Agent se eliminará del ordenador. Para completar la migración desde Kaspersky Endpoint Agent hasta Kaspersky Endpoint Security para Windows, debe transferir la configuración de directivas y tareas mediante el [Asistente de migración](#).

Si está utilizando Kaspersky Endpoint Security 11.4.0 a 11.6.0 para la interoperabilidad con Kaspersky Sandbox, la aplicación incluye Kaspersky Endpoint Agent. Puede instalar Kaspersky Endpoint Agent junto con Kaspersky Endpoint Security.

El componente Kaspersky Sandbox, que forma parte de Kaspersky Endpoint Security, admite la interoperabilidad con la solución Kaspersky Sandbox 2.0. La solución Kaspersky Sandbox 1.0 no es compatible.

## Añadir un certificado TLS

Para configurar una conexión de confianza con los servidores de Kaspersky Sandbox, debe preparar un certificado TLS. A continuación, debe añadir el certificado a los servidores de Kaspersky Sandbox y la directiva de Kaspersky Endpoint Security. Para obtener información sobre cómo preparar el certificado y añadirlo a los servidores, consulte la [Ayuda de Kaspersky Sandbox](#).

Puede añadir un certificado TLS en Web Console o localmente mediante la [línea de comandos](#).

*Cómo añadir un certificado TLS en Web Console:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.

2. 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 **Detection and Response** → **Kaspersky Sandbox**.

5. Haga clic en el enlace **Configuración de conexión del servidor**.

Esto abre la ventana de configuración de la conexión del servidor de Kaspersky Sandbox.

6. Debajo de **Certificado TLS del servidor**, haga clic en **Añadir** y seleccione el archivo de certificado TLS.

Kaspersky Endpoint Security solo puede tener un certificado TLS para un servidor de Kaspersky Sandbox. Si ha añadido un certificado TLS anteriormente, ese certificado se revoca. Solo se utiliza el último certificado añadido.

7. Configure las opciones de conexiones avanzadas para los servidores de Kaspersky Sandbox:

- **Tiempo de espera.** Tiempo de espera de conexión para el servidor de Kaspersky Sandbox. Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de espera de conexión de Kaspersky Sandbox si su velocidad de conexión es baja o si la conexión es inestable. El tiempo de espera recomendado para las solicitudes es de 0,5 segundos o menos.
- **Cola de peticiones de Kaspersky Sandbox.** Tamaño de la carpeta de cola de solicitudes. Cuando se accede a un objeto en el equipo (ejecutable iniciado o documento abierto, por ejemplo, en formato DOCX o PDF), Kaspersky Endpoint Security también puede enviar el objeto para que Kaspersky Sandbox lo analice. Si hay varias solicitudes, Kaspersky Endpoint Security crea una cola de solicitudes. De forma predeterminada, el tamaño de la carpeta de cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Kaspersky Sandbox deja de añadir nuevas solicitudes a la cola y envía el evento correspondiente a Kaspersky Security Center. Puede configurar el tamaño de la carpeta de cola de solicitudes en función de la configuración de su servidor.

8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security comprueba el certificado TLS. Si el certificado se comprueba correctamente, Kaspersky Endpoint Security carga el archivo del certificado en el equipo durante la próxima sincronización con Kaspersky Security Center. Si ha añadido dos certificados TLS, Kaspersky Sandbox utilizará el último certificado añadido para establecer una conexión de confianza.

## Añadir servidores de Kaspersky Sandbox

Para conectar equipos a servidores de Kaspersky Sandbox con imágenes virtuales de sistemas operativos, debe introducir una dirección de servidor y un puerto. Para obtener detalles sobre la implementación de imágenes virtuales y la configuración de los servidores de Kaspersky Sandbox, consulte la [Ayuda de Kaspersky Sandbox](#).

*Para añadir servidores de Kaspersky Sandbox a Web Console, haga lo siguiente:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.

2. 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 **Detection and Response** → **Kaspersky Sandbox**.
5. Debajo de **Servidores Kaspersky Sandbox**, haga clic en **Añadir**.
6. Esto abre una ventana donde debe introducir la dirección del servidor de Kaspersky Sandbox (IPv4, IPv6, DNS) y el puerto.
7. Guarde los cambios.

## Analizar en busca de indicadores de compromiso (tarea independiente)

Un *Indicador de compromiso (IOC)* es un conjunto de datos sobre un objeto o actividad que indica el acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. Las tareas de *Análisis de IOC* permiten encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta a la amenaza.

Kaspersky Endpoint Security busca indicadores de compromiso utilizando archivos IOC. Los *archivos IOC* son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos IOC deben cumplir con el [estándar OpenIOC](#). Kaspersky Endpoint Security genera automáticamente archivos IOC para Kaspersky Sandbox.

### Modo de ejecución de la tarea de análisis de IOC

La aplicación crea tareas de análisis de IOC independientes para Kaspersky Sandbox. La *tarea de análisis de IOC independiente* es una tarea de grupo que se crea automáticamente al reaccionar a una amenaza detectada por Kaspersky Sandbox. Kaspersky Endpoint Security genera automáticamente el archivo de IOC. Los archivos IOC personalizados no son compatibles. Las tareas se eliminan automáticamente 30 días después del momento de creación. Para obtener más detalles sobre las tareas de análisis de IOC independientes, consulte la [Ayuda de Kaspersky Sandbox](#).

### Configuración de la tarea Análisis de IOC

Kaspersky Sandbox puede crear y ejecutar tareas de *Análisis de IOC* de forma automática cuando reacciona a amenazas.

Puede configurar los ajustes solo en Web Console.

Necesita Kaspersky Security Center 13.2 para que las tareas de análisis de IOC independientes de Kaspersky Sandbox funcionen.

Para cambiar la configuración de la tarea *Análisis de IOC*, haga lo siguiente:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.  
Se abre la lista de tareas.
2. Seleccione la tarea **Análisis de IOC** de Kaspersky Endpoint Security.  
Se abre la ventana propiedades de la tarea.

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

4. Vaya a la sección **Configuración del análisis de IOC**.

5. Configure acciones al detectar un IOC:

- **Mover la copia a la cuarentena, eliminar objeto.** Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.
- **Ejecutar análisis de áreas críticas.** Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea [Análisis de áreas críticas](#). De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.

6. Configure el modo de ejecución de la tarea de análisis de IOC con la casilla **Ejecutar solo cuando el equipo está inactivo**. Esta casilla activa o desactiva la función que suspende la tarea *Análisis de IOC* cuando los recursos del equipo son limitados. Kaspersky Endpoint Security pone en pausa la tarea *Análisis de IOC* cuando el salvapantallas está apagado y el equipo está desbloqueado.

Esta opción de programación le permite conservar los recursos del equipo cuando se está utilizando.

7. Guarde los cambios.

Puede ver los resultados de la tarea en las propiedades de la tarea, dentro de la sección **Resultados**. Puede ver la información acerca de los indicadores de compromiso detectados en las propiedades de la tarea: **Configuración de la aplicación** → **Resultados del análisis de IOC**.

Los resultados del análisis de IOC se conservan durante 30 días. Después de dicho período, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

## Administración de Cuarentena

La *cuarentena* es un almacén local especial en el equipo donde se envían los archivos infectados por virus o los archivos no desinfectables. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la cuarentena solo cuando trabaja con las soluciones Kaspersky Sandbox y Kaspersky Endpoint 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](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Security utiliza la cuenta del sistema (SYSTEM) para poner archivos en cuarentena.

La cuarentena solo se puede configurar mediante Web Console. También puede usar Web Console para administrar objetos en cuarentena (restaurar, eliminar, añadir, etc.). Localmente, en el equipo solo puede [restaurar el objeto a través de la línea de comando](#).

## Configuración del tamaño máximo de Cuarentena

De forma predeterminada, el tamaño de la Cuarentena está limitado a 200 MB. Cuando se alcanza el límite máximo de almacenamiento, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos de Cuarentena.

*Para configurar el tamaño máximo de Cuarentena, haga lo siguiente:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 almacenes**.
5. En el bloque **Cuarentena**, configure el tamaño de Cuarentena:
  - **Limitar el tamaño de Cuarentena a N MB.** Tamaño máximo de cuarentena en MB. Por ejemplo, puede establecer el tamaño máximo de la cuarentena en 200 MB. Cuando la cuarentena alcanza el tamaño máximo, 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 deja de colocar nuevos objetos en cuarentena. Debe vaciar manualmente la Cuarentena.
  - **Notificar cuando el almacenamiento de Cuarentena alcanza el N por ciento.** Valor umbral de la cuarentena. Por ejemplo, puede establecer el umbral de la cuarentena en 50 %. Cuando la cuarentena alcanza el umbral, Kaspersky Endpoint Security envía el evento correspondiente a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación continúa poniendo en cuarentena nuevos objetos.
6. Guarde los cambios.

## Envío de datos sobre archivos en Cuarentena a Kaspersky Security Center

Para realizar acciones con objetos en cuarentena en Web Console, debe activar el envío de datos de archivos en Cuarentena al Servidor de administración. Por ejemplo, puede descargar un archivo desde la cuarentena para analizarlo en Web Console. El envío de datos de archivos en Cuarentena debe estar activado para todas las funciones de [Kaspersky Sandbox](#) y [Kaspersky Endpoint Detection and Response](#) para que funcione.

*Para activar la transferencia de datos de archivos en Cuarentena a Kaspersky Security Center, haga lo siguiente:*

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. 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 almacenes**.
5. En la sección **Transferencia de datos al Servidor de administración**, seleccione la casilla de verificación **Acerca de los archivos en Cuarentena**.
6. Guarde los cambios.

Como resultado, en Web Console, puede ver la lista de archivos en Cuarentena en un equipo (**Operaciones** → **Almacenamientos** → **Cuarentena**). Puede usar Web Console para administrar objetos en Cuarentena (restaurar, eliminar, añadir, etc.).

# Kaspersky Security para Windows Server



Kaspersky Endpoint Security 11.8.0 admite la funcionalidad básica de la solución Kaspersky Security para Windows Server (KSWs). *Kaspersky Security para Windows Server* protege los servidores que ejecutan los sistemas operativos Microsoft Windows y los almacenamientos conectados a la red contra virus y otras amenazas de seguridad informática a las que están expuestos los servidores y los almacenamientos conectados a la red al intercambiar archivos. Para obtener información detallada sobre cómo funciona la solución, consulte la [Ayuda de Kaspersky Security para Windows Server](#). A partir de Kaspersky Endpoint Security 11.8.0, puede migrar de KSWs a Kaspersky Endpoint Security para Windows y utilizar la misma solución para proteger estaciones de trabajo y servidores.

## Instalación de KES encima de KSWs

Kaspersky Endpoint Security (KES) es compatible con la funcionalidad básica de la aplicación Kaspersky Security for Windows Server (KSWs). A partir de la versión 11.8.0 de Kaspersky Endpoint Security, puede utilizar KES en lugar de KSWs.

Deberá desinstalar KSWs antes de instalar KES. Puede desinstalar la aplicación de forma remota con la tarea [Desinstalar aplicación en remoto](#) o [localmente en el servidor](#). Después de desinstalar KSWs, puede ser necesario el reinicio del servidor. Si desea instalar Kaspersky Endpoint Security sin tener que reiniciar el ordenador, se le recomienda asegurarse de que la aplicación Kaspersky Security for Windows Server esté completamente desinstalada. A continuación, encontrará el listado de archivos y servicios que deberá comprobar. Si la aplicación no se ha desinstalado por completo, pueden producirse errores de servidor después de la instalación de Kaspersky Endpoint Security. También se le recomienda asegurarse de que la aplicación esté completamente desinstalada si ha usado la herramienta kavremover. La [herramienta kavremover](#) no es compatible con KSWs.

Después de desinstalar KSWs, [instale Kaspersky Endpoint Security para Windows](#) con cualquier método disponible.

## Comprobar la eliminación de Kaspersky Security for Windows Server

Asegúrese de que Kaspersky Security for Windows Server se haya desinstalado por completo:

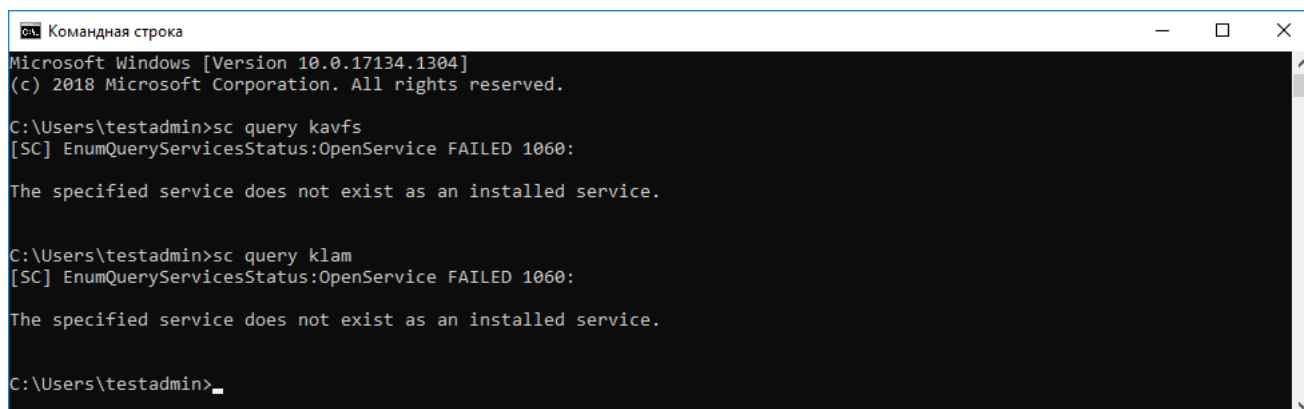
- La carpeta %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ no existe.
- Los siguientes servicios no están en ejecución:
  - Kaspersky Security Service (KAVFS)
  - Kaspersky Security Management Service (KAVFSGT)
  - Kaspersky Security Exploit Prevention Service (KAVFSSLP)
  - Kaspersky Security Script Checker Service (KAVFSSCS)

Puede comprobar los servicios que están en ejecución en el Administrador de tareas o mediante el comando `sc query` (ver imagen a continuación).

- Los siguientes controladores no están instalados:
  - klam.sys

- kflt.sys
- klramdisk.sys
- klelaml.sys
- kfltdev.sys
- klips.sys
- klids.sys
- klwtpee

Puede comprobar cuáles son los controladores instalados en la carpeta `C:\Windows\System32\drivers` o mediante el comando `sc query`. Si no aparece el servicio o el controlador, recibirá el siguiente mensaje:



```

Microsoft Windows [Version 10.0.17134.1304]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\testadmin>sc query kavfs
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>sc query klam
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>

```

Comprobar la eliminación de los servicios y controladores de Kaspersky Security for Windows Server

Si en el servidor aún hay controladores o archivos de la aplicación, elimínelos de forma manual. Si algunos servicios de Kaspersky Security for Windows Server siguen en ejecución, deténgalos (`sc stop`) y elimínelos (`sc delete`) de forma manual. Para detener el controlador `klam.sys`, use el comando `fltmc unload klam`.

## Activación de KES con una clave de KSWS

Después de instalar la aplicación, puede activar Kaspersky Endpoint Security para Windows (KES) con una clave de licencia de Kaspersky Security para Windows Server (KSWS). El proceso de activación después de la migración depende del método de activación de KSWS (consulte la tabla a continuación).

Activación de Kaspersky Endpoint Security para Windows con una clave de Kaspersky Security para Windows Server

Método de activación de Kaspersky Security para Windows Server	Migración de la clave de Kaspersky Endpoint Security para Windows.
Distribución automática de la clave de licencia de KSWS a los equipos.	Si la distribución automática de claves está activada en las propiedades de la clave de licencia de KSWS, KES se activa automáticamente con la clave de KSWS.
La clave de KSWS se añade	Si su KSWS se activa con la tarea, la clave de licencia de KSWS se eliminará durante la migración de KSWS. Debe activar la aplicación nuevamente. Por ejemplo, puede <a href="#">añadir</a>

<p>mediante una tarea.</p>	<p><a href="#">una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.</a></p>
<p>La clave de KSWs se añade localmente en la interfaz de la aplicación.</p>	<p>Si su KSWs se activa localmente mediante el Asistente de activación de aplicaciones, la clave de licencia de KSWs se eliminará durante la migración de KSWs. Debe activar la aplicación nuevamente. Por ejemplo, puede <a href="#">añadir una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.</a></p>
<p>La clave de KSWs se añade al paquete de instalación.</p>	<p>Si su KSWs se activa con la clave del paquete de instalación, la clave de licencia de KSWs se eliminará durante la migración de KSWs. Debe activar la aplicación nuevamente. Por ejemplo, puede <a href="#">añadir una clave de licencia al paquete de instalación de Kaspersky Endpoint Security para Windows.</a></p>

## Administración de la aplicación desde la línea de comandos

Kaspersky Endpoint Security se puede administrar a través de la línea de comandos. Para ver la lista de comandos de administración disponibles, utilice el comando `HELP`. Para conocer la sintaxis de un comando específico, escriba `HELP <comando>`.

Se deben anular los caracteres especiales en el comando. Para escapar los caracteres `&`, `|`, `(`, `)`, `<`, `>`, `^`, utilice el carácter `^` (por ejemplo, para usar el carácter `&`, introduzca `^&`). Para anular el carácter `%`, introduzca `%%`.

## Instalación de la aplicación

Kaspersky Endpoint Security se puede instalar desde la línea de comandos en una de las siguientes formas:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que la instalación se inicie en el modo silencioso, su participación en el proceso de instalación ya no se requiere. Para instalar la aplicación en modo silencioso, utilice las claves `/s` y `/qn`.

Antes de instalar la aplicación en modo silencioso, abra y lea el Contrato de licencia de usuario final y el texto de la Política de privacidad. Encontrará ambos documentos en el [kit de distribución de Kaspersky Endpoint Security](#). Instale la aplicación únicamente si ha leído y comprende y acepta en su totalidad las disposiciones y los términos del Contrato de licencia de usuario final; si comprende y acepta el hecho de que sus datos se procesarán y transmitirán (incluso a otros países) según lo descrito en la Política de privacidad; y si ha leído y comprende en su totalidad la Política de privacidad. Si no está de acuerdo con las disposiciones y los términos del Contrato de licencia de usuario final y de la Política de privacidad, no instale ni utilice Kaspersky Endpoint Security.

*Para instalar la aplicación o actualizar una versión anterior de la aplicación:*

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<nombre de usuario>
/pKLPASSWD=<contraseña> /pKLPASSWDAREA=<alcance de la contraseña>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<nivel de seguimiento>] [/s]
```

o bien

```
msiexec /i <nombre del kit de distribución> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<nombre de usuario> KLPASSWD=<contraseña>
KLPASSWDAREA=<alcance de la contraseña>] [ENABLETRACES=1|0 TRACESLEVEL=<nivel de
seguimiento>] [/qn]
```

Como resultado, la aplicación se instalará en el equipo. Para confirmar que la aplicación está instalada y comprobar su configuración, use el comando [status](#).



EULA=1	<p>Aceptación de las condiciones del Contrato de licencia de usuario final. El contenido del Contrato de licencia se incluye en el <a href="#">kit de distribución de Kaspersky Endpoint Security</a>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Se requiere la aceptación de los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar la versión de esta.</p> </div>
PRIVACYPOLICY=1	<p>Aceptación de la Política de privacidad. El texto de la Política de privacidad se incluye en el <a href="#">Kit de distribución de Kaspersky Endpoint Security</a>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Para instalar la aplicación o actualizar su versión, debe aceptar la Política de privacidad.</p> </div>
KSN	<p>Aceptación o rechazo de la participación en Kaspersky Security Network (KSN). Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security solicitará la confirmación de su consentimiento o el rechazo de la participación en KSN cuando se inicie Kaspersky Endpoint Security por primera vez. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: aceptación de la participación en KSN.</li> <li>• 0: rechazo de la participación en KSN (valor predeterminado).</li> </ul> <p>El paquete de distribución de Kaspersky Endpoint Security se optimiza para su uso con Kaspersky Security Network. Si optara por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que la instalación se haya completado.</p>
ALLOWREBOOT=1	<p>Reinicio automático del equipo, si es necesario después de la instalación o la actualización de la aplicación. Si no se establece ningún valor para este parámetro, se bloquea el reinicio automático del equipo.</p> <p>Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.</p>
SKIPPRODUCTCHECK=1	<p>Desactivación de la comprobación de software no compatible. La lista de software no compatible está disponible en el archivo incompatible.txt que se incluye en el <a href="#">kit de distribución</a>. Si no se establece ningún valor para este parámetro y se detecta software no compatible, la instalación de Kaspersky Endpoint Security finalizará.</p>
SKIPPRODUCTUNINSTALL=1	<p>Desactivación de la eliminación automática del software no compatible detectado. Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security intentará eliminar el software no compatible.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>No se puede actualizar la eliminación automática de software incompatible al instalar Kaspersky Endpoint Security con el instalador msiexec. Use setup_kes.exe para activar la eliminación automática de software incompatible.</p> </div>
KLLOGIN	<p>Configure el nombre de usuario para acceder a las funciones y ajustes de</p>

	<p>Kaspersky Endpoint Security (el componente <a href="#">Protección con contraseña</a>). El nombre de usuario se configura a la par de los parámetros KLPASSWD y KLPASSWDAREA. El nombre de usuario KLAdmin se utiliza de forma predeterminada.</p>
KLPASSWD	<p>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 KLLLOGIN y KLPASSWDAREA).</p> <p>Si especifica una contraseña, pero no un nombre de usuario con el parámetro KLLLOGIN, se utilizará de forma predeterminada el nombre de usuario KLAdmin.</p>
KLPASSWDAREA	<p>Especifique el alcance de la contraseña para acceder a Kaspersky Endpoint Security. Cuando un usuario intente realizar una acción que esté dentro de este alcance, Kaspersky Endpoint Security le solicitará las credenciales de la cuenta (parámetros KLLLOGIN y KLPASSWD). Si necesita especificar más de un valor, use el carácter "; ". Valores disponibles:</p> <ul style="list-style-type: none"> <li>• SET: modificar la configuración de la aplicación.</li> <li>• EXIT: salir de la aplicación.</li> <li>• DISPROTECT: desactivar componentes de protección y detener tareas de análisis.</li> <li>• DISPOLICY: desactivar la directiva de Kaspersky Security Center.</li> <li>• UNINST: eliminar la aplicación del equipo.</li> <li>• DISCTRL: desactivar componentes de control.</li> <li>• REMOVELIC: eliminar la clave.</li> <li>• REPORTS: consultar informes.</li> </ul>
ENABLETRACES	<p>Activar o desactivar el rastreo de la aplicación. Una vez que Kaspersky Endpoint Security se inicia, los archivos de seguimiento se guardan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: el rastreo está activado.</li> <li>• 0: el rastreo está desactivado (valor predeterminado).</li> </ul>
TRACESLEVEL	<p>Nivel de detalle del seguimiento. Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 100 (crítico). Solo mensajes sobre errores graves.</li> <li>• 200 (alto). Mensajes sobre todos los errores, incluidos los errores graves.</li> <li>• 300 (diagnóstico). Mensajes sobre todos los errores, además de las advertencias.</li> <li>• 400 (importante). Todos los mensajes de error y de advertencia, así como otra información adicional.</li> <li>• 500 (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado).</li> </ul>

	<ul style="list-style-type: none"> <li>• 600 (bajo). Todos los mensajes.</li> </ul>
AMPPL	<p>Activa o desactiva el uso de la tecnología AM-PPL (Anti-Malware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para obtener más información sobre la tecnología AM-PPL, visite el <a href="#">sitio web de Microsoft</a>.</p> <p>La tecnología AM-PPL está disponible para los sistemas operativos Windows 10 versión 1703 (RS2) o posterior, y Windows Server 2019.</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: los procesos de Kaspersky Endpoint Security se protegen con la tecnología AM-PPL.</li> <li>• 0: los procesos de Kaspersky Endpoint Security no se protegen con la tecnología AM-PPL.</li> </ul>
RESTAPI	<p>Administrar la aplicación a través de la API REST. Para administrar la aplicación a través de la API REST, debe especificar el nombre de usuario (parámetro RESTAPI_User).</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> <li>• 1: se permite la administración a través de la API REST.</li> <li>• 0: se bloquea la administración a través de la API REST (valor predeterminado).</li> </ul> <p>Para administrar la aplicación a través de la API REST, debe permitirse la administración mediante sistemas de administración. Para ello, configure el parámetro AdminKitConnector=1. Si administra la aplicación a través de la API REST, no es posible administrarla mediante los sistemas de administración de Kaspersky.</p>
RESTAPI_User	<p>Nombre de usuario de la cuenta de dominio de Windows utilizada para administrar la aplicación a través de la API REST. La administración de la aplicación a través de la API REST solo está disponible para este usuario. Introduzca el nombre de usuario con el formato &lt;DOMINIO&gt;\&lt;NombreUsuario&gt; (por ejemplo, RESTAPI_User=EMPRESA\Administrador). Solo puede seleccionar un usuario para que funcione con la API REST.</p> <p>Añadir un nombre de usuario es un requisito previo para poder administrar la aplicación a través de la API REST.</p>
RESTAPI_Port	<p>Puerto utilizado para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782.</p>
RESTAPI_Certificate	<p>Certificado para identificar solicitudes (por ejemplo, RESTAPI_Certificate=C:\cert.pem). La interacción segura de Kaspersky Endpoint Security con el cliente REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga útil de cada solicitud.</p>
ADMINKITCONNECTOR	<p>Administración de aplicaciones mediante sistemas de administración. Los sistemas de administración incluyen, por ejemplo, Kaspersky Security Center. Además de los sistemas de administración de Kaspersky, puede usar soluciones de terceros. Kaspersky Endpoint Security proporciona una API para este fin.</p> <p>Valores disponibles:</p>

- 1: se permite la administración de aplicaciones con la ayuda de sistemas de administración (valor predeterminado).
- 0: se permite la administración de aplicaciones solo a través de la interfaz local.

**Ejemplo:**

```
setup_ks.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_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Cuando concluya la instalación, Kaspersky Endpoint Security se activará con una licencia de prueba (a menos que haya especificado un código de activación en el [archivo setup.ini](#)). La licencia de evaluación suele durar poco tiempo. Cuando finaliza la licencia de evaluación, se desactivan todas las funciones de Kaspersky Endpoint Security. Para continuar usando la aplicación, deberá activarla con una licencia comercial a través del [Asistente de activación de la aplicación](#) o con un [comando especial](#).

Al instalar la aplicación o actualizar la versión de aplicación en el modo silencioso, se admite el uso de los archivos siguientes:

- [Setup.ini](#): configuración general para instalación de la aplicación
- [Install.cfg](#): configuración del funcionamiento de Kaspersky Endpoint Security
- Setup.reg: claves del registro

Las claves del registro del archivo setup.reg se escriben en el registro solo si el valor `setup.reg` está establecido para el parámetro `SetupReg` en el [archivo setup.ini](#). El archivo setup.reg es generado por los expertos de Kaspersky. No se recomienda modificar el contenido de este archivo.

Para aplicar la configuración de los archivos setup.ini, install.cfg, y setup.reg, coloque estos archivos en la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security. También puede colocar el archivo setup.reg en una carpeta diferente. Si lo hace, debe especificar la ruta al archivo en el siguiente comando de instalación de la aplicación: `SETUPREG=<path to the setup.reg file>`.

## Activación de la aplicación

*Para activar la aplicación desde la línea de comandos,*

introduzca la siguiente cadena en la línea de comandos:

```
avp.com license /add <código de activación o archivo clave> [/login=<nombre de usuario> /password=<contraseña>]
```

Las credenciales de la cuenta de usuario (/login=<nombre de usuario> /password=<contraseña>) se necesitan cuando [la protección con contraseña está activada](#).

## Eliminar la aplicación

Kaspersky Endpoint Security se puede desinstalar desde la línea de comandos de los siguientes modos:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que la desinstalación se inicie en el modo silencioso, su participación en el proceso de eliminación ya no se requiere. Para desinstalar la aplicación en modo silencioso, utilice las claves /s y /qn.

*Para desinstalar la aplicación en modo silencioso:*

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

- Si el proceso de eliminación no está [protegido con contraseña](#):

```
setup_kes.exe /s /x
```

o bien

```
msiexec.exe /x <GUID> /qn
```

<GUID> es el id. único de la aplicación. Puede utilizar el siguiente comando para descubrir el GUID de la aplicación:

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

- Si el proceso de eliminación está [protegido con contraseña](#):

```
setup_kes.exe /pKLLOGIN=<nombre de usuario> /pKLASSWD=<contraseña> /s /x
```

o bien

```
msiexec.exe /x <GUID> KLLOGIN=<nombre de usuario> KLPASSWD=<contraseña> /qn
```

Ejemplo:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

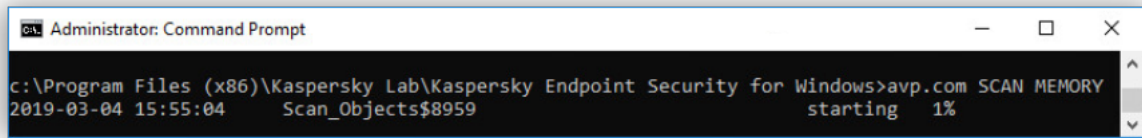
## Comandos AVP

*Para administrar Kaspersky Endpoint Security a través de la línea de comandos:*

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para ejecutar un comando, escriba lo siguiente:

avp.com <comando> [options]

Kaspersky Endpoint Security ejecutará el comando especificado (consulte la siguiente imagen).



Administración de la aplicación desde la línea de comandos

## SCAN. Análisis antivirus

Ejecutar la tarea de análisis antivirus.

### Sintaxis del comando

```
SCAN [<cobertura del análisis>] [<acción al detectar una amenaza>] [<tipos de archivos>] [<exclusiones de análisis>] [/R[A]:<archivo del informe>] [<tecnologías de análisis>] [/C:<archivo de configuración para análisis antivirus>]
```

Cobertura del análisis	
<archivos para analizar>	<p>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:</p> <ul style="list-style-type: none"><li>"C:\Archivos de programa (x86)\Carpeta de ejemplo" (ruta larga).</li><li>C:\ARCHIV~2\CARPET~1 (ruta corta).</li></ul>
/ALL	<p>Ejecutar la tarea <i>Análisis completo</i>. Kaspersky Endpoint Security analiza los siguientes objetos:</p> <ul style="list-style-type: none"><li>Memoria del núcleo;</li><li>Objetos cargados en el inicio del sistema operativo</li><li>Sectores de arranque;</li><li>Copia de seguridad del sistema operativo</li><li>Todas las unidades de disco duro y unidades extraíbles</li></ul>
/MEMORY	Analizar la memoria del núcleo
/STARTUP	Analizar los objetos que se cargan cuando se inicia el sistema operativo
/MAIL	Analizar el buzón de correo de Outlook

/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.
/@:<archivo 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: <ul style="list-style-type: none"> <li>"C:\Archivos de programa (x86)\Carpeta de ejemplo" (ruta larga).</li> <li>C:\ARCHIV~2\CARPET~1 (ruta corta).</li> </ul>

Acción al detectar una amenaza	
/i0	Informar. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.
/i1	Desinfectar; bloquear si la desinfección falla. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección no es posible, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.
/i2	Desinfectar; eliminar si la desinfección falla. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos. Esta acción está seleccionada de forma predeterminada.
/i3	Cuando se detecte un archivo infectado, desinfectarlo. Eliminarlo si no se lo puede desinfectar. También eliminar los archivos compuestos (por ejemplo, los archivos de almacenamiento) cuando un archivo infectado no se pueda desinfectar o eliminar.
/i4	Eliminar los archivos infectados. También eliminar los archivos compuestos (por ejemplo, los archivos de almacenamiento) cuando un archivo infectado no se pueda eliminar.
/i8	Solicitar una acción al usuario en cuanto se detecte una amenaza.
/i9	Solicitar una acción al usuario después de que se complete el análisis.

Tipos de archivos	
/fe	Archivos analizados por extensión. Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . El formato de archivo se determina en función de su extensión.
/fi	Analizar archivos por formato. Si se activa este parámetro, Kaspersky Endpoint Security analiza <a href="#">únicamente los archivos infectables</a> . Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.
/fa	Todos los archivos. Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones).

Esta es la configuración predeterminada.

Exclusiones del análisis	
-e:a	No analizar archivos RAR, ARJ, ZIP, CAB, LHA, JAR ni ICE.
-e:b	No analizar las bases de datos de correo ni los mensajes de correo entrantes o salientes.
-e:<máscara de archivos>	No analizar los archivos que coincidan con la máscara de archivos especificada. Por ejemplo: <ul style="list-style-type: none"><li>• La máscara *.exe comprende las rutas a todos los archivos de extensión exe.</li><li>• La máscara ejemplo* comprende las rutas a todos los archivos de nombre EJEMPLO.</li></ul>
-e:<segundos>	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).

Modo para registrar los eventos en un archivo de informe	
/R:<archivo de informe>	Guardar solo los eventos críticos en el archivo del informe.
/RA:<archivo de informe>	Guardar todos los eventos en el archivo del informe.

Tecnologías de análisis	
/iChecker=on off	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).
/iSwift=on off	Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

Configuración avanzada	
/C:<archivo de configuración de análisis antivirus>	El archivo de configuración de análisis antivirus. Deberá crear este archivo manualmente y guardarlo en formato TXT. Puede incluir lo siguiente: [<cobertura del análisis>] [<acción al detectar una amenaza>] [<tipos de archivos>] [<exclusiones de análisis>] [/R[A]:<archivo del informe>] [<tecnologías de análisis>].



Ejemplo:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

## UPDATE. Actualización de las bases de datos y módulos de la aplicación

Ejecute la tarea de *Actualización*.

### Sintaxis del comando

```
UPDATE [local] ["<origen de actualización>"] [/R[A]:<archivo de informe>] [/C:<archivo con configuración de actualización >]
```

Configuración de la tarea de actualización	
local	<p>Inicio de la tarea de <i>Actualización</i> que se creó automáticamente después de instalar la aplicación. Puede cambiar la configuración de la tarea de <i>Actualización</i> en la interfaz de la aplicación local o en la consola de Kaspersky Security Center. Si esta opción no está configurada, Kaspersky Endpoint Security inicia la tarea de <i>Actualización</i> con la configuración predeterminada o con la configuración especificada en el comando. Puede establecer la configuración de la tarea de Actualización de la siguiente manera:</p> <ul style="list-style-type: none"><li>• UPDATE inicia la tarea de <i>Actualización</i> con la configuración predeterminada: el origen de actualizaciones son los servidores de actualización de Kaspersky, la cuenta es Sistema y otras opciones de configuración predeterminadas.</li><li>• UPDATE local inicia la tarea de <i>Actualización</i> que se creó automáticamente después de la instalación (tarea predefinida).</li><li>• UPDATE &lt;configuración de actualización&gt; inicia la tarea de <i>Actualización</i> con una configuración definida manualmente (ver a continuación).</li></ul>

Origen de actualizaciones	
"<origen de actualizaciones>"	Dirección de un servidor HTTP/FTP o de una carpeta compartida con el paquete de actualización. No es posible especificar más de un origen. Si no se especifica el origen de actualizaciones, Kaspersky Endpoint Security utiliza la fuente predeterminada: los servidores de actualización de Kaspersky.

Modo para registrar los eventos en un archivo de informe	
/R:<archivo de informe>	Guardar solo los eventos críticos en el archivo del informe.
/RA:<archivo de informe>	Guardar todos los eventos en el archivo del informe.

Configuración avanzada	
------------------------	--

/C:<archivo de configuración de actualizaciones>

Archivo con la configuración de la tarea de *Actualización*. Deberá crear este archivo manualmente y guardarlo en formato TXT. Puede incluir lo siguiente: ["<origen de actualizaciones>"] [/R[A]:<archivo de informe>].

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.

### Sintaxis del comando

```
ROLLBACK [/R[A]:<archivo de informe>]
```

### Modo para registrar los eventos en un archivo de informe

/R:<archivo de informe>

Guardar solo los eventos críticos en el archivo del informe.

/RA:<archivo de informe>

Guardar todos los eventos en el archivo del informe.

Ejemplo:

```
avp.com ROLLBACK /RA:rollback.txt
```

## TRACES. Rastreo

Activar o desactivar la función de seguimiento. Los [archivos de seguimiento](#) se almacenan en el equipo siempre que la aplicación esté en uso y se eliminan permanentemente cuando se quita la aplicación. Los archivos de seguimiento —exceptuados los del Agente de autenticación— se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. De manera predeterminada, la función está deshabilitada.

### Sintaxis del comando

```
TRACES on|off [<nivel de seguimiento>] [<configuración avanzada>]
```

### Nivel de seguimiento

<nivel de seguimiento>

Nivel de detalle del seguimiento. Valores disponibles:

- **100** (crítico). Solo mensajes sobre errores graves.
- **200** (alto). Mensajes sobre todos los errores, incluidos los errores graves.

- **300** (diagnóstico). Mensajes sobre todos los errores, además de las advertencias.
- **400** (importante). Todos los mensajes de error y de advertencia, así como otra información adicional.
- **500** (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado).
- **600** (bajo). Todos los mensajes.

Configuración avanzada	
all	Ejecutar un comando con los parámetros <code>dbg</code> , <code>file</code> y <code>mem</code> .
dbg	Usar la función <code>OutputDebugString</code> y guardar el archivo de seguimiento. La función <code>OutputDebugString</code> le envía una cadena de caracteres al depurador de la aplicación para que se la muestre en pantalla. Para más detalles, visite el <a href="#">sitio web de MSDN</a> .
file	Guardar un archivo de seguimiento (sin límite de tamaño).
rot	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.
mem	Guardar datos de seguimiento en archivos de volcado.

#### Ejemplos:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

## START. Iniciar un perfil

Iniciar un perfil (por ejemplo, para actualizar las bases de datos o activar un componente de protección).

#### Sintaxis del comando

```
START <perfil> [/R[A]:<archivo de informe>]
```

Perfil	
<perfil>	Nombre de perfil. Un <i>perfil</i> es un componente, tarea o característica de Kaspersky Endpoint Security. Para ver la lista de <a href="#">perfiles</a> disponibles, utilice el comando <code>HELP START</code> .

<b>Modo para registrar los eventos en un archivo de informe</b>	
/R:<archivo de informe>	Guardar solo los eventos críticos en el archivo del informe.
/RA:<archivo de informe>	Guardar todos los eventos en el archivo del informe.

Ejemplo:  
avp.com START Scan\_Objects

## STOP. Detener un perfil

Detener el perfil que se está ejecutando (por ejemplo, detener un análisis, un componente de protección o un análisis de unidades extraíbles).

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe contar con los permisos **Desactivar componentes de protección** y **Desactivar componentes de control**.

### Sintaxis del comando

```
STOP <perfil> /login=<nombre de usuario> /password=<contraseña>
```

<b>Perfil</b>	
<perfil>	Nombre de perfil. Un <i>perfil</i> es un componente, tarea o característica de Kaspersky Endpoint Security. Para ver la lista de <a href="#">perfiles</a> disponibles, utilice el comando <code>HELP STOP</code> .

<b>Autenticación</b>	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de cuenta de usuario con los permisos de <a href="#">protección con contraseña</a> requeridos.

## STATUS. Estado del perfil

Mostrar en qué estado se encuentran los [perfiles de la aplicación](#) (por ejemplo, `en ejecución` o `terminado`). Para ver la lista de perfiles disponibles, utilice el comando `HELP STATUS`.

Kaspersky Endpoint Security también muestra el estado de los perfiles de servicio. Puede que necesite esta información si se comunica con el Soporte técnico de Kaspersky.

### Sintaxis del comando

```
avp.com STATUS [<perfil>]
```

Si introduce el comando sin un perfil, Kaspersky Endpoint Security muestra el estado de todos los perfiles de la aplicación.

## STATISTICS. Estadísticas sobre el funcionamiento de los perfiles

Ver información estadística sobre alguno de los [perfiles de la aplicación](#) (por ejemplo, la duración de un análisis o la cantidad de amenazas detectadas.) Puede ver la lista de perfiles disponibles mediante el comando `HELP STATISTICS`.

### Sintaxis del comando

```
STATISTICS <perfil>
```

## RESTORE. Restauración de archivos de Copia de seguridad

De ser necesario, puede restaurar un archivo almacenado en Copia de seguridad a su carpeta original. Si en la ruta especificada ya existe un archivo con el mismo nombre, se añade el sufijo "-copy" al nombre de ese archivo. El archivo restaurado se guarda con su nombre original.

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Restaurar desde copia de seguridad**.

*Copias de seguridad* almacena copias de seguridad de los archivos que se modificaron o eliminaron durante la desinfección. Una *copia de seguridad* es una copia del archivo creada antes de que el archivo se desinfectara o se eliminara. Las copias de seguridad de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. El usuario cuya cuenta se usó para instalar la Kaspersky Endpoint Security tiene derechos de acceso limitado a esta carpeta.

Kaspersky Endpoint Security no ofrece la posibilidad de configurar permisos de acceso de usuario a copias de seguridad de los archivos.

### Sintaxis del comando

```
RESTORE [/REPLACE] <nombre de archivo> /login=<nombre de usuario> /password=  
<contraseña>
```

Configuración avanzada	
/REPLACE	Si el archivo ya existe, sobrescribirlo.
<nombre de archivo>	Nombre del archivo que se va a restaurar.

Autenticación	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de cuenta de usuario con los permisos de <a href="#">protección con contraseña</a> requeridos.

#### Ejemplo:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

## EXPORT. Exportar ajustes de la aplicación

Exportar ajustes de configuración de Kaspersky Endpoint Security a un archivo. El archivo se guardará en la carpeta C:\Windows\SysWOW64.

#### Sintaxis del comando

```
EXPORT <perfil> <nombre de archivo>
```

<b>Perfil</b>	
<perfil>	Nombre de perfil. Un <i>perfil</i> es un componente, tarea o característica de Kaspersky Endpoint Security. Para ver la lista de <a href="#">perfiles</a> disponibles, utilice el comando <code>HELP EXPORT</code> .

<b>Archivo para la exportación</b>	
<nombre de archivo>	Nombre del archivo en el que se guardarán los ajustes de configuración exportados. 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.

#### Ejemplos:

- avp.com EXPORT ids ids\_config.dat
- avp.com EXPORT fm fm\_config.txt

## IMPORT. Importar configuración de la aplicación

Importar en Kaspersky Endpoint Security la configuración que se guardó en un archivo creado con el comando `EXPORT`.

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Configurar parámetros de la aplicación**.

#### Sintaxis del comando

```
IMPORT <nombre de archivo> /login=<nombre de usuario> /password=<contraseña>
```

<b>Archivo para importar</b>	
------------------------------	--

<nombre de archivo>	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.
---------------------	--

<b>Autenticación</b>	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de cuenta de usuario con los permisos de <a href="#">protección con contraseña</a> requeridos.

Ejemplo:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

## ADDKEY. Aplicar un archivo clave.

Aplicar un archivo clave para activar Kaspersky Endpoint Security. Si la aplicación ya está activada, la clave se añade como clave de reserva.

### Sintaxis del comando

```
ADDKEY <nombre de archivo> /login=<nombre de usuario>/password=<contraseña>
```

<b>Archivo clave</b>	
<nombre de archivo>	Nombre del archivo clave.

<b>Autenticación</b>	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de una cuenta de usuario. Estos datos solo se necesitan si la <a href="#">protección con contraseña</a> está activada.

Ejemplo:

```
avp.com ADDKEY file.key
```

## LICENSE. Administración de licencias

Realizar operaciones con las claves de licencia de Kaspersky Endpoint Security.

Para ejecutar este comando y eliminar una clave de licencia, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Quitar clave**.

### Sintaxis del comando

```
LICENSE <operación> [/login=<nombre de usuario> /password=<contraseña>]
```

<b>Operación</b>	
------------------	--

/ADD <nombre de archivo>	Aplicar un archivo clave para activar Kaspersky Endpoint Security. Si la aplicación ya está activada, la clave se añade como clave de reserva.
/ADD <código de activación>	Activar Kaspersky Endpoint Security con un código de activación. Si la aplicación ya está activada, la clave se añade como clave de reserva.
/REFRESH <nombre de archivo>	Renovar la licencia usando un archivo clave. Se añade una clave de reserva como resultado. Se activa cuando caduca la licencia. El comando no se puede utilizar para añadir una clave activa.
/REFRESH <código de activación>	Renovar la licencia usando un código de activación. Se añade una clave de reserva como resultado. Se activa cuando caduca la licencia. El comando no se puede utilizar para añadir una clave activa.
/DEL /login=<nombre de usuario> /password= <contraseña>	Quitar una clave de licencia. La clave de licencia de reserva también se quitará.

<b>Autenticación</b>	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de cuenta de usuario con los permisos de <a href="#">protección con contraseña</a> requeridos.

#### Ejemplo:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCC-DDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

## RENEW. Compra de una licencia

Abrir el sitio web de Kaspersky para comprar o renovar una licencia.

## PBATESTRESET. Restablecer los resultados de la comprobación de disco antes de cifrar el disco

Restablezca los resultados de la comprobación de compatibilidad para el Cifrado de disco completo (FDE), incluidas las tecnologías Cifrado de disco de Kaspersky y Cifrado de unidad BitLocker.

Antes de aplicar el cifrado de disco completo, la aplicación realiza una serie de pruebas para verificar si el equipo puede cifrarse. Si el equipo no es compatible con el Cifrado de disco completo (FDE), Kaspersky Endpoint Security deja constancia de la incompatibilidad. Si se intenta realizar una nueva operación de cifrado, la aplicación omite la verificación y simplemente advierte que el cifrado no puede aplicarse. Esto significa que, ante un cambio en la configuración de hardware del equipo, los resultados de la verificación deben descartarse, y se debe volver a comprobar si el disco duro del equipo es compatible con las tecnologías Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker.



## EXIT. Salir de la aplicación

Cerrar Kaspersky Endpoint Security. La aplicación se descargará de la RAM del equipo.

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Salir de la aplicación**.

### Sintaxis del comando

```
EXIT /login=<nombre de usuario> /password=<contraseña>
```

## EXITPOLICY. Desactivar una directiva

Desactivar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse.

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Desactivar la directiva de Kaspersky Security Center**.

### Sintaxis del comando

```
EXITPOLICY /login=<nombre de usuario> /password=<contraseña>
```

## STARTPOLICY. Activar una directiva

Activar una directiva de Kaspersky Security Center en el equipo. Los parámetros de la aplicación tomarán los valores que indique la directiva.

## DISABLE. Desactivar la protección

Desactivar el componente Protección frente a amenazas en archivos si la licencia de Kaspersky Endpoint Security ha caducado. No podrá ejecutar este comando si la aplicación no se ha activado en el equipo o la licencia aún es válida.

## SPYWARE. Detección de spyware

Activar o desactivar la detección de spyware. De manera predeterminada, la detección de spyware está activada.

### Sintaxis del comando

SPYWARE on|off

## KSN. Transición de KSN global/privada

Selección de una solución de Kaspersky Security Network para determinar la reputación de archivos o sitios web. Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura de KSN:

- *KSN Global*. Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky Security Network y, a su vez, envían a Kaspersky información sobre los objetos que se detectan en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos de Kaspersky Security Network.
- *KSN privada*. Esta es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky Security Network y a otros datos estadísticos sin enviar datos a KSN desde sus propios equipos. KSN Privada se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:
  - porque las estaciones de trabajo locales no tienen acceso a Internet;
  - porque, por motivos legales o debido a las políticas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

### Sintaxis del comando

```
KSN /global | /private <nombre del archivo>
```

<b>Archivo de configuración de KSN privada</b>	
<nombre de archivo>	Nombre del archivo de configuración que contiene la configuración del servidor proxy KSN. Este archivo tiene la extensión PKCS7 o PEM.

#### Ejemplo:

```
avp.com KSN /global
```

```
avp.com KSN/privado C:/ksn_config.pkcs7
```

## Comandos KESCLI

Los comandos KESCLI le permiten recibir información sobre el estado de la protección del equipo con el componente OPSWAT y realizar tareas habituales, como análisis antivirus y actualizaciones de bases de datos.

Puede consultar la lista de comandos KESCLI mediante el comando `--help` o el comando abreviado `-h`.

*Para administrar Kaspersky Endpoint Security a través de la línea de comandos:*

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para ejecutar un comando, escriba lo siguiente:

```
kescli <comando> [opciones]
```

Kaspersky Endpoint Security ejecutará el comando especificado (consulte la siguiente imagen).

```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File"      1      3/16/2021 17:14:37      "https://secure.eicar.org/eicar.com.txt"      41      1
"EICAR-Test-File"      1      3/16/2021 17:14:38      "https://www.eicar.org/download/eicar.com"      41      1
```

Administración de la aplicación desde la línea de comandos

## Scan. Análisis antivirus

Ejecutar la tarea de análisis antivirus.

### Sintaxis del comando

```
kescli --opswat Scan "<cobertura del análisis>" <acción al detectar una amenaza>
```

Puede verificar el estado de finalización de la tarea de *Análisis completo* con el comando [GetScanState](#) y consultar la fecha y la hora en la que se completó por última vez con el comando [GetLastScanTime](#).

<b>Cobertura del análisis</b>	
<archivos para analizar>	Lista de archivos y carpetas, separados con ; (punto y coma). Por ejemplo: "C:\Program Files (x86)\Example Folder".

<b>Acción al detectar una amenaza</b>	
0	Informar. Si se selecciona esta opción, Kaspersky Endpoint Security añade información sobre los archivos infectados a la lista de amenazas activas al detectarlos.
1	Desinfectar; eliminar si la desinfección falla. Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.  Esta acción está seleccionada de forma predeterminada.

Ejemplo:

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

## GetScanState. Estado de finalización del análisis

Reciba información sobre el estado de finalización de la tarea de *Análisis completo*:

- 1: el análisis está en proceso.
- 0: no se está ejecutando el análisis.

### Sintaxis del comando

```
--opswat GetScanState
```

### Ejemplo:

```
kescli --opswat GetScanState
```

## GetLastScanTime. Especificación del tiempo para completar el análisis

Reciba información sobre la fecha y hora de la última instancia en la que se completó la tarea de *Análisis completo*.

### Sintaxis del comando

```
--opswat GetLastScanTime
```

### Ejemplo:

```
kescli --opswat GetLastScanTime
```

## GetThreats. Obtención de datos sobre amenazas detectadas

Reciba una lista de las amenazas detectadas (*Informe de amenazas*). En este informe, encontrará información sobre amenazas y la actividad de virus durante los últimos 30 días previos a la creación del informe.

### Sintaxis del comando

```
--opswat GetThreats
```

Al ejecutar este comando, Kaspersky Endpoint Security enviará una respuesta con el siguiente formato:

```
<nombre del objeto detectado> <tipo de objeto> <fecha y hora de la detección> <ruta del  
archivo> <acción al detectar una amenaza> <nivel de peligro de la amenaza>
```

```

Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File"      1      3/16/2021 17:14:37      "https://secure.eicar.org/eicar.com.txt"      41      1
"EICAR-Test-File"      1      3/16/2021 17:14:38      "https://www.eicar.org/download/eicar.com"      41      1

```

Administración de la aplicación desde la línea de comandos

Tipo de objeto	
0	Desconocido (Desconocido).
1	Virus (Virware).
2	Programas troyanos (Trojware).
3	Programas maliciosos (Software malicioso).
4	Programas de anuncios (Software publicitario).
5	Programas de marcado automático (Pornware).
6	Aplicaciones que puede utilizar un ciberdelincuente para hacerle daño al equipo o los datos del usuario (Riskware).
7	Objetos comprimidos cuyo método de compresión puede usarse para proteger código malicioso (Packed).
20	Objetos desconocidos (Archivos x).
21	Aplicaciones conocidas (Software).
22	Archivos ocultos (Oculto).
23	Aplicaciones que solicitan atención (Programa potencialmente no deseado [PUP]).
24	Comportamiento extraño (Anomalía).
30	Sin determinar (Sin detectar).
40	Banners de anuncios (Banner).
50	Ataque de red (Ataque).
51	Acceso a registros (Registro).
52	Actividad sospechosa (Sospecha).
60	Vulnerabilidades (Vulnerabilidad).
70	Phishing.
80	Archivo adjunto no deseado en correos electrónicos (Archivo adjunto).
90	Software malicioso detectado por Kaspersky Security Network (Urgente).
100	Enlace desconocido (URL sospechosa).
110	Otro software malicioso (Comportamiento).

Acción al detectar una amenaza	
0	Desconocido (desconocido).

1	Se resolvió la amenaza (listo).
2	Se infectó el objeto infectado y no se lo desinfectó (infectado).
5	No se desinfectó el objeto en carpeta comprimida (comprimido).
9	Se desinfectó el objeto (desinfectado).
10	No se desinfectó el objeto (sin desinfectar).
11	Se eliminó el objeto (eliminado).
13	Se creó una copia de seguridad del objeto (en copia de seguridad).
15	Se movió el objeto a Copia de seguridad (en cuarentena).
23	Se eliminó el objeto al reiniciar el equipo (eliminar al reiniciar).
25	Se desinfectó el objeto al reiniciar el equipo (desinfectar al reiniciar).
29	Se movió el objeto a Copia de seguridad por el usuario (añadido por el usuario).
30	Se añadió el objeto a las exclusiones (añadido para excluir).
31	Se movió el objeto a Copia de seguridad al reiniciar el equipo (en cuarentena al reiniciar).
36	Falso positivo (falsa alarma).
38	Se finalizó el proceso (finalizado).
40	No se detectó el objeto (sin hallar).
41	No se ha podido resolver la amenaza (sin analizar).
42	Se restauró el objeto (deshacer).
43	Se creó el objeto a partir de la actividad de amenazas (generado por una amenaza).
44	Se restauró el objeto al reiniciar el equipo (deshacer al reiniciar).
0xffffffff	No se procesó el objeto (desechado).

Nivel de peligro de la amenaza	
0	Desconocido
1	Máximo
2	Análisis medio
4	Mínimo
8	Información (menor que <i>mínimo</i> )

## UpdateDefinitions. Actualización de las bases de datos y módulos de la aplicación

Ejecute la tarea de *Actualización*. Kaspersky Endpoint Security emplea una fuente predeterminada: los servidores de actualización de Kaspersky.

#### Sintaxis del comando

```
--opswat UpdateDefinitions
```

Puede consultar la fecha y hora en la que se completó la última tarea de *Actualización* con el comando [GetDefinitionsetState](#).

#### Ejemplo:

```
kescli --opswat UpdateDefinitions
```

## GetDefinitionState. Especificación del tiempo para completar la actualización

Reciba información sobre la fecha y hora de la última instancia en la que se completó la tarea de *Actualización*.

#### Sintaxis del comando

```
--opswat GetDefinitionState
```

#### Ejemplo:

```
kescli --opswat GetDefinitionState
```

## EnableRTP. Activación de la protección

Active los componentes de protección de Kaspersky Endpoint Security en el equipo: Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red y Prevención de intrusiones en el host.

#### Sintaxis del comando

```
--opswat EnableRTP
```

Puede verificar el estado de funcionamiento del componente Protección frente a amenazas en archivos con el comando [GetRealTimeProtectionState](#).

#### Ejemplo:

```
kescli --opswat EnableRTP
```

## GetRealTimeProtectionState. Estado de la Protección frente a amenazas en archivos

Reciba información sobre el estado de funcionamiento del componente Protección frente a amenazas en archivos:

- 1: el componente está activado.

- 0: el componente está desactivado.

#### Sintaxis del comando

```
--opswat GetRealTimeProtectionState
```

#### Ejemplo:

```
kescli --opswat GetRealTimeProtectionState
```

## Version. Identificación de la versión de la aplicación

Identifique la versión de Kaspersky Endpoint Security para Windows.

#### Sintaxis del comando

```
--Version
```

También puede emplear el comando abreviado `-v`.

#### Ejemplo:

```
kescli -v
```

## Comandos de administración de Detection and Response

Puede utilizar la línea de comandos para administrar la funcionalidad integrada de las soluciones de Detection and Response (por ejemplo, Kaspersky Sandbox o Kaspersky Endpoint Detection and Response Optimum). Puede administrar las soluciones de Detection and Response si la administración mediante la consola de Kaspersky Security Center no es posible. Para ver la lista de comandos de administración disponibles, utilice el comando `HELP`. Para conocer la sintaxis de un comando específico, escriba `HELP <comando>`.

*Para administrar las funciones integradas de las soluciones de Detection and Response mediante la línea de comando, haga lo siguiente:*

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para ejecutar un comando, escriba lo siguiente:

```
avp.com <comando> [options]
```

Kaspersky Endpoint Security ejecutará el comando especificado (consulte la siguiente imagen).

## SANDBOX. Administrar Kaspersky Sandbox



## Comandos para administrar el componente Kaspersky Sandbox:

- Active o desactive el componente Kaspersky Sandbox.

El componente Kaspersky Sandbox permite la interoperabilidad con la solución Kaspersky Sandbox.

- Configure el componente Kaspersky Sandbox:

- Conecte el equipo a los servidores de Kaspersky Sandbox.

Los servidores utilizan imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows para ejecutar objetos que se deben analizar. Puede introducir una dirección IP (IPv4 o IPv6) o un nombre de dominio completo. Para obtener detalles sobre la implementación de imágenes virtuales y la configuración de los servidores de Kaspersky Sandbox, consulte la [Ayuda de Kaspersky Sandbox](#).

- Configure el tiempo de espera de la conexión para el servidor Kaspersky Sandbox.

Tiempo de espera para recibir una respuesta a una solicitud de análisis de objetos del servidor de Kaspersky Sandbox. Una vez transcurrido el tiempo de espera, Kaspersky Sandbox redirige la solicitud al siguiente servidor. El valor del tiempo de espera depende de la velocidad y la estabilidad de la conexión. El valor predeterminado es 5 segundos.

- Configure una conexión confiable entre el equipo y los servidores de Kaspersky Sandbox.

Para configurar una conexión de confianza con los servidores de Kaspersky Sandbox, debe preparar un certificado TLS. A continuación, debe añadir el certificado a los servidores de Kaspersky Sandbox y la directiva de Kaspersky Endpoint Security. Para obtener información sobre cómo preparar el certificado y añadirlo a los servidores, consulte la [Ayuda de Kaspersky Sandbox](#).

- Muestra la configuración actual del componente.

### Sintaxis del comando

```
stop sandbox [/login=<nombre de usuario> /password=<contraseña>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<dirección del servidor>:<puerto>] [--timeout=
<Tiempo de espera de conexión del servidor de Kaspersky Sandbox (ms)>] [--pinned-
certificate=<ruta del certificado TLS>][/login=<nombre de usuario> /password=
<contraseña>]
sandbox /show
```

Operación	
stop	Desactive el componente Kaspersky Sandbox.
start	Active el componente Kaspersky Sandbox.
set	Configure el componente Kaspersky Sandbox. La configuración que puede modificar es la siguiente: <ul style="list-style-type: none"><li>• Utilice una conexión de confianza (--tls);</li><li>• Añada un certificado TLS (--pinned-certificate);</li><li>• Configure el tiempo de espera de la conexión del servidor de Kaspersky Sandbox (--timeout);</li><li>• Añada servidores de Kaspersky Sandbox (--servers).</li></ul>
show	Muestra la configuración actual del componente. Obtiene la siguiente respuesta:

```
sandbox.timeout=<tiempo de espera de conexión del servidor de Kaspersky Sandbox (ms)>
sandbox.tls=<estado de la conexión de confianza>
Sandbox.servers=<lista de servidores de Kaspersky Sandbox>
```

#### Autenticación

```
/login=<nombre de usuario>
/password=<contraseña>
```

Credenciales de cuenta de usuario con los permisos de [protección con contraseña](#) requeridos.

#### Ejemplo:

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

## PREVENCIÓN. Administración de la prevención de ejecución

Desactive la Prevención de ejecución o muestre la configuración del componente actual, incluida la lista de reglas de prevención de ejecución.

#### Sintaxis del comando

```
prevention disable
prevention /show
```

Cuando ejecute el comando `prevention /show`, obtendrá la siguiente respuesta:

```
prevention.enable=true|false
```

```
prevention.mode=audit|prevent
```

```
prevention.rules
```

```
id: <id de la regla>
```

```
target: script|process|document
```

```
md5: <hash MD5 del archivo>
```

```
sha256: <hash SHA256 del archivo>
```

```
pattern: <ruta del objeto>
```

```
case-sensitive: true|false
```

Valores de retorno de comando:

- -1 significa que el comando no es compatible con la versión de Kaspersky Endpoint Security que está instalada en el dispositivo.
- 0 significa que el comando se ejecutó correctamente.
- 1 significa que no se pasó un argumento obligatorio al comando.
- 2 significa que ocurrió un error general.

- 4 significa que hubo un error de sintaxis.
- 9: operación incorrecta (por ejemplo, un intento de desactivar el componente cuando ya está desactivado).

## AISLAMIENTO. Administrar el aislamiento de red

Desactive Aislamiento de red en el equipo o muestre la configuración actual del componente. La configuración del componente también incluye una lista de conexiones de red añadidas a exclusiones.

Sintaxis del comando:

```
isolation /OFF /login=<nombre de usuario> /password=<contraseña>
isolation /STAT
```

Como resultado de ejecutar el comando `stat`, recibe la siguiente respuesta: `Network isolation on|off`.

## RESTORE. Restauración de archivos de la cuarentena

Puede restaurar un archivo almacenado en Cuarentena a su carpeta de origen. Si se ha eliminado la carpeta de destino, la aplicación coloca el archivo en una carpeta especial en el equipo. Luego, debe mover el archivo manualmente a la carpeta de destino. La *cuarentena* es un almacén local especial en el equipo donde se envían los archivos infectados por virus o los archivos no desinfectables. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la cuarentena solo cuando trabaja con las soluciones Kaspersky Sandbox y Kaspersky Endpoint 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](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

Para ejecutar este comando, es necesario que [la protección con contraseña esté activada](#). El usuario debe tener el permiso **Restaurar desde copia de seguridad**.

El objeto se pone en cuarentena en la cuenta del sistema (SYSTEM).

Sintaxis del comando

```
RESTORE [/REPLACE] <nombre de archivo> /login=<nombre de usuario> /password=
<contraseña>
```

Configuración avanzada	
/REPLACE	Si el archivo ya existe, sobrescribirlo.
<nombre de archivo>	Nombre del archivo que se va a restaurar.

Autenticación	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de cuenta de usuario con los permisos de <a href="#">protección con contraseña</a> requeridos.

#### Ejemplo:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

Valores de retorno de comando:

- -1 significa que el comando no es compatible con la versión de Kaspersky Endpoint Security que está instalada en el dispositivo.
- 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)

Ejecute la tarea Analizar en busca de indicadores de compromiso (IOC). Un *Indicador de compromiso (IOC)* es un conjunto de datos sobre un objeto o actividad que indica el acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. Las tareas de *Análisis de IOC* permiten encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta a la amenaza.

#### Sintaxis del comando

```
IOCSCAN <ruta completa al archivo de IOC>[/path=<ruta a la carpeta de archivos de IOC>
[/process=on|off] [/hint=<ruta completa al archivo ejecutable de un proceso|ruta
completa del archivo>] [/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=<fecha de publicación del evento>] [/channels=<lista de
canales>] [/files=on|off] [/drives=<todos|sistema|críticos|personalizados>]
[/excludes=<lista de exclusiones>][scope=<lista de carpetas para analizar>]
```

Archivos IOC	
<ruta completa al archivo de IOC>	Ruta completa al archivo de IOC que desea utilizar para el análisis. Puede especificar varios archivos IOC separados por espacios. La ruta completa al archivo de IOC se debe introducir sin el argumento /path. Por ejemplo, C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<ruta a la carpeta con archivos IOC>	Ruta a la carpeta con archivos IOC que desea usar para el análisis. Los <i>archivos IOC</i> son archivos que contienen los conjuntos de indicadores que la aplicación intenta hacer coincidir para contar una detección. Los archivos IOC deben cumplir con el <a href="#">estándar OpenIOC</a> . Por ejemplo, C:\Users\Admin\Desktop\IOC

Tipo de datos para análisis de IOC	
/process=on off	Analice los datos del proceso al realizar el análisis de IOC (término ProcessItem).

	<p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza los procesos que se ejecutan en el ordenador al realizar el análisis. Si el archivo de IOC contiene términos de IOC del documento de IOC <code>ProcessItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del proceso solo si el documento de IOC <code>ProcessItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/hint=&lt;ruta completa al archivo ejecutable del proceso ruta completa al archivo&gt;</code></p>	<p>Analice los datos del archivo al realizar el análisis de IOC (términos <code>ProcessItem</code> y <code>FileItem</code>).</p> <p>Puede seleccionar el archivo de una de las siguientes formas:</p> <ul style="list-style-type: none"> <li>• <code>&lt;ruta completa al archivo ejecutable del proceso&gt;</code> – <code>ProcessItem</code>;</li> <li>• <code>&lt;ruta completa al archivo&gt;</code> – <code>FileItem</code>.</li> </ul>
<p><code>/registry=on off</code></p>	<p>Analice los datos del registro de Windows al realizar un análisis de IOC (término <code>RegistryItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza el registro de Windows. Si el archivo de IOC contiene términos del documento de IOC <code>RegistryItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza el registro de Windows solo si el documento de IOC de <code>RegistryItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p> <p>Para el tipo de datos <code>RegistryItem</code>, Kaspersky Endpoint Security analiza <a href="#">un grupo de claves de registro</a>.</p>
<p><code>/dnsentry=on off</code></p>	<p>Analice los datos sobre los registros en la caché de DNS local al realizar el análisis de IOC (término <code>DnsEntryItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza la caché de DNS local. Si el archivo de IOC contiene términos del documento de IOC <code>DnsEntryItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza la caché de DNS local solo si el documento de IOC <code>DnsEntryItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/arpentry=on off</code></p>	<p>Analice los datos sobre los registros en la tabla ARP al realizar el análisis de IOC (término <code>ArpEntryItem</code>).</p>

	<p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza la tabla ARP. Si el archivo de IOC contiene términos del documento de IOC <code>ArpEntryItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza la tabla ARP solo si el documento de IOC de <code>ArpEntryItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/ports=on off</code></p>	<p>Analice los datos sobre los puertos abiertos para escuchar al realizar el análisis de IOC (término <code>PortItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, 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 <code>PortItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza la tabla de conexiones activas solo si el documento de IOC <code>PortItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/services=on off</code></p>	<p>Analice los datos sobre los servicios instalados en el dispositivo al realizar el análisis de IOC (término <code>ServiceItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, 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 <code>ServiceItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del servicio solo si el documento de IOC de <code>ServiceItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/system=on off</code></p>	<p>Analice los datos del entorno al realizar el análisis de IOC (término <code>SystemInfoItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza los datos del entorno. Si el archivo de IOC contiene términos del documento de IOC <code>SystemInfoItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del entorno solo si el documento de IOC <code>SystemInfoItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/users=on off</code></p>	<p>Analice los datos sobre los usuarios al realizar el análisis de IOC (término <code>UserItem</code>).</p>

	<p>Si el valor del argumento es <code>off</code>, 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 <code>UserItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>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 <code>UserItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/volumes=on off</code></p>	<p>Analice datos sobre volúmenes al realizar el análisis de IOC (término <code>VolumItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza los datos sobre los volúmenes del dispositivo. Si el archivo de IOC contiene términos del documento de IOC <code>VolumItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza los datos del volumen solo si el documento de IOC de <code>VolumItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/eventlog=on off</code></p>	<p>Analice los datos sobre los registros en el registro de eventos de Windows al realizar el análisis de IOC (término <code>EventLogItem</code>).</p> <p>Si el valor del argumento es <code>off</code>, Kaspersky Endpoint Security no analiza los registros del registro de eventos de Windows. Si el archivo de IOC contiene términos del documento de IOC <code>EventLogItem</code>, estos se ignoran (se detectan como no coincidentes).</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza el registro de eventos de Windows si el documento de IOC <code>EventLogItem</code> se describe en el archivo de IOC que se proporciona para el análisis.</p>
<p><code>/datetime=&lt;fecha de publicación del evento&gt;</code></p>	<p>Tenga en cuenta la fecha en la que se publicó el evento en el registro de eventos de Windows al determinar la cobertura de análisis de IOC para el documento de IOC correspondiente.</p> <p>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.</p> <p>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.</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza los eventos con cualquier fecha de publicación. La configuración <code>TaskSettings::BaseSettings::EventLogItem::datetime</code> no se puede editar.</p>

	<p>La configuración se utiliza solo si el documento de IOC EventLogItem se describe en el archivo de IOC proporcionado para el análisis.</p>
<p>/channel=&lt;lista de canales&gt;</p>	<p>Lista de nombres de canales (registros) para los que desea realizar un análisis de IOC.</p> <p>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.</p> <p>El nombre del registro se especifica como una cadena de acuerdo con el nombre del registro (canal) especificado en las propiedades del registro (el parámetro de Nombre completo) o en las propiedades del evento (el parámetro &lt;Canal&gt;/&lt;/Canal&gt; en el esquema xml del evento). Puede especificar varios canales separados por espacios.</p> <p>Si no se especifica el argumento, Kaspersky Endpoint Security analiza los registros en busca de canales <b>Aplicación, Sistema, Seguridad</b>.</p>
<p>/files=on off</p>	<p>Analice los datos del archivo al realizar el análisis de IOC (término FileItem).</p> <p>Si el valor del argumento es off, Kaspersky Endpoint Security no analiza los datos del archivo. Si el archivo de IOC contiene términos del documento de IOC FileItem, estos se ignoran (se detectan como no coincidentes).</p> <p>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.</p>
<p>/drives= &lt;todos sistema críticos personalizados&gt;</p>	<p>Establezca la cobertura de análisis de IOC al analizar los datos para el documento de IOC de FileItem.</p> <p>Puede establecer los siguientes valores para la cobertura del análisis:</p> <ul style="list-style-type: none"> <li>• &lt;todos&gt; para todas las coberturas de archivo disponibles.</li> <li>• &lt;sistema&gt; para archivos en carpetas donde está instalado el sistema operativo.</li> <li>• &lt;críticos&gt; para archivos temporales en carpetas de usuario y del sistema.</li> <li>• &lt;personalizado&gt; para archivos en alcances definidos por el usuario (/scope=&lt;lista de carpetas para analizar&gt;).</li> </ul> <p>Si no se especifica el argumento, el análisis se realiza para áreas críticas.</p>
<p>/excludes=&lt;lista de exclusiones&gt;</p>	<p>Establezca la cobertura de la exclusión al analizar los datos del documento de IOC de FileItem. Puede especificar varias rutas separadas por espacios.</p>
<p>/scope=&lt;lista de carpetas para</p>	<p>Alcance del análisis de IOC definido por el usuario al</p>



analizar>

analizar los datos para el documento de IOC de Fileitem (/drives=custom). Puede especificar varias rutas separadas por espacios.

Valores de retorno de comando:

- -1 significa que el comando no es compatible con la versión de Kaspersky Endpoint Agent que está instalada en el dispositivo.
- 0 significa que el comando se ejecutó correctamente.
- 1 significa que no se pasó un argumento obligatorio al comando.
- 2 significa que ocurrió un error general.
- 4 significa que hubo un error de sintaxis.

Si el comando se ejecutó correctamente (valor devuelto 0) y se detectaron indicadores de compromiso en el camino, Kaspersky Endpoint Security envía la siguiente información del resultado de la tarea a la línea de comandos:

Uuid	Id. del archivo de IOC desde el encabezado de la estructura del archivo de IOC (la etiqueta <ioc id="">)
Nombre	Descripción del archivo de IOC desde el encabezado de la estructura del archivo de IOC (la etiqueta <descripción></descripción>)
Elementos de indicador coincidentes	Lista de id. de todos los indicadores coincidentes.
Objetos coincidentes	Datos para cada documento de IOC para el que hubo una coincidencia.

## MDRLICENSE. Activación MDR

Realice operaciones con el archivo de configuración BLOB para activar Managed Detection and Response. El archivo BLOB contiene el ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra dentro del archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en Kaspersky Managed Detection and Response Console. Para obtener información detallada sobre un archivo BLOB, consulte la [Ayuda de Kaspersky Managed Detection and Response](#).

Se requieren privilegios de administrador para realizar operaciones con un archivo BLOB. La configuración de Managed Detection and Response en la directiva también debe estar disponible para su edición (🔑).

### Sintaxis del comando

```
MDRLICENSE <operación> [/login=<nombre de usuario> /password=<contraseña>]
```

Operación	
/ADD	Aplique el archivo de configuración BLOB para la integración con Kaspersky Managed

<nombre de archivo>	Detection and Response (formato de archivo P7). Puede aplicar solo un archivo BLOB. Si ya se añadió un archivo BLOB al equipo, se reemplazará el archivo.
/DEL	Elimina el archivo de configuración BLOB.

<b>Autenticación</b>	
/login=<nombre de usuario> /password=<contraseña>	Credenciales de cuenta de usuario con los permisos de <a href="#">protección con contraseña</a> requeridos.

#### Ejemplo:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

## 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: No se puede iniciar la tarea 'EntAppControl'`. Del mismo modo, Kaspersky Endpoint Security puede mostrar un código como `error=8947906D` (consulte la siguiente tabla).

#### Códigos de error

Código de error	Descripción
09479001	La clave de licencia de Kaspersky Endpoint Security ya se está utilizando en este equipo.
0947901D	La licencia ha caducado. No es posible actualizar las bases de datos.
89479002	No se encuentra la clave.
89479003	Falta la firma digital o está dañada.
89479004	Datos dañados.
89479005	Archivo clave dañado.
89479006	Licencia o clave de licencia caducada.
89479007	No se ha especificado el archivo clave.
89479008	No se puede aplicar el archivo clave.
89479009	Error al guardar datos.
8947900A	Error al leer datos.
8947900B	Error de E/S.
8947900C	No se encuentran las bases de datos.
8947900E	No se ha cargado la biblioteca de licencias.
8947900F	Bases de datos dañadas o actualizadas manualmente.
89479010	Las bases de datos están dañadas.

89479011	No se puede usar un archivo clave no válido para añadir una clave de reserva.
89479012	Error del sistema.
89479013	Lista de claves rechazadas dañada.
89479014	La firma digital del archivo no coincide con la firma digital de Kaspersky.
89479015	No se puede utilizar una clave para una licencia no comercial como clave para una licencia comercial.
89479016	Se necesita la licencia beta para utilizar la versión beta de la aplicación.
89479017	El archivo clave no es compatible con esta aplicación.
89479018	Clave bloqueada por Kaspersky.
89479019	La aplicación ya se ha usado con una licencia de prueba. No se puede añadir una clave de prueba nuevamente.
8947901A	Archivo clave dañado.
8947901B	La firma digital no existe, está dañada o no coincide con la firma digital de Kaspersky.
8947901C	No se puede añadir una clave si la licencia no comercial correspondiente ha caducado.
8947901E	La fecha de creación o uso del archivo clave no es válida. Compruebe que la fecha del sistema sea correcta.
8947901F	No se puede añadir una clave para la licencia de prueba: ya hay otra clave que está activa para la licencia de prueba.
89479020	Falta la lista de claves rechazadas o está dañada.
89479021	Falta la descripción de la actualización o está dañada.
89479022	Error en los datos de servicio de la clave de licencia.
89479023	No se puede usar un archivo clave no válido para añadir una clave de reserva.
89479025	Error al enviar la solicitud al servidor de activación. Posibles motivos: error de conexión a Internet o problemas temporales en el servidor de activación. Intente activar la aplicación más tarde con el código de activación. Si vuelve a encontrar este error, póngase en contacto con su proveedor de Internet.
89479026	Error en la respuesta del servidor de activación.
89479027	No se pudo obtener el estado de la respuesta.
89479028	Error al guardar el archivo temporal.
89479029	El código de activación se escribió con errores o la fecha del sistema no es correcta. Compruebe que la fecha del sistema en el equipo sea correcta.
8947902A	El archivo clave no es compatible con esta aplicación o la licencia ha caducado. No se puede activar Kaspersky Endpoint Security usando el archivo clave de otra aplicación.
8947902B	Error al recibir el archivo clave. Se escribió un código de activación incorrecto.
8947902C	El servidor de activación ha devuelto el error 400.
8947902D	El servidor de activación ha devuelto el error 401.
8947902E	El servidor de activación ha devuelto el error 403.
8947902F	El servidor de activación ha devuelto el error 404.
89479030	El servidor de activación ha devuelto el error 405.

89479031	El servidor de activación ha devuelto el error 406.
89479032	Se requiere autenticación para usar el servidor proxy. Compruebe las opciones de red.
89479033	Se ha agotado el tiempo de espera para la solicitud.
89479034	El servidor de activación ha devuelto el error 409.
89479035	El servidor de activación ha devuelto el error 410.
89479036	El servidor de activación ha devuelto el error 411.
89479037	El servidor de activación ha devuelto el error 412.
89479038	El servidor de activación ha devuelto el error 413.
89479039	El servidor de activación ha devuelto el error 414.
8947903A	El servidor de activación ha devuelto el error 415.
8947903C	Error interno del servidor.
8947903D	Funcionalidad no compatible.
8947903E	La respuesta de la puerta de enlace no es válida. Compruebe las opciones de red.
8947903F	Servicio no disponible (error HTTP 503).
89479040	Se ha agotado el tiempo de espera para la respuesta de la puerta de enlace. Compruebe las opciones de red.
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 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	Clave de licencia caducada.
89479054	La fecha del sistema configurada en el equipo no es correcta.
89479055	La licencia de prueba ha caducado.
89479056	La licencia ha caducado.
89479057	Se ha superado el límite de activaciones para el código especificado.
89479058	El procedimiento de activación terminó debido a un error del sistema.

89479059	No se puede utilizar una clave para una licencia no comercial 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 fecha de publicación de las bases de datos es posterior a la fecha de caducidad de la licencia.
89479066	No se puede reemplazar la clave de licencia activa por una clave caducada.
89479067	No se puede añadir una clave de licencia de reserva si caduca antes que la licencia actual.
89479068	Falta la clave de suscripción actualizada.
8947906A	Código de activación incorrecto (la suma de comprobación no coincide).
8947906B	La clave ya está activa.
8947906C	Los tipos de licencia que corresponden a las claves activa y la de reserva no coinciden.
8947906D	Componente no compatible con la licencia.
8947906E	No es posible añadir la clave de suscripción como clave de licencia de reserva.
89479213	Error general de capa de transporte.
89479214	No se ha podido establecer conexión con el servidor de activación.
89479215	Formato de URL no válido.
89479216	No se ha podido convertir la dirección del servidor proxy.
89479217	No se ha podido convertir la dirección del servidor. Verifique la configuración de su conexión a Internet.
89479218	No se ha podido establecer conexión con el servidor de activación o el servidor proxy.
89479219	Acceso remoto denegado.
8947921A	Se ha agotado el tiempo de espera para la respuesta.
8947921B	Error al enviar la solicitud HTTP.
8947921C	Error de conexión SSL.
8947921D	Operación interrumpida por devolución de llamada.
8947921E	Demasiados intentos de reenvío.
8947921F	Error de comprobación de destinatario.
89479220	Respuesta vacía del servidor de activación.
89479221	Error al enviar datos.
89479222	Error al recibir datos.
89479223	Error del certificado SSL local.
89479224	Error de cifrado SSL.
89479225	Error del certificado SSL del servidor.
89479226	El contenido del paquete de red no es válido.

89479227	Acceso denegado para el usuario.
89479228	Archivo de certificado SSL no válido.
89479229	Error al establecer la conexión SSL.
8947922A	Error al enviar o recibir un paquete de red. Inténtelo de nuevo más tarde.
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 de licencia disponible para el código de activación escrito.
89479404	Clave activa bloqueada.
89479405	No se encuentran los parámetros obligatorios de la solicitud de activación.
89479406	Nombre de usuario o contraseña incorrectos.
89479407	Se ha enviado un código de activación incorrecto al servidor.
89479408	El código de activación no es válido para Kaspersky Endpoint Security. No puede activar Kaspersky Endpoint Security con un archivo clave de una aplicación desconocida.
89479409	A la solicitud le falta un código de activación.
8947940B	La licencia ha caducado (según los datos del servidor de activación).
8947940C	Se ha superado el número de activaciones para este código.
8947940D	Formato de ID de solicitud no válido.
8947940E	El código de activación no es válido para Kaspersky Endpoint Security. El código de activación está destinado a otra aplicación de Kaspersky.
8947940F	No se puede actualizar la clave de licencia.
89479410	El código de activación no es válido para esta región.
89479411	El código de activación no es válido para la versión de Kaspersky Endpoint Security localizada a este idioma.
89479412	Se requiere acceso adicional al servidor de activación.
89479413	El servidor de activación ha devuelto el error 643.
89479414	El servidor de activación ha devuelto el error 644.
89479415	El servidor de activación ha devuelto el error 645.
89479416	El servidor de activación ha devuelto el error 646.
89479417	El servidor de activación no admite el formato del código de activación.
89479418	Formato del código de activación no válido.
89479419	La hora del sistema configurada en el equipo no es correcta.
8947941A	El código de activación no es válido para esta versión de Kaspersky Endpoint Security.
8947941B	La suscripción ha caducado.
8947941C	Cantidad de activaciones superada para esta clave de licencia.
8947941D	La firma digital de la clave de licencia no es válida.

8947941E	Se requieren datos adicionales.
8947941F	Error al verificar los datos del usuario.
89479420	Suscripción inactiva.
89479421	Se están realizando tareas de mantenimiento en el servidor de activación.
89479501	Error de Kaspersky Endpoint Security desconocido.
89479502	Parámetro transferido no válido (por ejemplo, una lista vacía de direcciones de servidores de activación).
89479503	Código de activación incorrecto.
89479504	Nombre de usuario no válido.
89479505	Contraseña de usuario no válida.
89479506	Respuesta no válida del servidor de activación.
89479507	Solicitud de activación interrumpida.
89479509	El servidor de activación ha devuelto 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`, `EXPORT` e `IMPORT`. Con los perfiles, puede configurar parámetros de la aplicación (por ejemplo, `STOP DeviceControl`) o ejecutar tareas (por ejemplo, `START Scan_My_Computer`).

Estos son los perfiles disponibles:

- `AdaptiveAnomaliesControl` – Control de anomalías adaptativo.
- `AMSI` – Protección AMSI.
- `BehaviorDetection` – Detección de comportamientos.
- `DeviceControl` – Control de dispositivos.
- `EntAppControl` – Control de aplicaciones.
- `File_Monitoring` o `FM` – Protección contra archivos peligrosos.
- `Firewall` o `FW` – Firewall.
- `HIPS` – Prevención de intrusiones en el host.
- `IDS` – Protección frente a amenazas en la red.
- `IntegrityCheck` – Comprobación de integridad.
- `Mail_Monitoring` o `EM` – Protección frente a amenazas en el correo.
- `Rollback` – reversión de la actualización.

- Scan\_ContextScan – Análisis desde el menú contextual.
- Scan\_IdleScan – Análisis en segundo plano.
- Scan\_Memory – Memoria del kernel.
- Scan\_My\_Computer – Análisis completo.
- Scan\_Objects – Análisis personalizado.
- Scan\_Qscan – Análisis de los objetos que se cargan durante el inicio del sistema operativo.
- Scan\_Removable\_Drive – Análisis de unidades extraíbles.
- Scan\_Startup o STARTUP – Análisis de áreas críticas.
- Updater – Actualización.
- Web\_Monitoring o WM – Protección frente a amenazas web.
- WebControl – Control web.

Kaspersky Endpoint Security también es compatible con los perfiles de servicio. Puede necesitar este tipo de perfil si en alguna oportunidad se comunica con el Soporte técnico de Kaspersky.



# Administrar la aplicación a través de la API REST

Kaspersky Endpoint Security le permite configurar la aplicación, ejecutar un análisis, actualizar las bases de datos antivirus y realizar otras tareas utilizando soluciones de terceros. Kaspersky Endpoint Security proporciona una API para este fin. La API REST de Kaspersky Endpoint Security funciona a través de HTTP y consta de un conjunto de métodos de solicitud y respuesta. En otras palabras, puede administrar Kaspersky Endpoint Security a través de una solución de terceros, en lugar de mediante la interfaz de la aplicación local o la Consola de administración de Kaspersky Security Center.

Para comenzar a usar la API REST, debe [instalar Kaspersky Endpoint Security con compatibilidad con la API REST](#). El cliente REST y Kaspersky Endpoint Security tienen que estar instalados en el mismo equipo.

Para garantizar una interacción segura entre Kaspersky Endpoint Security y el cliente REST:

- Configure la protección del cliente de REST contra el acceso no autorizado según las recomendaciones del desarrollador del cliente de REST. Configure la protección de la carpeta del cliente de REST contra la escritura con la ayuda de la Lista de Control de Acceso Discrecional - DACL.
- Para ejecutar el cliente de REST, utilice una cuenta aparte con derechos de administrador. Deniegue el acceso interactivo al sistema para esta cuenta.

La aplicación se administra a través de la API REST en `http://127.0.0.1` o `http://localhost`. No se puede administrar Kaspersky Endpoint Security de forma remota a través de la API REST.



[ABRIR LA DOCUMENTACIÓN DE LA API REST](#)

## Instalar la aplicación con la API REST

Para administrar la aplicación a través de la API REST, debe instalar Kaspersky Endpoint Security con compatibilidad con la API REST. Si administra Kaspersky Endpoint Security a través de la API REST, no puede administrar la aplicación utilizando Kaspersky Security Center.

### Preparativos para la instalación de la aplicación con soporte de API REST

La interacción segura de Kaspersky Endpoint Security con el cliente REST requiere configurar la identificación de la solicitud. Para ello, debe instalar un certificado y posteriormente firmar la carga útil de cada solicitud.

Para crear un certificado, puede utilizar, por ejemplo, OpenSSL.

Ejemplo:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Utilice el algoritmo de cifrado RSA con una longitud de clave de 2048 bits o más.

Como resultado, obtendrá un certificado `cert.pem` y una clave privada `key.pem`.

### Instalar la aplicación con soporte de API REST

*Para instalar Kaspersky Endpoint Security con compatibilidad con la API REST:*

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta que contiene el paquete de distribución para Kaspersky Endpoint Security versión 11.2.0 o posterior.
3. Instale Kaspersky Endpoint Security con la siguiente configuración:

- RESTAPI=1

- RESTAPI\_User=<Nombre de usuario>

Nombre de usuario que se utilizará para administrar la aplicación a través de la API REST. Introduzca el nombre de usuario con el formato <DOMINIO>\<NombreUsuario> (por ejemplo, RESTAPI\_User=EMPRESA\Administrador). Puede administrar la aplicación a través de la API REST solo desde esta cuenta. Solo puede seleccionar un usuario para que funcione con la API REST.

- RESTAPI\_Port=<Puerto>

Puerto utilizado para el intercambio de datos. Parámetro opcional. El puerto predeterminado es el 6782.

- RESTAPI\_Certificate=<Ruta al certificado>

Certificado para identificar solicitudes (por ejemplo, RESTAPI\_Certificate=C:\cert.pem).

Puede instalar el certificado después de instalar la aplicación o actualizar el certificado después de que caduque.

#### [Cómo instalar un certificado para la identificación de solicitudes de API REST](#)

1. Desactivar [Autoprotección de Kaspersky Endpoint Security](#).

El mecanismo de Autoprotección impide la modificación o eliminación de los archivos de aplicaciones que se encuentran en el disco duro, de los procesos en la memoria y de las entradas en el registro del sistema.

2. Vaya a la clave de registro que contiene la configuración de la API REST:

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\Rest

3. Introduzca la ruta al certificado, por ejemplo, Certificado = C:\Folder\cert.pem.

4. Activar [Autoprotección de Kaspersky Endpoint Security](#).

5. [Reiniciar la aplicación](#).

- AdminKitConnector=1

Administración de aplicaciones mediante sistemas de administración. La administración está permitida de forma predeterminada.

También puede usar el [archivo setup.ini](#) para definir la configuración para que funcione con la API REST.

Ejemplo:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator  
/pRESTAPI_Certificate=C:\cert.pem /s
```

Como resultado, podrá administrar la aplicación a través de la API REST. Para verificar su funcionamiento, abra la documentación de la API REST utilizando una solicitud GET.

Ejemplo:  
GET <http://localhost:6782/kes/v1/api-docs>

Si ha instalado la aplicación con soporte para la API REST, Kaspersky Endpoint Security crea automáticamente una regla de permiso en la configuración de Control web para acceder a los recursos web (*Regla de servicio para la API REST*). Esta regla es necesaria para permitir que el cliente REST acceda a Kaspersky Endpoint Security en todo momento. Por ejemplo, si ha restringido el acceso de los usuarios a los recursos web, esto no afectará a la administración de la aplicación a través de la API REST. Recomendamos que no se elimine la regla ni se cambie la configuración de *Regla de servicio para la API REST*. Si eliminó la regla, Kaspersky Endpoint Security la restaurará después de que reinicie la aplicación.

## Funcionamiento con la API

No se puede restringir el acceso a la aplicación a través de la API REST utilizando la [protección con contraseña](#). Por ejemplo, no se puede impedir que un usuario desactive la protección a través de la API REST. Puede configurar la protección con contraseña a través de la API REST y restringir el acceso de los usuarios a la aplicación a través de la interfaz local.

Para administrar la aplicación a través de la API REST, debe ejecutar el cliente REST con la cuenta que especificó al [instalar la aplicación con compatibilidad con la API REST](#). Solo puede seleccionar un usuario para que funcione con la API REST.



### [ABRIR LA DOCUMENTACIÓN DE LA API REST](#)

Para administrar la aplicación a través de la API REST se tienen que realizar los pasos siguientes:

1. Obtenga los valores actuales de la configuración de la aplicación. Para hacerlo, envíe una solicitud GET.

Ejemplo:  
GET <http://localhost:6782/kes/v1/settings/ExploitPrevention>

2. La aplicación enviará una respuesta con la estructura y los valores de la configuración. Kaspersky Endpoint Security admite los formatos XML y JSON.

```
Ejemplo:  
{  
  "action": 0,  
  "enableSystemProcessesMemoryProtection": true,  
  "enabled": true  
}
```

3. Edite la configuración de la aplicación. Utilice la estructura de configuración recibida en respuesta a la solicitud GET.

```
Ejemplo:  
{  
  "action": 0,  
  "enableSystemProcessesMemoryProtection": false,  
  "enabled": true  
}
```

4. Guarde la configuración de la aplicación (la carga útil) en un JSON (payload.json).

5. Firme el JSON en formato PKCS7.

Ejemplo:

```
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -  
binary -outform pem -out signed_payload.pem
```

Como resultado, obtiene un archivo firmado con la carga útil de la solicitud (`signed_payload.pem`).

6. Edite la configuración de la aplicación. Para hacerlo, envíe una solicitud POST y adjunte el archivo firmado con la carga útil de la solicitud (`signed_payload.pem`).

La aplicación implementa la configuración nueva y envía una respuesta que contiene los resultados de la configuración de la aplicación (la respuesta puede estar vacía). Puede verificar que la configuración se actualice mediante una solicitud GET.

## Fuentes de información de la aplicación

La página de Kaspersky Endpoint Security del sitio web de Kaspersky

En [la página de Kaspersky Endpoint Security](#), encontrará información general sobre la aplicación, sus características y sus funciones.

La página de Kaspersky Endpoint Security contiene un enlace a la tienda en línea. Allí podrá comprar o renovar la aplicación.

La página de Kaspersky Endpoint Security de la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico.

En [la página de Kaspersky Endpoint Security de la Base de conocimientos](#), encontrará artículos con información útil, recomendaciones y respuestas a las dudas más frecuentes sobre la compra, la instalación y el uso de la aplicación.

Los artículos de la Base de conocimientos pueden contestar preguntas que se relacionan no solo con Kaspersky Endpoint Security, sino también con otras aplicaciones de Kaspersky. Los artículos también pueden contener novedades del Soporte técnico.

Debate sobre las aplicaciones de Kaspersky en la comunidad de usuarios

Si su pregunta no requiere una respuesta urgente, puede analizarla con los expertos de Kaspersky y con otros usuarios en nuestra [Comunidad](#).

En la Comunidad, puede ver los temas existentes, publicar sus comentarios y crear nuevos temas de discusión.

## Cómo ponerse en contacto con el Soporte técnico

Si no es posible encontrar una solución al problema en la documentación o en otras [fuentes de información acerca de Kaspersky Endpoint Security](#), le recomendamos que se ponga en contacto con el Soporte técnico. El Soporte técnico responderá a sus preguntas sobre la instalación y uso de Kaspersky Endpoint Security.

Kaspersky ofrece soporte para Kaspersky Endpoint Security durante su ciclo de vida (consulte la [página del ciclo de vida de la aplicación](#)). Antes de ponerse en contacto con el Soporte técnico, lea las [reglas de soporte](#).

Puede ponerse en contacto con Soporte técnico de una de las siguientes formas:

- [Visitando el sitio web de soporte técnico](#)
- Enviando una solicitud al Soporte técnico de Kaspersky a través del [portal CompanyAccount de Kaspersky](#)

Después de informar a los especialistas de Soporte técnico de Kaspersky acerca del problema, puede que le pidan que cree un *archivo de seguimiento*. El archivo de seguimiento permite supervisar poco a poco el proceso de ejecución de comandos de aplicación y determinar la etapa de funcionamiento de la aplicación en la que se produce el error.

Los especialistas de Soporte técnico pueden solicitar también información adicional sobre el sistema operativo, los procesos en ejecución del equipo e informes detallados sobre el funcionamiento de los componentes de aplicación.

Mientras el diagnóstico está en ejecución, los expertos del Soporte técnico pueden pedir que cambie la configuración de la aplicación por:

- Activar una función que permitirá recibir información de diagnóstico extendida.
- Ajustar la configuración de los componentes individuales de la aplicación, que no están disponibles a través de los elementos estándar de la interfaz de usuario.
- Cambiar opciones relativas al almacenamiento de la información de diagnóstico.
- Configurar la interceptación y el registro del tráfico de red.

Los expertos del Soporte técnico le darán toda la información que necesitará para realizar estas operaciones (descripción de la secuencia de pasos, parámetros que se deben modificar, archivos de configuración, secuencias de comandos, funcionalidad adicional de la línea de comandos, módulos de depuración, utilidades con fines especiales, etc.). También le informarán del alcance de los datos utilizados con fines de depuración. La información de diagnóstico extendida se guarda en el equipo del usuario. Los datos no se transmiten automáticamente a Kaspersky.

Las operaciones que se describen anteriormente solo se deben realizar bajo la supervisión de los especialistas de Soporte técnico siguiendo sus instrucciones. Cambiar la configuración de la aplicación por su cuenta de forma no descrita en la Ayuda en línea o en las recomendaciones del Servicio técnico puede provocar ralentizaciones y caídas del sistema operativo, reducir el nivel de protección de su equipo y dañar la disponibilidad e integridad de la información que se procesa.

## Contenido y almacenamiento de archivos de seguimiento

Usted es personalmente responsable de la seguridad de los datos que se almacenan en su equipo y, especialmente, de supervisar y restringir el acceso a los datos hasta que se envíen a Kaspersky.

Los archivos de seguimiento se almacenan en el equipo siempre que la aplicación esté en uso y se eliminan permanentemente cuando se quita la aplicación.

Los archivos de seguimiento —exceptuados los del Agente de autenticación— se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces.

El nombre de los archivos de rastreo tiene el siguiente formato: KES<número de versión del servicio\_fechaXX.XX\_horaXX.XX\_pidXXX.><tipo de archivo de rastreo>.log.

Puede ver los datos almacenados en los archivos de seguimiento.

Todos los archivos de seguimiento contienen los datos comunes siguientes:

- Hora del evento.
- Número del subprocesso de ejecución.

El archivo de seguimiento del Agente de autenticación no contiene esta información.

- Componente de la aplicación que causó el evento.
- Nivel de gravedad de eventos (evento informativo, advertencia, evento crítico, error).
- Una descripción del evento que implica la ejecución del comando por un componente de la aplicación y el resultado de la ejecución de este comando.

Kaspersky Endpoint Security guarda contraseñas de usuario en un archivo de seguimiento solo en forma cifrada.

## Contenidos de los archivos de seguimiento SRV.log, GUI.log y ALL.log

Los archivos de seguimiento SRV.log, GUI.log y ALL.log pueden almacenar la siguiente información además de los datos generales:

- Datos personales, incluido el apellido, el nombre y el segundo nombre, si se incluyen estos datos en la ruta a los archivos en un equipo local.
- Datos sobre el hardware instalado en el equipo (como datos de firmware de BIOS/UEFI). Estos datos se escriben en archivos de seguimiento cuando se realiza el Cifrado de disco de Kaspersky.
- El nombre de usuario y la contraseña si se transmitieron abiertamente. Estos datos se pueden registrar en archivos de seguimiento durante el análisis del tráfico de Internet.
- El nombre de usuario y la contraseña si se incluyen en encabezados HTTP.
- El nombre de la cuenta de Microsoft Windows si se incluye el nombre de la cuenta en un nombre de archivo.

- Su dirección de correo electrónico o una dirección web que contenga el nombre y la contraseña de su cuenta si se incluyen en el nombre del objeto detectado.
- Los sitios web que visita y a los que se le redirige desde estos. Estos datos se escriben en archivos de seguimiento cuando la aplicación analiza sitios web.
- Dirección del servidor proxy, nombre del equipo, puerto, dirección IP y nombre de usuario usado para iniciar sesión en el servidor proxy. Estos datos se escriben en los archivos de seguimiento si la aplicación utiliza a un servidor proxy.
- Direcciones IP remotas con las que el equipo establece conexiones.
- Asunto del mensaje, ID, nombre y dirección del remitente de la página web del remitente del mensaje en una red social. Estos datos se escriben en archivos de seguimiento si el componente Control web está activado.
- Datos de tráfico de red. Estos datos se escriben en archivos de seguimiento si los componentes de supervisión están activados (como Control web).
- Datos recibidos de los servidores de Kaspersky (como la versión de las bases de datos antivirus).
- Estados de los componentes de Kaspersky Endpoint Security y sus datos de funcionamiento.
- Datos sobre la actividad del usuario en la aplicación.
- Eventos del sistema operativo.

## Contenido de los archivos de seguimiento HST.log, BL.log, Dumpwriter.log, WD.log y AVPCon.dll.log

Además de datos generales, el archivo de seguimiento HST.log contiene información sobre la ejecución de una tarea de la actualización de la base de datos y del módulo de aplicación.

Además de datos generales, el archivo de seguimiento BL.log contiene información sobre los eventos que ocurren durante el funcionamiento de la aplicación, así como los datos requeridos para solucionar problemas de errores de aplicación. Este archivo se crea si se inicia la aplicación con el parámetro -bl de avp.exe.

Además de datos generales, el archivo de seguimiento Dumpwriter.log contiene información de servicio requerida para solucionar errores que se producen cuando se escribe el archivo de volcado de la aplicación.

Además de datos generales, el archivo de seguimiento WD.log contiene información sobre los eventos que se producen durante el funcionamiento del servicio avpsus, incluidos eventos de actualización del módulo de aplicación.

Además de datos generales, el archivo de seguimiento AVPCon.dll.log contiene información sobre los eventos que se producen durante el funcionamiento del módulo de conectividad de Kaspersky Security Center.

## Contenido de los archivos de seguimiento del rendimiento

El nombre de los archivos de seguimiento del rendimiento sigue este formato: KES<número de versión\_fechaXX.XX\_horaXX.XX\_pidXXX.>PERF.HAND.etl.

Además de los datos generales, los archivos de seguimiento del rendimiento contienen información sobre la carga del procesador, sobre los procesos en ejecución y sobre el tiempo de carga del sistema operativo y las aplicaciones.



## Contenido de los archivos de seguimiento del componente de protección AMSI

Además de datos generales, el archivo de seguimiento AMSI.log contiene información sobre los resultados de los análisis realizados por solicitud de aplicaciones de terceros.

## Contenido de archivos de seguimiento del componente Protección frente a amenazas en el correo

Además de datos generales, el archivo de seguimiento mcou. OUTLOOK. EXE. log puede contener partes de mensajes de correo electrónico, entre ellas direcciones de correo electrónico.

## Contenido de archivos de seguimiento del componente Analizar desde el menú contextual

Además de datos generales, el archivo de seguimiento shellx.dll.log contiene información sobre la ejecución de la tarea de análisis y los datos requeridos para depurar la aplicación.

## Contenido de los archivos de seguimiento del complemento web de la aplicación

Los archivos de seguimiento del complemento web de la aplicación se almacenan en el equipo en el que se ha instalado Kaspersky Security Center Web Console, dentro de la carpeta Archivos de programa\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-<tipo de archivo de seguimiento>.DESKTOP-<fecha de actualización del archivo>.log. Web Console comienza a guardar información en cuanto concluye su instalación. Los archivos de seguimiento se eliminan cuando Web Console se desinstala.

Además de los datos generales, los archivos de seguimiento del complemento web contienen la siguiente información:

- Contraseña del usuario KLAdmin para desbloquear la interfaz de Kaspersky Endpoint Security ([Protección con contraseña](#)).
- Contraseña temporal para desbloquear la interfaz de Kaspersky Endpoint Security ([Protección con contraseña](#)).
- Nombre de usuario y contraseña para el servidor de correo SMTP ([Notificaciones por correo electrónico](#)).
- Nombre de usuario y contraseña para el servidor proxy ([Servidor proxy](#)).
- Nombre de usuario y contraseña para la [tarea Cambiar componentes de la aplicación](#).
- Credenciales de cuentas y rutas especificadas en las propiedades de las directivas y de las tareas de Kaspersky Endpoint Security.

## Contenidos del archivo de seguimiento del Agente de autenticación

El archivo de seguimiento del Agente de autenticación se almacena en la carpeta System Volume Information y tiene el siguiente nombre: KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin.


Además de datos generales, el archivo de seguimiento del Agente de autenticación contiene información sobre el funcionamiento del Agente de autenticación y las acciones que el usuario lleva a cabo con el Agente de autenticación.

## Rastreo del funcionamiento de aplicaciones

El *rastreo de la aplicación* es un registro detallado de las acciones que realiza la aplicación y de los mensajes acerca de los eventos que se produjeron durante el funcionamiento de la aplicación.

La función de rastreo de la aplicación solo debe utilizarse bajo la supervisión del Soporte técnico de Kaspersky.

*Para crear un archivo de seguimiento de la aplicación:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Herramientas de soporte**.
3. Utilice el interruptor **Activar los rastros de la aplicación** para activar o desactivar el rastreo del funcionamiento de la aplicación.
4. En la lista desplegable **Rastreo**, seleccione un modo de seguimiento de la aplicación:
  - **Con rotación**. 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 número máximo de archivos por rotación y el tamaño máximo para cada archivo.
  - **Escribir a un solo archivo**. Guardar un archivo de seguimiento (sin límite de tamaño).
5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento:

Se le aconseja que aclare el nivel de seguimiento necesario con un especialista del Servicio de soporte técnico. Si no dispone de asistencia por parte del Soporte técnico, establezca el nivel de seguimiento en **Normal (500)**.

6. Reinicie Kaspersky Endpoint Security.
7. Para detener el proceso de seguimiento, regrese a la ventana **Herramientas de soporte** y desactive el seguimiento.

También puede crear archivos de seguimiento al instalar la aplicación desde la [línea de comandos](#), incluso al utilizar [el archivo setup.ini](#).

Como resultado, se crea un archivo de seguimiento del rendimiento en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Envíe ese archivo al Soporte técnico de Kaspersky.


Kaspersky Endpoint Security elimina los archivos de seguimiento de manera automática cuando se elimina la aplicación. También puede eliminar los archivos de forma manual. Para hacerlo, debe desactivar el rastreo y [detener la aplicación](#).

## Rastreo del rendimiento de aplicaciones

Kaspersky Endpoint Security le permite obtener información sobre los problemas que puedan ocurrir en el funcionamiento del equipo al utilizar la aplicación. Por ejemplo, si observa demoras al cargar el sistema operativo tras instalar la aplicación, puede recibir información al respecto. Para brindar esta información, Kaspersky Endpoint Security crea [archivos de seguimiento del rendimiento](#). Realizar un *rastreo del rendimiento* se refiere a registrar las acciones que la aplicación realiza con el fin de diagnosticar los problemas de rendimiento de Kaspersky Endpoint Security. Para obtener la información, Kaspersky Endpoint Security utiliza el servicio de Seguimiento de eventos para Windows (ETW). Diagnosticar los problemas de Kaspersky Endpoint Security y determinar sus causas es tarea del Soporte técnico de Kaspersky.

La función de rastreo de la aplicación solo debe utilizarse bajo la supervisión del Soporte técnico de Kaspersky.

*Para crear un archivo de seguimiento del rendimiento:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana que se abre, haga clic en el botón **Herramientas de soporte**.
3. Utilice el interruptor **Activar los rastreos de rendimiento** para activar o desactivar el seguimiento del rendimiento de las aplicaciones.
4. En la lista desplegable **Rastreo**, seleccione un modo de seguimiento de la aplicación:
  - **Con rotación**. 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.
  - **Escribir a un solo archivo**. Guardar un archivo de seguimiento (sin límite de tamaño).
5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento:
  - **Superficial**. Kaspersky Endpoint Security analizará los procesos más importantes del sistema operativo relacionados con el rendimiento.
  - **Detallado**. Kaspersky Endpoint Security analizará todos los procesos del sistema operativo relacionados con el rendimiento.
6. En la lista desplegable **Tipo de rastreo**, seleccione el tipo de rastreo:
  - **Información básica**. Kaspersky Endpoint Security analizará los procesos mientras el sistema operativo esté en funcionamiento. Utilice este tipo de seguimiento para problemas que continúen después de que el sistema operativo se haya cargado (por ejemplo, si tiene problemas para acceder a Internet a través del navegador).
  - **Al reiniciar**. Kaspersky Endpoint Security analizará los procesos únicamente mientras el sistema operativo se esté cargando. Una vez que el sistema operativo se haya cargado, Kaspersky Endpoint Security detendrá el proceso de seguimiento. Utilice este tipo de seguimiento si su problema está vinculado a alguna demora durante la carga del sistema operativo.
7. Reinicie el equipo e intente reproducir el problema.
8. Para detener el proceso de seguimiento, regrese a la ventana **Herramientas de soporte** y desactive el seguimiento.

Como resultado, se crea un archivo de seguimiento del rendimiento en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Envíe ese archivo al Soporte técnico de Kaspersky.


## Escritura de volcado

Un archivo de volcado contiene toda información sobre la memoria de trabajo de los procesos de la Kaspersky Endpoint Security en el momento en que se crea el archivo de volcado.

Los archivos de volcado guardados pueden contener datos confidenciales. Para controlar el acceso a los datos, debe garantizar de forma independiente la seguridad de los archivos de volcado.

Los archivos de volcado se almacenan en el equipo siempre que la aplicación esté en uso y se eliminan permanentemente cuando se elimina la aplicación. Los archivos de volcado se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces.

*Para activar y desactivar la escritura de volcado, haga lo siguiente:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. En el bloque **Información de depuración**, use la casilla de verificación **Activar escritura de volcado** para activar o desactivar la escritura de volcado de la aplicación.
4. Guarde los cambios.


## Protección de archivos de volcado y archivos de seguimiento

Los archivos de volcado y los archivos de rastreo contienen información sobre el sistema operativo y también pueden contener [datos de usuario](#). Para evitar el acceso no autorizado a dichos datos, puede activar la protección de los archivos de volcado y rastreo.

Si se activa la protección de los archivos de volcado y rastreo, los usuarios siguientes pueden acceder a dichos archivos:

- El administrador del sistema y el administrador local pueden acceder a los archivos de volcado, así como el usuario que activó la escritura de los archivos de volcado y rastreo.
- Únicamente el administrador del sistema y el administrador del equipo local pueden acceder a los archivos de rastreo.

*Para activar o desactivar la protección de los archivos de volcado y rastreo:*

1. En la ventana de la aplicación principal, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración general** → **Configuración de la aplicación**.
3. En el bloque de **información de depuración**, utilice la casilla de verificación **Activar la protección de los archivos de volcado y de rastreo** para activar o desactivar la protección de archivos.
4. Guarde los cambios.

Los archivos de volcado y rastreo que se escribieron mientras la protección estaba activa permanecen protegidos incluso después de que esta función se desactive.

## Limitaciones y advertencias

Kaspersky Endpoint Security presenta ciertas limitaciones que no suponen ningún impedimento para el funcionamiento de la aplicación.

[Instalación de la aplicación](#) 

- Para más información sobre la compatibilidad con los sistemas operativos Microsoft Windows 10, Microsoft Windows Server 2016 y Microsoft Windows Server 2019, visite la [Base de conocimientos del Soporte técnico](#).
- Para más información sobre la compatibilidad con Microsoft Windows 11 y Microsoft Windows Server 2022, visite la [Base de conocimientos del Soporte técnico](#).
- Después de instalarse en un equipo infectado, la aplicación no informa al usuario sobre la necesidad de ejecutar un análisis del equipo. Puede experimentar problemas para [activar la aplicación](#). Para resolver estos problemas, [inicie un Análisis de áreas críticas](#).
- Si se utilizan caracteres que no son ASCII (por ejemplo, letras rusas) en los archivos setup.ini y setup.reg, se recomienda editar el archivo con notepad.exe y guardar el archivo en codificación UTF-16LE. No se admiten otras codificaciones.
- La aplicación no admite el uso de caracteres que no sean ASCII al especificar la ruta de instalación de la aplicación en la [configuración del paquete de instalación](#).
- Cuando la [configuración de la aplicación se importa desde un archivo CFG](#), no se aplica el valor de la configuración que define la participación en Kaspersky Security Network. Después de importar la configuración, lea el texto de la Declaración de Kaspersky Security Network y confirme su consentimiento para participar en Kaspersky Security Network. Puede leer el texto de la Declaración en la interfaz de la aplicación o en el archivo ksn\_\*.txt ubicado en la carpeta que contiene el kit de distribución de la aplicación.
- Si desea eliminar y volver a instalar el cifrado (FLE o FDE) o el componente de Control de dispositivos, debe reiniciar el sistema antes de la reinstalación.
- Cuando utilice el sistema operativo Microsoft Windows 10, debe reiniciar el sistema después de eliminar el componente Cifrado de archivos (FLE).
- Al intentar instalar cualquier versión del módulo de cifrado AES en un equipo que tiene Kaspersky Endpoint Security para Windows 11.8.0 pero ningún componente de cifrado instalado, la instalación del módulo de cifrado terminará con un mensaje de error que indica que se ha instalado una versión más reciente de la aplicación. A partir de Kaspersky Endpoint Security 10 para Windows Service Pack 2 (versión 10.3.0.6294), no existe un archivo de instalación independiente para el módulo de cifrado. Las bibliotecas de cifrado se incluyen en el paquete de distribución de la aplicación. Kaspersky Endpoint Security 11.8.0 no es compatible con módulos de cifrado AES. Las bibliotecas necesarias para el cifrado se instalan automáticamente cuando se selecciona el componente Cifrado de disco completo (FDE) o Cifrado de archivos (FLE).
- La instalación de la aplicación puede terminar con un error que indica que *una aplicación sin nombre o que no se puede leer está instalada en el equipo*. Esto significa que las aplicaciones incompatibles o fragmentos de ellas permanecen en su equipo. Para eliminar artefactos de aplicaciones incompatibles, envíe una solicitud con una descripción detallada de la situación al Soporte técnico de Kaspersky a través de [CompanyAccount de Kaspersky](#).
- Si canceló la eliminación de la aplicación, inicie su recuperación después de que se reinicie el equipo.
- En equipos que ejecutan Windows 10 versión 1903 y 1909, las actualizaciones de Kaspersky Endpoint Security 10 para Windows Service Pack 2 Maintenance Release 3 (compilación 10.3.3.275), Service Pack 2 Maintenance Release 4 (compilación 10.3.3.304), 11.0.0 y 11.0.1 con el componente Cifrado de archivos (FLE) instalado pueden terminar con un error. Esto se debe a que el cifrado de archivos no es compatible con estas versiones de Kaspersky Endpoint Security para Windows en Windows 10 versión 1903 y 1909. Antes de instalar esta actualización, se recomienda [eliminar el componente de cifrado de archivos](#).
- La aplicación requiere Microsoft .NET Framework 4.0 o posterior. Microsoft .NET Framework 4.6.1 tiene vulnerabilidades. Si está utilizando Microsoft .NET Framework 4.6.1, debe instalar actualizaciones de

seguridad. Para obtener detalles sobre las actualizaciones de seguridad de Microsoft .NET Framework, consulte el [Sitio web de soporte técnico de Microsoft](#).

- Si está actualizando una versión anterior de la aplicación a la versión 11.8.0, para instalar Kaspersky Endpoint Agent, reinicie el equipo e inicie sesión en el sistema con una cuenta con derechos de administrador local. De lo contrario, Kaspersky Endpoint Agent no se instalará durante el procedimiento de actualización.
- Si la aplicación no se instaló correctamente con el componente Kaspersky Endpoint Agent seleccionado en un sistema operativo de servidor y aparece la ventana *Error del coordinador de Windows Installer*, consulte las instrucciones en el sitio web de soporte de Microsoft.
- Si la aplicación se instaló localmente en modo no interactivo, use el [archivo setup.ini](#) proporcionado para reemplazar los componentes instalados.
- Después de instalar Kaspersky Endpoint Security para Windows en algunas configuraciones de Windows 7, Windows Defender continúa funcionando. Se le recomienda que desactive Windows Defender manualmente para evitar un rendimiento degradado del sistema.

### [Actualización de la aplicación](#)



- Al actualizar desde Kaspersky Endpoint Security 10 para Windows Service Pack 2 (compilación 10.3.0.6294), [se activa el componente Prevención de intrusiones en el host](#).
- Cuando se actualiza Kaspersky Endpoint Security 10 para Windows Service Pack 2 (compilación 10.3.0.6294), los archivos colocados en Copia de seguridad o Cuarentena en la versión anterior se transfieren a Copia de seguridad en la versión nueva. Estos archivos no se transfieren para versiones anteriores a Kaspersky Endpoint Security 10 para Windows Service Pack 2 (compilación 10.3.0.6294). Para guardarlos, debe restaurar los archivos de Cuarentena y Copia de seguridad antes de actualizar la aplicación. Una vez completada la actualización, vuelva a analizar los archivos restaurados.
- A partir de la versión 11.0.0 de la aplicación, puede instalar el complemento MMC de Kaspersky Endpoint Security para Windows sobre la versión anterior del complemento. Para regresar a una versión anterior del complemento, elimine el complemento actual e instale una versión anterior.
- Al actualizar Kaspersky Endpoint Security 11.0.0 o 11.0.1 para Windows, la [configuración del programa de tareas local](#) para las tareas de *Actualización*, *Análisis de áreas críticas*, *Análisis personalizado* y *Comprobación de integridad* no se guardan.
- En equipos que ejecutan Windows 10 versión 1903 y 1909, las actualizaciones de Kaspersky Endpoint Security 10 para Windows Service Pack 2 Maintenance Release 3 (compilación 10.3.3.275), Service Pack 2 Maintenance Release 4 (compilación 10.3.3.304), 11.0.0 y 11.0.1 con el componente Cifrado de archivos (FLE) instalado pueden terminar con un error. Esto se debe a que el cifrado de archivos no es compatible con estas versiones de Kaspersky Endpoint Security para Windows en Windows 10 versión 1903 y 1909. Antes de instalar esta actualización, se recomienda [eliminar el componente de cifrado de archivos](#).
- La aplicación requiere Microsoft .NET Framework 4.0 o posterior. Microsoft .NET Framework 4.6.1 tiene vulnerabilidades. Si está utilizando Microsoft .NET Framework 4.6.1, debe instalar actualizaciones de seguridad. Para obtener detalles sobre las actualizaciones de seguridad de Microsoft .NET Framework, consulte el [Sitio web de soporte técnico de Microsoft](#).
- Si está actualizando una versión anterior de la aplicación a la versión 11.8.0, para instalar Kaspersky Endpoint Agent, reinicie el equipo e inicie sesión en el sistema con una cuenta con derechos de administrador local. De lo contrario, Kaspersky Endpoint Agent no se instalará durante el procedimiento de actualización.
- Si está actualizando Kaspersky Endpoint Security 10 para Windows Service Pack 2 Maintenance Release 4 con el componente Cifrado de archivos (FLE) instalado en equipos con Windows 10 versión 1809, 1903 y 1909, los controladores de FDE no se instalarán en la imagen de WinRE.
- Al actualizar Kaspersky Endpoint Security, la aplicación desactiva el uso de KSN hasta que se acepta la Declaración de Kaspersky Security Network. Además, el estado del equipo se puede cambiar a *Crítico* en Kaspersky Security Center; se recibe el evento *servidores KSN desactivados*. Si utiliza [Kaspersky Managed Detection and Response](#), recibirá eventos sobre violaciones del funcionamiento de la solución. El uso de KSN es necesario para el funcionamiento de Kaspersky Managed Detection and Response. Kaspersky Endpoint Security [activa el uso de KSN](#) tras la aplicación de la directiva mediante la cual el administrador acepta las condiciones de uso de KSN. Una vez que se ha aceptado la Declaración de Kaspersky Security Network, Kaspersky Endpoint Security reanuda su funcionamiento.
- Una vez que la aplicación se actualiza desde versiones anteriores a Kaspersky Endpoint Security 11 para Windows, se debe reiniciar el equipo.

## [Soporte para plataformas de servidores](#)

- El sistema de archivos ReFS es compatible con limitaciones:
  - Kaspersky Endpoint Security puede procesar incorrectamente los eventos de desinfección de amenazas. Por ejemplo, si la aplicación ha eliminado un archivo malicioso, el informe puede tener una entrada de Objeto no procesado. Al mismo tiempo, Kaspersky Endpoint Security desinfecta las amenazas de acuerdo con la configuración de la aplicación. Kaspersky Endpoint Security también puede crear un duplicado del evento *El objeto se desinfectará al reiniciar* para el mismo objeto.
  - Protección frente a amenazas en archivos puede omitir algunas amenazas. Al mismo tiempo, Análisis antivirus funciona correctamente.
  - Después de iniciar la comprobación de Antivirus, las exclusiones del análisis añadidas con iChecker se restablecen al reiniciar el servidor.
  - La tecnología iSwift no es compatible. Kaspersky Endpoint Security no considera las exclusiones de análisis añadidas mediante la tecnología iSwift.
  - Kaspersky Endpoint Security no detecta los archivos eicar.com y susp-eicar.com si el archivo meicar.exe ya existía en el equipo antes de instalar Kaspersky Endpoint Security.
  - Kaspersky Endpoint Security puede mostrar incorrectamente notificaciones de desinfección de amenazas. Por ejemplo, la aplicación puede mostrar una notificación de amenaza para una amenaza previamente desinfectada.
- Las tecnologías Cifrado de archivos (FLE) y Cifrado de disco de Kaspersky (FDE) no son compatibles con las plataformas de servidor. Al mismo tiempo, Kaspersky Endpoint Security puede procesar incorrectamente los eventos de cifrado de datos.
- En los sistemas operativos de servidor, no se muestra ninguna advertencia sobre la necesidad de una desinfección avanzada.
- Se ha excluido la compatibilidad con Microsoft Windows Server 2008. - No se admite la instalación de la aplicación en un equipo que ejecute el sistema operativo Microsoft Windows Server 2008.
- El modo básico se admite con limitaciones:
  - La interfaz gráfica de usuario local no está disponible, incluidas las notificaciones, las notificaciones emergentes y otros controles de la interfaz. La aplicación no puede mostrar ventanas de mensajes, incluidas las siguientes ventanas:
    - Solicitud de confirmación de la versión de la aplicación y la actualización del módulo;
    - Solicitud de reinicio del equipo;
    - Solicitud de credenciales de autenticación del servidor proxy.
    - Preguntar para acceder a un dispositivo (Control de Dispositivos).
  - Los siguientes componentes no están disponibles: Protección frente a amenazas web, Protección frente a amenazas en el correo, Control web, Prevención de ataques de BadUSB y Anti-Bridging.
  - Solo puede aceptar la Declaración de Kaspersky Security Network en la directiva de la aplicación en la consola de Kaspersky Security Center.

- El cifrado de unidad BitLocker solo está disponible con un módulo de plataforma segura (TPM). No se puede usar un PIN/contraseña para el cifrado porque la aplicación no puede mostrar la ventana de solicitud de contraseña para la autenticación previa al inicio. Si el sistema operativo tiene activado el modo de compatibilidad con los Estándares federales de procesamiento de la información (FIPS), instale una unidad extraíble para guardar la clave de cifrado antes de comenzar a cifrar la unidad.

## [Soporte para plataformas virtuales](#)

- No se admite el Cifrado de disco completo (FDE) en máquinas virtuales Hyper-V.
- No se admite el Cifrado de disco completo (FDE) en las plataformas virtuales Citrix.
- Windows 10 Enterprise multisesión es compatible con limitaciones:
  - Kaspersky Endpoint Security desinfecta las amenazas activas sin avisar al usuario, al igual que cuando [se desinfectan las amenazas activas en los servidores](#). Como el sistema operativo sigue funcionando en modo multisesión, otros usuarios activos pueden perder sus datos si la amenaza no se resuelve inmediatamente.
  - Cifrado de disco completo (FDE) no es compatible.
  - Administrar BitLocker no es compatible.
  - Usar Kaspersky Endpoint Security con unidades extraíbles no es compatible. La infraestructura Microsoft Azure define a las unidades extraíbles como unidades de red.
- No se admite la instalación y el uso del Cifrado de archivos (FLE) en plataformas virtuales Citrix.
- Para admitir la compatibilidad de Kaspersky Endpoint Security para Windows con Citrix PVS, realice la instalación con la opción [Garantizar compatibilidad con Citrix PVS activada](#). Esta opción se puede activar en el [Asistente de configuración](#) o mediante el [parámetro de línea de comando](#) /pCITRIXCOMPATIBILITY=1. En caso de instalación remota, el [archivo KUD](#) debe editarse añadiendo el siguiente parámetro: /pCITRIXCOMPATIBILITY=1.
- Citrix XenDesktop. Antes de iniciar la clonación, debe [desactivar la Autoprotección](#) para clonar máquinas virtuales que usan vDisk.
- Al preparar una máquina de plantilla para la imagen maestra de Citrix XenDesktop con Kaspersky Endpoint Security para Windows preinstalado y Agente de Red de Kaspersky Security Center, añada los siguientes tipos de exclusiones al archivo de configuración:
 

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

Para obtener detalles sobre Citrix XenDesktop, visite el [Sitio web de soporte de Citrix](#).
- En algunos casos, es posible que un intento de desconectar de forma segura una unidad extraíble no tenga éxito en una máquina virtual implementada en un hipervisor VMware ESXi. Intente desconectar de forma segura el dispositivo una vez más.

## [Compatibilidad con Kaspersky Security Center](#)

- Puede administrar el componente Control de anomalías adaptativo solo en Kaspersky Security Center 11 o versiones posteriores.
- Es posible que el informe de amenazas de Kaspersky Security Center 11 no muestre información sobre la acción realizada en las amenazas detectadas por Protección vía AMSI.
- El estado operativo de los componentes Protección vía AMSI y Control de anomalías adaptativo está disponible solo en Kaspersky Security Center versión 11 o posteriores. Puede ver el estado operativo en la Consola de Kaspersky Security Center, dentro de las propiedades del equipo en la sección **Tareas**. Los informes para estos componentes también están disponibles solo en Kaspersky Security Center versión 11 o posteriores.

## [Administración de licencias](#)

- Si aparece el mensaje *Error al recibir datos* del sistema, verifique que el equipo en el que está realizando la activación tenga acceso a la red o establezca la configuración de activación a través del servidor proxy de activación de Kaspersky Security Center.
- La aplicación no puede activarse por suscripción a través de Kaspersky Security Center si la licencia ha caducado o si hay una licencia de prueba activa en el equipo. Para reemplazar una licencia de prueba o una licencia que caducará pronto con una licencia de suscripción, [utilice la tarea de distribución de licencias](#).
- En la interfaz de la aplicación, la fecha de caducidad de la licencia se muestra en la hora local del equipo.
- La instalación de la aplicación con un archivo llave incrustado en un equipo que tiene acceso a Internet inestable puede resultar en la visualización temporal de eventos que indiquen que la aplicación no está activada o que la licencia no permite el funcionamiento del componente. Esto se debe a que la aplicación primero se instala e intenta activar la licencia de prueba incorporada, que requiere acceso a Internet para la activación durante el procedimiento de instalación.
- Durante el período de evaluación, la instalación de cualquier actualización o parche de la aplicación en un equipo que tiene un acceso a Internet inestable puede resultar en la visualización temporal de eventos que indiquen que la aplicación no está activada. Esto se debe a que la aplicación vuelve a instalar e intenta activar la licencia de prueba incorporada, que requiere acceso a Internet para la activación al instalar una actualización.
- Si la licencia de prueba se activó automáticamente durante la instalación de la aplicación y luego la aplicación se eliminó sin guardar la información de la licencia, la aplicación no se activará automáticamente con la licencia de prueba cuando se reinstale. En este caso, active manualmente la aplicación.
- Si está usando Kaspersky Security Center versión 11 y Kaspersky Endpoint Security versión 11.8.0, es posible que los informes de rendimiento de componentes no funcionen correctamente. Si instaló componentes de Kaspersky Endpoint Security que no están incluidos en su licencia, el Agente de red puede enviar errores de estado de componentes al registro de eventos de Windows. Para evitar errores, elimine los componentes que no están incluidos en su licencia.

## [Motor de reparación](#)

- La aplicación solo puede restaurar archivos en dispositivos que utilizan los sistemas de archivos NTFS o FAT32.
- La aplicación puede restaurar archivos de las siguientes extensiones: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls,xlsx, xlsx, xlsx, 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.
- La aplicación no controla los cambios que se realizan en los archivos a través de las interfaces de red (esta situación puede ocurrir, por ejemplo, si un archivo está almacenado en una carpeta compartida y un proceso se inicia a distancia desde otro equipo).

## [Firewall](#)

- La filtración de paquetes o conexiones por dirección local, interfaz física y período de vida del paquete (TTL) se admite en los siguientes casos:
  - Por dirección local para paquetes salientes o conexiones en reglas de la aplicación para TCP y UDP y reglas de paquetes.
  - Por dirección local para paquetes o conexiones entrantes (excepto UDP) en reglas de bloques de aplicaciones y reglas de paquetes.
  - Por período de vida del paquete (TTL) en reglas de paquetes en bloque para paquetes entrantes o salientes.
  - Por interfaz de red para paquetes entrantes y salientes o conexiones en reglas de paquetes.
- En las versiones de la aplicación 11.0.0 y 11.0.1, las direcciones MAC definidas se aplican incorrectamente. La configuración de la dirección MAC para las versiones 11.0.0, 11.0.1 y 11.1.0 o posteriores no son compatibles. Después de actualizar la aplicación o el complemento de estas versiones a la versión 11.1.0 o posterior, debe verificar y reconfigurar las direcciones MAC definidas en las reglas del Firewall.
- Al actualizar la aplicación de las versiones 11.1.1 y 11.2.0 a la versión 11.8.0, los estados de los permisos para las siguientes reglas de Firewall no se migran:
  - Solicitudes al servidor DNS sobre TCP.
  - Solicitudes al servidor DNS sobre UDP.
  - Cualquier actividad de la red.
  - Respuestas entrantes inaccesibles del destino de ICMP.
  - Secuencia ICMP entrante.
- Si ha configurado un adaptador de red o un período de vida (TTL) de paquetes en una regla para paquetes permitidos, la prioridad de esta regla es inferior a la de una regla de aplicaciones bloqueadas. En otras palabras, si se ha bloqueado la actividad de red de una aplicación (por ejemplo, si la aplicación está en el grupo de confianza *Restricción máxima*), no puede permitir actividad de red en la aplicación con una regla de paquetes con esta configuración. En el resto de los casos, la prioridad de una regla de paquetes es superior a una regla de red de la aplicación.
- Al [importar reglas de paquetes de Firewall](#), Kaspersky Endpoint Security puede modificar los nombres de las reglas. La aplicación determina reglas con conjuntos idénticos de parámetros generales: protocolo, dirección, puertos remotos y locales, período de vida del paquete (TTL). Si este conjunto de parámetros generales es idéntico para varias reglas, la aplicación asigna el mismo nombre a estas reglas o añade una etiqueta de parámetro al nombre. De esta manera, Kaspersky Endpoint Security importa todas las reglas de paquetes, pero el nombre de las reglas que tienen configuraciones generales idénticas se puede modificar.
- Si ha [activado la notificación de eventos de la aplicación en una reglas de la red](#), al mover la aplicación a un grupo de confianza diferente, no se aplicarán las restricciones de este grupo de confianza. Por lo tanto, si la aplicación está en el grupo de confianza, no tendrá restricciones de red. Luego activó la notificación de eventos para esta aplicación y la movió al grupo de confianza No fiable. El Firewall no aplicará las restricciones de red para esta aplicación. Le recomendamos que primero mueva la aplicación al grupo de confianza apropiado y luego active la notificación de eventos. Si este método no es adecuado, puede configurar manualmente las restricciones para la aplicación en la configuración de las reglas de la red. La restricción se aplica solo a la interfaz local de la aplicación. Mover la aplicación entre grupos de confianza en la directiva funciona correctamente.

- Los componentes de Firewall y Prevención de intrusiones tienen configuración común: derechos de la aplicación y recursos protegidos. Si cambia esta configuración para el Firewall, Kaspersky Endpoint Security aplica automáticamente la nueva configuración a la Prevención de intrusiones. Si, por ejemplo, ha permitido cambios en la configuración general de la directiva de Firewall (el candado está abierto), la configuración de Prevención de intrusiones también se podrá editar.
- Cuando se activa una [regla de paquete de red](#) en Kaspersky Endpoint Security 11.6.0 o versiones anteriores, la columna **Nombre de la aplicación** en el informe del Firewall siempre muestra el valor *Kaspersky Endpoint Security*. Asimismo, el Firewall bloqueará la conexión al nivel del paquete para todas las aplicaciones. Este comportamiento se ha modificado para Kaspersky Endpoint Security 11.7.0 o versiones posteriores. Se añadió la columna **Tipo de regla** al [informe del Firewall](#). Cuando se activa una regla de paquete de red, el valor en la columna **Nombre de la aplicación** permanece vacío.

### [Prevención de ataques de BadUSB](#)

- Kaspersky Endpoint Security restablece el límite de tiempo para el bloqueo del dispositivo USB cuando el ordenador está bloqueado (por ejemplo, cuando se cumple el límite de tiempo para el bloqueo de pantalla). Es decir, si introduce un código de autorización erróneo para el dispositivo USB muchas veces y la aplicación bloquea el dispositivo USB, Kaspersky Endpoint Security le permite repetir el intento de autorización después de desbloquear el ordenador. En este caso, Kaspersky Endpoint Security no bloquea el dispositivo USB durante el tiempo especificado en la [configuración del componente Prevención de ataques de BadUSB](#).
- Kaspersky Endpoint Security restablece el límite de tiempo de bloqueo del dispositivo USB cuando la [protección del ordenador está pausada](#). Es decir, si introduce un código de autorización erróneo para el dispositivo USB muchas veces y la aplicación bloquea el dispositivo USB, Kaspersky Endpoint Security le permite repetir el intento de autorización después de [reanudar la protección del ordenador](#). En este caso, Kaspersky Endpoint Security no bloquea el dispositivo USB durante el tiempo especificado en la [configuración del componente Prevención de ataques de BadUSB](#).

### [Control de aplicaciones](#)

- Solo se admiten archivos ZIP de menos de 104 MB cuando se administran reglas de Control de aplicaciones en Kaspersky Security Center Web Console. No se admiten archivos en otros formatos, como RAR o 7z. No existe tal restricción si trabaja con reglas de Control de aplicaciones en la Consola de administración (MMC).
- Cuando se trabaja en Microsoft Windows 10 en modo de lista de aplicaciones rechazadas, las reglas de bloqueo pueden aplicarse incorrectamente, lo que podría causar el bloqueo de aplicaciones que no están especificadas en las reglas.
- Cuando el componente Control de aplicaciones bloquea las aplicaciones web progresivas (PWA), appManifest.xml se indica como la aplicación bloqueada en el informe.
- Al añadir la aplicación estándar Bloc de notas a una regla de Control de aplicaciones para Windows 11, no se recomienda especificar la ruta a la aplicación. En equipos que ejecutan Windows 11, el sistema operativo utiliza Metro Notepad, ubicado en la carpeta C:\Archivos de programa\WindowsApps\Microsoft.WindowsNotepad\*\Notepad\Notepad.exe. En versiones anteriores del sistema operativo, Bloc de notas se encuentra en las siguientes carpetas:
  - C:\Windows\notepad.exe
  - C:\Windows\System32\notepad.exe
  - C:\Windows\SysWOW64\notepad.exe

Al añadir Bloc de notas a una regla de Control de aplicaciones, puede especificar el nombre de la aplicación y el hash del archivo desde las propiedades de la aplicación en ejecución, por ejemplo.

## Control de dispositivos

- El acceso a los dispositivos de impresión que se añadieron a la lista de confianza es bloqueado por las reglas de bloqueo de dispositivos y bus.
- Para los dispositivos MTP, se admite el control de las operaciones de lectura, escritura y conexión si está utilizando los controladores integrados de Microsoft del sistema operativo. Si un usuario instala un controlador personalizado para trabajar con un dispositivo (por ejemplo, como parte de iTunes o Android Debug Bridge), es posible que el control de las operaciones de lectura y escritura no funcione.
- Cuando se trabaja con dispositivos MTP, las reglas de acceso se cambian después de volver a conectar el dispositivo.
- Si está añadiendo un dispositivo a la lista de confianza según una máscara de modelo y usa caracteres que están incluidos en la ID pero no en el nombre del modelo, estos dispositivos no se añaden. En una estación de trabajo, estos dispositivos se añadirán a la lista de confianza según una máscara de identificación.

## Control Web

- Los formatos OGV y WEBM no son compatibles.
- El protocolo RTMP no es compatible.



## Control de anomalías adaptativo

- Se recomienda crear exclusiones automáticamente según el evento. Al [añadir manualmente una exclusión](#), añada el carácter \* al comienzo de la ruta al especificar el objeto de destino.
- [No se puede generar un informe de reglas de Control de anomalías adaptativo](#) si la muestra incluye al menos un evento cuyo nombre contiene más de 260 caracteres.
- No se admite la adición de exclusiones del repositorio Activación de reglas del Control de anomalías adaptativo si las propiedades de un objeto o proceso tienen un valor que supera los 256 caracteres (por ejemplo, una ruta a un objeto objetivo). Puede [añadir una exclusión manualmente en la configuración de directivas](#). También puede añadir una exclusión en el [informe sobre las reglas del Control de anomalías adaptativo](#).

## Cifrado de unidad (FDE)

- 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 del AES-NI (nuevas instrucciones del estándar de cifrado avanzado de Intel). Si el procesador no es compatible con las AES-NI, es posible que se disminuya el rendimiento del equipo.
- Cuando hay procesos que intentan acceder a dispositivos encriptados antes de que la aplicación les haya otorgado acceso a dichos dispositivos, la aplicación muestra una advertencia que indica que dichos procesos deben terminarse. Si los procesos no se pueden terminar, vuelva a conectar los dispositivos cifrados.
- Las ID únicas de los discos duros se muestran en las estadísticas de cifrado del dispositivo en formato invertido.
- No se recomienda formatear los dispositivos mientras se cifran.
- Cuando se conectan simultáneamente varias unidades extraíbles a un equipo, la política de cifrado se puede aplicar a una sola unidad extraíble. Cuando se vuelven a conectar los dispositivos extraíbles, la política de cifrado se aplica correctamente.
- Es posible que el cifrado no se inicie en un disco duro muy fragmentado. Desfragmentar el disco duro.
- Cuando los discos duros están cifrados, la hibernación se bloquea desde el momento en que comienza la tarea de cifrado hasta el primer reinicio de un equipo con Microsoft Windows 7/8/8.1/10, y después de la instalación del cifrado del disco duro hasta el primer reinicio de los sistemas operativos Microsoft Windows 8/8.1/10. Cuando se descifran los discos duros, la hibernación se bloquea desde el momento en que la unidad de arranque se descifra por completo hasta el primer reinicio del sistema operativo. Cuando la opción **Inicio rápido** está activada en Microsoft Windows 8/8.1/10, el bloqueo de la hibernación evita que apague el sistema operativo.
- Los equipos que cuenten con el sistema operativo Windows 7 no permiten cambiar la contraseña durante la recuperación cuando el disco está cifrado con tecnología BitLocker. Una vez que se introduce la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no le solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, no es posible establecer un nuevo código PIN o contraseña. Este problema proviene de las particularidades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.
- No se recomienda utilizar la herramienta xbootmgr.exe con proveedores adicionales activados. Por ejemplo, Dispatcher, Network o Drivers.
- No se admite el formateo de una unidad extraíble cifrada en un equipo que tenga instalado Kaspersky Endpoint Security para Windows.
- No se admite el formateo de una unidad extraíble cifrada con el sistema de archivos FAT32 (la unidad se muestra como cifrada). Para formatear una unidad, vuelva a formatearla con el sistema de archivos NTFS.
- Para obtener detalles sobre cómo restaurar un sistema operativo desde una copia de seguridad a un dispositivo GPT cifrado, visite la [Base de conocimientos de soporte técnico](#).
- No pueden coexistir varios agentes de descarga en un equipo cifrado.

- Es imposible acceder a una unidad extraíble que se cifró previamente en un equipo diferente cuando se cumplen todas las condiciones siguientes de manera simultánea:

- No hay conexión con el servidor de Kaspersky Security Center.
- El usuario está intentando la autorización con un nuevo token o contraseña.

Si ocurre una situación similar, reinicie el equipo. Una vez reiniciado el equipo, se otorgará acceso a la unidad extraíble encriptada.

- Es posible que el Agente de autenticación no admita el descubrimiento de dispositivos USB cuando el modo xHCI para USB está activado en la configuración del BIOS.
- El Cifrado de disco de Kaspersky (FDE) para la parte SSD de un dispositivo que se utiliza para almacenar en caché los datos utilizados con más frecuencia no es compatible con dispositivos SSHD.
- No se admite el cifrado de discos duros en sistemas operativos Microsoft Windows 8/8.1/10 de 32 bits que se ejecutan en modo UEFI.
- Reinicie el equipo antes de volver a cifrar un disco duro descifrado.
- El cifrado del disco duro no es compatible con Kaspersky Anti-Virus para UEFI. No se recomienda utilizar el cifrado del disco duro en equipos que tengan instalado Kaspersky Anti-Virus para UEFI.
- [La creación de cuentas del Agente de autenticación](#) basadas en cuentas de Microsoft se admite con las siguientes limitaciones:
  - La tecnología [Single Sign-On](#) no es compatible.
  - No se admite la creación automática de cuentas del Agente de autenticación si se selecciona la opción de crear cuentas para los usuarios que inician sesión en el sistema en los últimos N días.
- Si el nombre de una cuenta del Agente de autenticación tiene el formato <domain>/<Windows account name>, después de cambiar el nombre del equipo, también debe cambiar los nombres de las cuentas que se crearon para los usuarios locales de ese equipo. Por ejemplo, imagine que hay un usuario local Ivanov en el equipo Ivanov, y una cuenta de Agente de autenticación con el nombre Ivanov/Ivanov ha sido creado para este usuario. Si el nombre del equipo Ivanov se ha cambiado a Ivanov-PC, debe cambiar el nombre de la cuenta del Agente de autenticación para el usuario Ivanov de Ivanov/Ivanov a Ivanov-PC/Ivanov. Puede cambiar el nombre de la cuenta con la tarea de administración de cuentas del Agente de autenticación. Antes de que se haya cambiado el nombre de la cuenta, es posible la autenticación en el entorno previo al arranque utilizando el nombre antiguo (por ejemplo, Ivanov/Ivanov).
- Si a un usuario se le permite acceder a un equipo que fue encriptado usando la tecnología Cifrado de disco de Kaspersky solo usando un token, y este usuario necesita completar el procedimiento de recuperación de acceso, asegúrese de que este usuario tenga acceso basado en contraseña a este equipo después de que es acceso al equipo encriptado ha sido restaurado. Es posible que no se guarde la contraseña que estableció el usuario al restaurar el acceso. En este caso, el usuario tendrá que volver a completar el procedimiento para restaurar el acceso al equipo encriptado la próxima vez que se reinicie el equipo.
- Al descifrar un disco duro con la [Herramienta de recuperación FDE](#), el proceso de descifrado puede terminar con un error si los datos del dispositivo de origen se sobrescriben con los datos descifrados. Parte de los datos del disco duro permanecerán cifrados. Se recomienda elegir la opción para guardar los datos descifrados en un archivo en la configuración de descifrado del dispositivo cuando se utiliza la Herramienta de recuperación FDE.
- Si se ha cambiado la contraseña del Agente de autenticación, aparecerá un mensaje con el texto *Su contraseña se ha cambiada correctamente. Aparece la opción Haga clic en Aceptar* y el usuario reinicia el

equipo, la nueva contraseña no se guarda. La contraseña anterior se debe utilizar para la autenticación posterior en el entorno previo al arranque.

- El cifrado de disco es incompatible con la tecnología Intel Rapid Start.
- El cifrado de disco es incompatible con la tecnología ExpressCache.
- En algunos casos, al intentar descifrar una unidad cifrada con la [Herramienta de recuperación FDE](#), la herramienta detecta por error el estado del dispositivo como "no cifrado" después de que se completa el procedimiento "Solicitud-Respuesta". El registro de la herramienta muestra un evento que indica que el dispositivo se descifró correctamente. En este caso, debe reiniciar el procedimiento de recuperación de datos para descifrar el dispositivo.
- Una vez que el complemento de Kaspersky Endpoint Security para Windows se actualiza en Web Console, las propiedades del equipo del cliente no muestran la clave de recuperación de BitLocker hasta que se reinicia el servicio de Web Console.
- Para ver las otras limitaciones del soporte de cifrado de disco completo y una lista de dispositivos para los que el cifrado de discos duros es compatible con restricciones, consulte la [Base de conocimientos de soporte técnico](#).

### [Cifrado de archivos \(FLE\)](#)

- El cifrado de archivos y carpetas no es compatible con los sistemas operativos de la familia Microsoft Windows Embedded.
- Una vez instalada la aplicación, debe reiniciar el sistema operativo para que el cifrado de archivos y carpetas funcione correctamente.
- Si un archivo cifrado se almacena en un equipo que tiene la funcionalidad de cifrado disponible y usted accede al archivo desde un equipo donde el cifrado no está disponible, se proporcionará acceso directo a este archivo. Un archivo cifrado que se almacena en una carpeta de red en un equipo que tiene la función de cifrado disponible se copia en forma descifrada a un equipo que no tiene la función de cifrado disponible.
- Se recomienda descifrar los archivos que se cifraron con el Sistema de cifrado de archivos antes de cifrar los archivos con Kaspersky Endpoint Security para Windows.
- Después de cifrar un archivo, su tamaño aumenta en 4 kB.
- Después de cifrar un archivo, el atributo de *Archivo comprimido* se establece en las propiedades del archivo.
- Si un archivo que se descomprime de un archivo cifrado tiene el mismo nombre que un archivo que ya existe en su equipo, el nuevo archivo que se descomprimió de un archivo cifrado sobrescribirá al último. No se notifica al usuario sobre la operación de sobrescritura.
- Antes de descomprimir un archivo cifrado, asegúrese de tener suficiente espacio libre en el disco para alojar los archivos desempaquetados. Si no tiene suficiente espacio en disco, el desempaquetado del archivo puede completarse pero los archivos pueden dañarse. En este caso, es posible que Kaspersky Endpoint Security no muestre ningún mensaje de error.
- La interfaz de [Administrador de archivos portátil](#) no muestra mensajes sobre errores que ocurren durante su funcionamiento.
- Kaspersky Endpoint Security para Windows no inicia el [Administrador de archivos portátil](#) en un equipo que tiene instalado el componente Cifrado de archivos.
- No puede usar el [Administrador de archivos portátil](#) para acceder a una unidad extraíble si las siguientes condiciones se cumplen simultáneamente:
  - No hay conexión con Kaspersky Security Center;
  - Kaspersky Endpoint Security para Windows no está instalado en el equipo.
  - El cifrado de datos (FDE o FLE) no se ha realizado en el equipo.

El acceso es imposible aunque se conozca la contraseña del Administrador de archivos portátil.

- Cuando se utiliza el cifrado de archivos, la aplicación es incompatible con el cliente de correo Sylpheed.
- Kaspersky Endpoint Security para Windows no es compatible con [la regla de restricción de acceso a archivos cifrados](#) para algunas aplicaciones. Esto se debe al hecho de que algunas operaciones de archivo las realiza una aplicación de terceros. Por ejemplo, el copiado de archivos lo realiza el administrador de archivos, no la aplicación en sí. De esta forma, si el acceso a los archivos cifrados se deniega al cliente de correo Outlook, Kaspersky Endpoint Security permitirá al cliente de correo acceder al archivo cifrado si el usuario ha copiado archivos en el mensaje de correo electrónico mediante el portapapeles o usando la función de arrastrar y soltar. La operación de copiado la realiza un administrador de archivos, para el que no se especifican las reglas de restricción de acceso a archivos cifrados (es decir, se permite el acceso).

- Cuando las unidades extraíbles están cifradas con [soporte para modo portátil](#), el control de antigüedad de la contraseña no se puede desactivar.
- No se admite el cambio de la configuración del archivo de página. El sistema operativo utiliza los valores predeterminados en lugar de los valores de los parámetros especificados.
- Utilice la extracción segura cuando trabaje con unidades extraíbles cifradas. No podemos garantizar la integridad de los datos si la unidad extraíble no se extrae de forma segura.
- Una vez que los archivos están cifrados, sus originales no cifrados se eliminan de forma segura.
- No se admite la sincronización de archivos offline mediante el Almacenamiento en caché del lado del cliente (CSC). Se recomienda prohibir la administración offline de recursos compartidos a nivel de directiva del grupo. Los archivos que están en modo offline se pueden editar. Después de la sincronización, es posible que se pierdan los cambios realizados en un archivo offline. Para obtener detalles sobre la compatibilidad con el Almacenamiento en caché del lado del cliente (CSC) al utilizar el cifrado, consulte la [Base de conocimientos de soporte técnico](#).
- No se admite la [creación de un archivo comprimido cifrado](#) en la raíz del disco duro del sistema.
- Puede experimentar problemas al acceder a archivos cifrados a través de la red. Se recomienda mover los archivos a una fuente diferente o asegurarse de que el equipo que se utiliza como servidor de archivos esté administrado por el mismo Servidor de administración de Kaspersky Security Center.
- Cambiar la distribución del teclado puede hacer que se bloquee la ventana de introducción de la contraseña para un archivo autoextraíble cifrado. Para resolver este problema, cierre la ventana de introducción de la contraseña, cambie la distribución de teclado en su sistema operativo y vuelva a introducir la contraseña para el archivo comprimido cifrado.
- Cuando se utiliza el cifrado de archivos en sistemas que tienen varias particiones en un disco, se recomienda utilizar la opción que determina automáticamente el tamaño del archivo pagefile.sys. Una vez que el equipo se reinicia, el archivo pagefile.sys puede moverse entre las particiones del disco.
- Después de aplicar las reglas de cifrado de archivos, incluidos los archivos de la carpeta Mis documentos, asegúrese de que los usuarios a los que se les ha aplicado el cifrado puedan acceder correctamente a los archivos cifrados. Para hacerlo, haga que cada usuario inicie sesión en el sistema cuando haya una conexión a Kaspersky Security Center disponible. Si un usuario intenta acceder a archivos cifrados sin una conexión a Kaspersky Security Center, el sistema puede bloquearse.
- Si los archivos del sistema se incluyen de alguna manera en el alcance del cifrado de archivos, es posible que en los informes aparezcan eventos relacionados con errores al cifrar estos archivos. Los archivos especificados en estos eventos no están realmente encriptados.
- Los procesos PICO no son compatibles.
- No se admiten las rutas que distinguen entre mayúsculas y minúsculas. Cuando se aplican reglas de cifrado o reglas de descifrado, las rutas de los eventos del producto se muestran en minúsculas.
- No se recomienda cifrar los archivos que utiliza el sistema al inicio. Si estos archivos están cifrados, un intento de acceder a archivos cifrados sin una conexión a Kaspersky Security Center puede hacer que el sistema se bloquee o genere solicitudes de acceso a los archivos no cifrados.
- Si los usuarios trabajan conjuntamente con un archivo en la red bajo reglas FLE a través de aplicaciones que utilizan el método de asignación de archivo a memoria (como WordPad o FAR) y aplicaciones diseñadas para trabajar con archivos grandes (como Notepad ++), el archivo en forma no cifrada se puede bloquear indefinidamente sin la capacidad de acceder a él desde el equipo en el que reside.

- Kaspersky Endpoint Security no cifra los archivos que se encuentran en el almacenamiento en la nube de OneDrive o en otras carpetas que tienen OneDrive como nombre. Kaspersky Endpoint Security también bloquea la copia de archivos cifrados a carpetas de OneDrive si esos archivos no se añaden a la [regla de descifrado](#).
- Cuando se instala el componente de cifrado de archivos, la gestión de usuarios y grupos no funciona en modo WSL (Subsistema de Windows para Linux).
- Cuando está instalado el componente de cifrado de nivel de archivo, no se admite POSIX (Interfaz de sistema operativo portátil) para cambiar el nombre y eliminar archivos.
- No se recomienda cifrar los archivos temporales, ya que esto puede provocar la pérdida de datos. Por ejemplo, Microsoft Word crea archivos temporales al procesar un documento. Si se cifran los archivos temporales, pero no el archivo original, el usuario puede recibir un error de *Acceso denegado* al intentar guardar el documento. Además, Microsoft Word puede llegar a guardar el archivo, pero no se podrá abrir el documento la próxima vez que se intente hacerlo, lo cual quiere decir que se perderán los datos. Para evitar la pérdida de datos, deberá [excluir la carpeta de archivos temporales de las reglas de cifrado](#).
- Después de actualizar Kaspersky Endpoint Security para Windows a la versión 11.0.1 o una anterior, para acceder a los archivos cifrados después de reiniciar el ordenador, compruebe que el Agente de red esté en ejecución. El Agente de red se inicia con un retraso, por lo cual no podrá acceder a los archivos cifrados inmediatamente después de que se cargue el sistema operativo. No es necesario esperar a que se inicie el Agente de red después del siguiente inicio del ordenador.

#### [Otras limitaciones](#)

- Si la aplicación devuelve errores o se bloquea durante el funcionamiento, puede reiniciarse automáticamente. Si la aplicación encuentra errores recurrentes que provocan el fallo de la aplicación, esta realiza las operaciones siguientes:
  1. Desactiva las funciones de control y protección (la funcionalidad de cifrado permanece activa).
  2. Informa al usuario de que las funciones se han desactivado.
  3. Trata de restablecer la funcionalidad de la aplicación después de actualizar las bases de datos antivirus o de aplicar las actualizaciones de los módulos de la aplicación.
- Las direcciones web que se [añadir a la lista de confianza](#) pueden procesarse incorrectamente.
- Kaspersky Endpoint Security supervisa el tráfico HTTP que cumple con los estándares RFC 2616, RFC 7540, RFC 7541, RFC 7301. Si Kaspersky Endpoint Security detecta otro formato de intercambio de datos en el tráfico HTTP, la aplicación bloquea esta conexión para evitar que se descarguen archivos maliciosos de Internet.
- Kaspersky Endpoint Security evita la comunicación a través del protocolo QUIC. Los navegadores usan el protocolo de transporte estándar (TLS o SSL) independientemente de que la compatibilidad con QUIC esté activada en el navegador o no.
- System Watcher. No se muestra la información completa sobre los procesos.
- Cuando se inicia Kaspersky Endpoint Security para Windows por primera vez, es posible que una aplicación firmada digitalmente se coloque temporalmente en el grupo incorrecto. Después, la aplicación firmada digitalmente se incluirá en el grupo correcto.
- Al analizar el correo con la [extensión Protección frente a amenazas en el correo para Microsoft Outlook](#), se recomienda utilizar el modo de intercambio en caché (la opción Usar modo de intercambio en caché).
- La [tarea Análisis antivirus](#) no es compatible con la versión de 64 bits de Microsoft Outlook. Esto significa que Kaspersky Endpoint Security no analiza los archivos de 64 bits de MS Outlook (archivos PST y OST) si hay una versión de 64 bits de MS Outlook instalada en el equipo, aunque [el correo esté incluido en la cobertura del análisis](#).
- En Kaspersky Security Center, cuando se pasa de utilizar Kaspersky Security Network global a utilizar Kaspersky Security Network privada, o viceversa, la [opción de participar en Kaspersky Security Network está desactivada](#) en la directiva del producto. Después del cambio, lea atentamente el texto de la Declaración de Kaspersky Security Network y confirme su consentimiento para participar en KSN. Puede leer el texto de la Declaración en la interfaz de la aplicación o al editar la directiva del producto.
- Durante una nueva exploración de un objeto malicioso que fue bloqueado por software de terceros, no se notifica al usuario cuando se detecta nuevamente la amenaza. El evento de nueva detección de amenazas se muestra en el informe del producto y en el informe de Kaspersky Security Center.
- El componente [Endpoint Sensor](#) no se puede instalar en Microsoft Windows Server 2008.
- El informe de Kaspersky Security Center sobre el cifrado de dispositivos no incluirá información sobre los dispositivos que se cifraron con Microsoft BitLocker en plataformas del servidor o en estaciones de trabajo en las que no está instalado el componente Control de dispositivos.
- No se puede activar la visualización de todas las entradas del informe en Kaspersky Security Center Web Console. En Web Console, solo se puede cambiar la cantidad de entradas que se muestra en los informes. De manera predeterminada, Kaspersky Security Center Web Console muestra 1000 entradas por informe. Puede activar la visualización de todas las entradas de los informes en Consola de administración (MMC).



- No se puede establecer la visualización de más de 1000 entradas por informe en Kaspersky Security Center Console. Si establece un valor superior a 1000, Kaspersky Security Center Console mostrará 1000 entradas por informe.
- Cuando se utiliza una jerarquía de directivas, se puede acceder a la configuración de la sección Cifrado de unidades extraíbles en una directiva secundaria para editarla, si la directiva principal prohíbe la modificación de esa configuración.
- Debe activar Audit Logon en la configuración del sistema operativo para garantizar el correcto funcionamiento de las [exclusiones para la protección de carpetas compartidas frente al cifrado externo](#).
- Si la [protección de carpetas compartidas está activada](#), Kaspersky Endpoint Security para Windows supervisa los intentos de cifrar las carpetas compartidas para cada sesión de acceso remoto que se inició antes del inicio de Kaspersky Endpoint Security para Windows, incluso si el equipo desde el que se inició la sesión de acceso remoto ha sido añadido a las exclusiones. Si no desea que Kaspersky Endpoint Security para Windows supervise los intentos de cifrar las carpetas compartidas para las sesiones de acceso remoto que se iniciaron desde un equipo que se añadió a las exclusiones y que se iniciaron antes del inicio de Kaspersky Endpoint Security para Windows, finalice y vuelva a establecer la sesión de acceso remoto o reinicie el equipo en el que está instalado Kaspersky Endpoint Security para Windows.
- Si la [tarea de actualización se ejecuta con los permisos de una cuenta de usuario específica](#), los parches del producto no se descargarán cuando se actualice desde una fuente que requiera autorización.
- Es posible que la aplicación no se inicie debido a un rendimiento insuficiente del sistema. Para resolver este problema, use la opción Ready Boot o aumente el tiempo de espera del sistema operativo para iniciar los servicios.
- La aplicación no puede funcionar en Modo seguro.
- Para garantizar que las versiones 11.5.0 y 11.6.0 de Kaspersky Endpoint Security para Windows puedan funcionar correctamente con el software Cisco AnyConnect, debe instalar el Módulo de cumplimiento versión 4.3.183.2048 o posterior. Más información sobre la compatibilidad con Cisco Identity Services Engine en la [documentación de Cisco](#).
- No podemos garantizar el funcionamiento de Audio Control hasta después del primer reinicio luego de instalar la aplicación.
- En la Consola de administración (MMC), en la configuración de la Prevención de intrusiones en la ventana para configurar los permisos de las aplicaciones, el botón **Eliminar** no está disponible. Puede eliminar una aplicación de un grupo de confianza mediante el menú contextual de la aplicación.
- En la interfaz local de la aplicación, en la configuración de Prevención de intrusiones, los permisos de la aplicación y los recursos protegidos no están disponibles para su visualización si el equipo está gestionado por una directiva. Los controles de desplazamiento, búsqueda, filtro y otras ventanas no están disponibles. Puede ver los permisos de la aplicación en las propiedades de la directiva en Kaspersky Security Center Console.
- Cuando los archivos de seguimiento rotados están activados, no se crean seguimientos para el componente AMSI y el complemento de Outlook.
- Los seguimientos de rendimiento no se pueden recopilar manualmente en Windows Server 2008.
- No se admiten seguimientos de rendimiento para el tipo de seguimiento "Reiniciar".
- El registro de volcado no es compatible con el proceso Pico.
- La tarea de verificación de disponibilidad de KSN ya no es compatible.

- Deshabilitar la opción "Desactivar la administración externa de los servicios del sistema" no le permitirá detener el servicio de la aplicación que se instaló con el parámetro AMPPL=1 (de forma predeterminada, el valor del parámetro se establece en 1 comenzando con la versión del sistema operativo Windows 10RS2). El parámetro AMPPL con un valor de 1 habilita el uso de la tecnología de Procesos de protección para el servicio del producto.
- Para ejecutar un análisis personalizado de una carpeta, el usuario que inicia el análisis personalizado debe tener los permisos para leer los atributos de esta carpeta. De lo contrario, el análisis personalizado de carpetas será imposible y terminará con un error.
- Cuando una regla de análisis definida en una directiva incluye una ruta sin el carácter `\` al final, por ejemplo, `C:\fo1der1\fo1der2`, el análisis se ejecutará para la ruta `C:\fo1der1\`.
- Al actualizar la aplicación de la versión 11.1.0 a la 11.8.0, la configuración de Protección vía AMSI se restablece a sus valores predeterminados.
- Si utiliza directivas de restricción de software (SRP), es posible que el equipo no cargue (muestre una pantalla negra). Recomendamos que cambie la configuración de SRP de la siguiente manera: configure el valor de **Todos los archivos de software excepto bibliotecas (como DLL)** para el parámetro **Aplicar directivas de restricción de software a los siguientes objetos**, y añada reglas con el nivel de seguridad **Sin restricciones** para las rutas a los archivos de la aplicación (`C:\Program Files\Common Files\Kaspersky Lab` y `C:\Program Files\Kaspersky Lab`). Para obtener más información sobre SRP, consulte la [documentación de Microsoft](#).
- Si el equipo pertenece a un dominio del objeto de directivas de grupo (GPO) de Microsoft con el parámetro DriverLoadPolicy establecido en 8 (solo Bueno), reiniciar el equipo con Kaspersky Endpoint Security instalado provoca un BSOD. Para que se produzca un fallo, el parámetro Antimalware de inicio temprano (ELAM) de la directiva de grupo debe estar establecido en 1 (Bueno y desconocido). La configuración de ELAM se encuentra en la directiva en: **Configuración del equipo** → **Plantillas administrativas** → **Sistema** → **Antimalware de inicio temprano**.
- No se admite la administración de la configuración del complemento de Outlook a través de Rest API.
- La configuración de ejecución de tareas para un usuario específico no se puede transferir entre dispositivos a través de un archivo de configuración. Después de aplicar la configuración desde un archivo de configuración, especifique manualmente el nombre de usuario y la contraseña.
- Después de instalar una actualización, la tarea de comprobación de integridad no funciona hasta que se reinicia el sistema para aplicar la actualización.
- Cuando el nivel de seguimiento rotado se cambia a través de la utilidad de diagnóstico remoto, Kaspersky Endpoint Security para Windows muestra incorrectamente un valor en blanco para el nivel de seguimiento. Sin embargo, los archivos de seguimiento se escriben según el nivel de seguimiento correcto. Cuando el nivel de seguimiento rotado se cambia a través de la interfaz local de la aplicación, el nivel de seguimiento se modifica correctamente pero la utilidad de diagnóstico remoto muestra incorrectamente el nivel de seguimiento que fue definido por última vez por la utilidad. Esto puede hacer que el administrador no tenga información actualizada sobre el nivel de seguimiento actual, y la información relevante puede estar ausente de los seguimientos si un usuario cambia manualmente el nivel de seguimiento en la interfaz local de la aplicación.
- En la interfaz local, la configuración de Protección con contraseña no permite cambiar el nombre de la cuenta de administrador (de forma predeterminada, KLAdmin). Para cambiar el nombre de la cuenta de administrador, debe deshabilitar Protección con contraseña y, a continuación, habilitar Protección con contraseña y especificar un nuevo nombre de la cuenta de administrador.
- No puede analizar un objeto puesto en cuarentena como resultado de la tarea de [Mover archivo a Cuarentena](#).

- Kaspersky Endpoint Security no ejecuta tareas de [análisis de IOC](#) en las unidades de red si la ruta de la carpeta en las propiedades de la tarea comienza con la letra de una unidad. Kaspersky Endpoint Security solo admite el formato de ruta UNC para tareas de [análisis de IOC](#) en las unidades de red. Por ejemplo, `\\server\shared_folder`.
- La [importación de un archivo de configuración de una aplicación](#) termina en un error si la configuración de [integración con Kaspersky Sandbox](#) está activada en el archivo de configuración. Antes de exportar los ajustes de la aplicación, desactive Kaspersky Sandbox. Luego, realice el procedimiento de exportación/importación. Una vez importado el archivo de configuración, active Kaspersky Sandbox.
- Cuando se detecta un indicador de compromiso durante la ejecución de una tarea de [análisis de IOC](#), la aplicación pone en cuarentena solo un archivo para el término FileItem. La cuarentena de archivos para otros términos no es compatible.
- No es posible colocar en cuarentena un flujo de datos alternativo (ADS) que supere los 4 MB. Kaspersky Endpoint Security omite tales ADS sin notificar al usuario.
- Para administrar los detalles de las alertas, necesitará el complemento web de Kaspersky Endpoint Security para Windows 11.7.0 o posterior. Los detalles de las alertas son necesarios para la solución [Endpoint Detection and Response](#) (EDR Optimum y EDR Expert). Los detalles de la alerta están disponibles solo en Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console.
- 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).

# Glosario

## Administrador de archivos portátil

Aplicación que brinda una interfaz para trabajar con archivos cifrados en unidades extraíbles cuando las funciones de cifrado necesarias para ello no están disponibles en el equipo.

## Agente de autenticación

Interfaz que le permite completar la autenticación para acceder a discos duros cifrados y cargar el sistema operativo después del cifrado del disco duro de arranque.

## Agente de red

Un componente de Kaspersky Security Center que permite la interacción entre el servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es común a todas las aplicaciones de Kaspersky que se ejecutan con Windows. Las versiones dedicadas del Agente de red están destinadas para aplicaciones que se ejecutan con otros sistemas operativos.

## Archivador

Uno o varios archivos comprimidos en un solo archivo comprimido. Se requiere una aplicación especializada llamada "archivador" para comprimir y descomprimir datos.

## Archivo de IOC

Un archivo que contiene un conjunto de indicadores de compromiso (IOC) que la aplicación intenta hacer coincidir para contar una detección. La probabilidad de detección puede ser mayor si se encuentran coincidencias exactas con múltiples archivos de IOC para el objeto como resultado del análisis.

## Archivo infectable

Un archivo que, por su estructura o formato, puede ser utilizado por intrusos como "contenedor" y distribuidor de un código malicioso. Como regla, estos son archivos ejecutables, con extensiones de archivo como .com, .exe y .dll. Hay un riesgo bastante alto de intrusión de código malicioso en esos archivos.

## Archivo infectado

Un archivo que contiene código malicioso (se ha detectado código de software malicioso [malware] conocida durante el análisis del archivo). Kaspersky no recomienda utilizar estos archivos, ya que podrían infectar el equipo.

## Base de datos de direcciones web maliciosas

Lista de direcciones web cuyo contenido puede considerarse como peligroso. Los expertos de Kaspersky se encargan de crear la lista. Se actualiza con regularidad y está incluida en el kit de distribución de la aplicación de Kaspersky.

## Base de datos de direcciones web phishing

Una lista de direcciones web que los especialistas de Kaspersky han determinado como relacionadas con phishing. La base de datos se actualiza con regularidad y forma parte del kit de distribución de la aplicación de Kaspersky.

## Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas de la seguridad del equipo que conoce Kaspersky a la fecha en la que se publica la base de datos antivirus. Las firmas de bases de datos antivirus ayudan a detectar código malicioso en objetos analizados. Los autores de estas bases de datos antivirus son especialistas de Kaspersky, que las actualizan cada hora.

## Certificado de licencia

Un documento que Kaspersky transfiere al usuario junto con el archivo clave o el código de activación. Contiene información sobre la licencia que se concede al usuario.

## Clave activa

Clave que utiliza la aplicación actualmente.

## Clave adicional

Clave que certifica el derecho a utilizar la aplicación, pero que actualmente no se utiliza.

## Cobertura de protección

Objetos que son analizados constantemente por el componente Protección frente a amenazas básicas cuando este se ejecuta. Las coberturas de protección de los distintos componentes tienen distintas propiedades.

## Cobertura del análisis

Objetos que Kaspersky Endpoint Security analiza mientras realiza una tarea de análisis.

## Desinfección

Método de procesamiento de objetos infectados que da lugar a la recuperación completa o parcial de datos. No se pueden desinfectar todos los objetos infectados.

## Emisor del certificado

El centro de certificación que emitió el certificado.

## Falsa alarma

Una falsa alarma se produce cuando la aplicación Kaspersky notifica un archivo que no está infectado como infectado, porque la firma del archivo es similar a la de un virus.

## Forma normalizada de la dirección de un recurso web

La forma normalizada de la dirección de un recurso web es una representación textual de la dirección de un recurso web obtenido a través de la normalización. La normalización es un proceso mediante el que la representación textual de la dirección de un recurso web cambia de acuerdo con reglas concretas (por ejemplo, exclusión del nombre de usuario, contraseña y puerto de conexión de la representación textual de la dirección del recurso web; además, la dirección del recurso web cambia de mayúsculas a minúsculas).

En cuanto al funcionamiento de componentes de protección, el fin de la normalización de las direcciones de recursos web consiste en evitar analizar varias veces direcciones de sitios web que puedan diferir en la sintaxis, pese a ser físicamente equivalente.

Ejemplo:

Forma no normalizada de una dirección: `www.Example.com\.`

Forma normalizada de una dirección: `www.example.com.`

## Grupo de administración

Un conjunto de dispositivos que comparten funciones comunes y un conjunto de aplicaciones de Kaspersky instaladas en ellos. Los dispositivos se agrupan de modo que se puedan administrar de forma práctica como una sola unidad. Un grupo puede incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada una de las aplicaciones instaladas en el grupo.

## IOC

Indicador de compromiso Un conjunto de datos sobre una actividad u objeto malicioso.

## Máscara

Representación del nombre de un archivo y de su extensión mediante comodines.

Las máscaras de archivos pueden contener cualquier carácter que se permita en los nombres de archivos, incluidos comodines:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
- Dos caracteres `**` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en la carpeta llamada `Carpeta` y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. La máscara `**` solo puede usarse para crear exclusiones del análisis.
- El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Carpeta` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

## Módulo de plataforma segura

Un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del ordenador e interactúa con todos los otros componentes del sistema a través del bus de hardware.

## Objeto OLE

Un archivo adjunto o un archivo incrustado en otro archivo. Las aplicaciones de Kaspersky permiten analizar objetos OLE en busca de virus. Por ejemplo, si incluye una tabla de Microsoft Excel® en un documento de Microsoft Office Word, la aplicación analizará la tabla como un objeto OLE.

## OpenIOC

Estándar abierto de descripciones de indicadores de compromiso (IOC) basado en XML y que incluye más de 500 indicadores de compromiso diferentes.

## Tarea

Funciones realizadas por la aplicación de Kaspersky como tareas, por ejemplo: Protección de archivos de tiempo real, Análisis completo de dispositivo, Actualización de bases de datos.

# Apéndices

Esta sección contiene información que complementa el cuerpo del documento.

## Apéndice 1. Configuración de la aplicación

Puede utilizar una [directiva](#), [tareas](#) o la [interfaz de la aplicación](#) para configurar Kaspersky Endpoint Security. En las secciones correspondientes se proporciona información detallada sobre los componentes de la aplicación.

### Protección frente a amenazas en archivos

El componente Protección frente a amenazas en archivos le permite evitar la infección del sistema de archivos del equipo. De forma predeterminada, el componente Protección frente a amenazas en archivos permanece todo el tiempo en la RAM del equipo. El componente analiza los archivos en todas las unidades del equipo, así como en las unidades conectadas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

El componente analiza los archivos a los que accede el usuario o la aplicación. Si se detecta un archivo malicioso, Kaspersky Endpoint Security bloquea la operación del archivo. A continuación, la aplicación desinfecta o elimina el archivo malicioso, en función de la configuración del componente Protección frente a amenazas en archivos.

Cuando se intenta acceder a un archivo cuyo contenido está almacenado en la nube de OneDrive, Kaspersky Endpoint Security descarga el contenido y lo analiza.

Configuración de componente Protección frente a amenazas en archivos

Parámetro	Descripción
<b>Nivel de seguridad</b> (disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)	<p>Para Protección frente a amenazas en archivos, Kaspersky Endpoint Security puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan <i>niveles de seguridad</i>.</p> <ul style="list-style-type: none"><li>• <b>Máximo.</b> Si se selecciona este nivel de seguridad de archivos, el componente Protección frente a amenazas en archivos realiza el control más estricto de todos los archivos abiertos, guardados y ejecutados. El componente Protección frente a amenazas en archivos analiza todos los tipos de archivos en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. También analiza archivos comprimidos, paquetes de instalación y objetos OLE incrustados.</li><li>• <b>Recomendado.</b> Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección frente a amenazas en archivos solo analiza los formatos de archivos especificados en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo y en los objetos de OLE incrustados. El componente Protección frente a amenazas en archivos no analiza los archivos ni los paquetes de instalación.</li><li>• <b>Mínimo.</b> La configuración de este nivel de seguridad garantiza la velocidad máxima de análisis. El componente Protección frente a amenazas en archivos solo analiza los archivos con extensiones especificadas en todas las unidades de disco duro, unidades de red y unidades extraíbles del equipo. El componente Protección frente a amenazas en archivos no analiza los archivos compuestos.</li></ul>



<p><b>Tipos de archivos</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p><b>Todos los archivos.</b> Si se activa este parámetro, Kaspersky Endpoint Security comprueba todos los archivos sin excepción (todos los formatos y extensiones).</p> <p><b>Archivos analizados por formato.</b> Si se activa este parámetro, Kaspersky Endpoint Security analiza <u>únicamente los archivos infectables</u> <a href="#">?</a>. Antes de analizar un archivo en busca de código malicioso, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.</p> <p><b>Archivos analizados por extensión.</b> Si se activa este parámetro, Kaspersky Endpoint Security analiza <u>únicamente los archivos infectables</u> <a href="#">?</a>. El formato de archivo se determina en función de su extensión.</p>
<p><b>Cobertura del análisis</b></p>	<p>Contiene objetos que son analizados por el componente Protección frente a amenazas en archivos. Los objetos de análisis pueden ser discos duros, unidades extraíbles o de red, carpetas, archivos individuales o máscaras que engloben varios archivos.</p> <p>De forma predeterminada, el componente Protección frente a amenazas en archivos analiza los archivos ejecutados en cualquier disco duro, en las unidades de red o en las unidades extraíbles. El alcance de protección de estos objetos no puede modificarse ni eliminarse. Sí es posible excluir un objeto (por ejemplo, una unidad extraíble) de los análisis.</p>
<p><b>Aprendizaje automático y análisis de firmas</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>El método de aprendizaje automático y análisis de firmas utiliza la base de datos de Kaspersky Endpoint Security, que contiene descripciones de las amenazas conocidas y métodos para erradicarlas. La protección que utiliza este método proporciona el nivel de seguridad mínimo aceptable.</p> <p>Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas siempre están activados.</p>
<p><b>Análisis heurístico</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.</p> <p>Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.</p>
<p><b>Acción al detectar una amenaza</b></p>	<p><b>Desinfectar; eliminar si la desinfección falla.</b> Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.</p> <p><b>Desinfectar; bloquear si falla la desinfección.</b> Si se selecciona esta opción, Kaspersky Endpoint Security automáticamente trata de desinfectar todos los archivos infectados que se detecten. Si la desinfección no es posible, Kaspersky Endpoint Security añade información sobre los archivos infectados que se detectan a la lista de amenazas activas.</p> <p><b>Bloquear.</b> Si se selecciona esta opción, el componente Protección frente a amenazas en archivos automáticamente bloquea todos los archivos infectados sin intentar desinfectarlos.</p>

	<p>Antes de intentar desinfectar o eliminar un archivo infectado, Kaspersky Endpoint Security crea una copia de seguridad del archivo en caso de que necesite <a href="#">restaurarlo o que sea posible desinfectarlo en el futuro</a>.</p>
<b>Analizar solamente archivos nuevos y modificados</b>	<p>Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como a compuestos.</p>
<b>Analizar archivos</b>	<p>Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo. Kaspersky Endpoint Security analiza los archivos no solo por su extensión, sino también por su formato.</p>
<b>Analizar paquetes de distribución</b>	<p>Use esta casilla para activar o desactivar el análisis de paquetes de distribución de terceros.</p>
<b>Analizar archivos en formatos de Microsoft Office</b>	<p>Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.</p>
<b>No descomprimir archivos compuestos grandes</b>	<p>Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security no escanea archivos compuestos cuyo tamaño exceda el valor especificado.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.</p> </div>
<b>Extraer archivos compuestos en segundo plano</b>	<p>Si la casilla de verificación está seleccionada, Kaspersky Endpoint Security proporciona acceso a archivos compuestos cuyo tamaño sea superior al valor especificado antes de analizar estos archivos. En este caso, Kaspersky Endpoint Security extrae y analiza los archivos compuestos en segundo plano.</p> <p>Kaspersky Endpoint Security proporciona acceso a archivos compuestos cuyo tamaño sea inferior a este valor solo después de extraer y analizar estos archivos.</p> <p>Si la casilla de verificación no está seleccionada, Kaspersky Endpoint Security proporciona acceso a archivos compuestos solo después de extraer y analizar archivos de cualquier tamaño.</p>
<b>Modo de análisis</b> <i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>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.</p> </div> <p><b>Modo inteligente.</b> En este modo, Protección frente a amenazas en archivos analiza un objeto en función de un análisis de las acciones aplicadas al objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.</p>

	<p><b>Al acceder y modificar.</b> En este modo, Protección frente a amenazas en archivos analiza objetos cuando se intenta abrirlos o modificarlos.</p> <p><b>Al acceder.</b> En este modo, Protección frente a amenazas en archivos analiza objetos solo tras intentar abrirlos.</p> <p><b>Al ejecutar.</b> En este modo, Protección frente a amenazas en archivos solo analiza objetos tras intentar ejecutarlos.</p>
<p><b>Tecnología iSwift</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.</p>
<p><b>Tecnología iChecker</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>Esta tecnología permite aumentar la velocidad del análisis mediante la exclusión de ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta las fechas de las bases de datos de Kaspersky Endpoint Security, la fecha del último análisis del archivo y cualquier modificación realizada en la configuración del análisis. La tecnología iChecker presenta limitaciones: no funciona con archivos de gran tamaño y se aplica solamente a los archivos que tienen una estructura que reconoce la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, y RAR).</p>
<p><b>Pausar la Protección frente a amenazas en archivos</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>Esto detiene temporalmente y automáticamente el funcionamiento de Protección frente a amenazas en archivos a la hora especificada o al trabajar con las aplicaciones especificadas.</p>

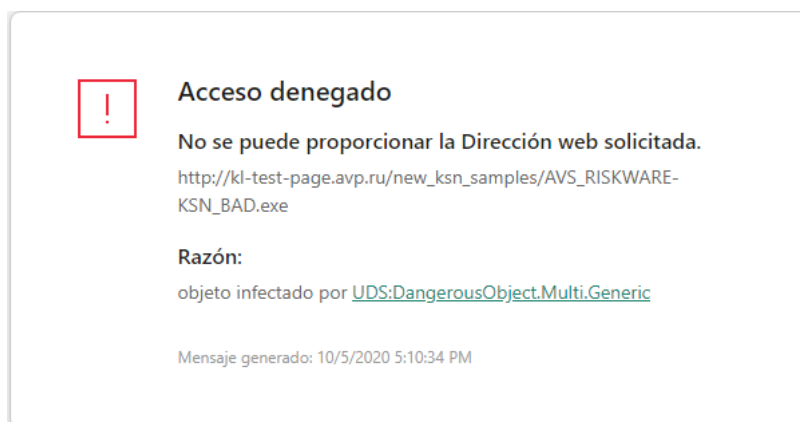
## Protección frente a amenazas web

El componente Protección frente a amenazas web evita la descarga de archivos maliciosos de Internet y también bloquea los sitios web maliciosos y de phishing. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

Kaspersky Endpoint Security analiza tráfico HTTP, HTTPS y FTP. Kaspersky Endpoint Security analiza direcciones IP y URLs. Puede [especificar los puertos que Kaspersky Endpoint Security supervisará](#) o seleccionar todos los puertos.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario [activar el análisis de conexiones cifradas](#).

Cuando un usuario intenta abrir un sitio web malicioso o de phishing, Kaspersky Endpoint Security bloqueará el acceso y le mostrará una advertencia (vea la imagen más abajo).



Mensaje de acceso al sitio web denegado

Configuración de componente Protección frente a amenazas web

Parámetro	Descripción
<b>Nivel de seguridad</b> <i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i>	<p>Para la Protección frente a amenazas web, Kaspersky Endpoint Security puede aplicar diferentes grupos de parámetros. Estos grupos de parámetros guardados en la aplicación se denominan <i>niveles de seguridad</i>.</p> <ul style="list-style-type: none"><li>• <b>Alta.</b> El nivel de seguridad en el que componente Protección frente a amenazas web realiza el máximo análisis del tráfico web que el equipo recibe a través de los protocolos HTTP y FTP. Protección frente a amenazas web analiza en detalle todos los objetos del tráfico web mediante todo el conjunto de bases de datos de la aplicación, y realiza el <a href="#">análisis heurístico</a> más exhaustivo posible.</li><li>• <b>Recomendado.</b> El nivel de seguridad que ofrece el equilibrio perfecto entre el rendimiento de Kaspersky Endpoint Security y la seguridad del tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web.</li><li>• <b>Baja.</b> La configuración de este nivel de seguridad de tráfico web garantiza el análisis más rápido de tráfico web. El componente Protección frente a amenazas web realiza un análisis heurístico en el nivel Análisis medio.</li></ul>
<b>Acción al detectar una amenaza</b>	<p><b>Bloquear descarga.</b> Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.</p> <p><b>Notificar.</b> Si esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, Kaspersky Endpoint Security permite que este objeto se descargue en el equipo, pero añade información sobre el objeto a la lista de amenazas activas.</p>
<b>Contrastar la dirección web con la base de datos de direcciones</b>	<p>Al analizar los enlaces para determinar si están incluidos en la base de datos de direcciones web maliciosas, se le permite rastrear sitios web que hayan sido incluidos en la lista de rechazados. Kaspersky realiza el mantenimiento de la base de datos de direcciones web maliciosas, que se incluye en el paquete de instalación de la aplicación y que se actualiza con las actualizaciones de la base de datos de Kaspersky Endpoint Security.</p>

<p><b>web maliciosas</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	
<p><b>Usar análisis heurístico</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.</p> <p>Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico realiza instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.</p>
<p><b>Contrastar la dirección web con la base de datos de direcciones web de phishing</b></p> <p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>La base de datos de direcciones web fraudulentas incluye las direcciones web de sitios actualmente conocidos que se emplean para lanzar ataques fraudulentos. Kaspersky complementa esta base de datos de enlaces de phishing con direcciones obtenidas de la organización internacional conocida como Anti-Phishing Working Group. La base de datos de direcciones fraudulentas se incluye en el paquete de instalación de la aplicación y se complementa con actualizaciones de la base de datos de Kaspersky Endpoint Security.</p>
<p><b>No analizar tráfico Web de direcciones Web de confianza</b></p>	<p>Si se selecciona la casilla de verificación, el componente Protección frente a amenazas web no analiza el contenido de páginas o sitios web cuyas direcciones estén incluidas en la lista de direcciones web de confianza. Puede añadir a esta lista de direcciones web de confianza tanto direcciones específicas como máscaras de páginas o sitios web.</p>

## Protección frente a amenazas en el correo

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el [servicio en la nube Kaspersky Security Network](#) y el análisis heurístico.

Protección frente a amenazas en el correo puede analizar tanto los mensajes entrantes como los salientes. La aplicación es compatible con POP3, SMTP, IMAP y NNTP en los siguientes clientes de correo:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Microsoft Outlook Express
- Windows Mail

Protección frente a amenazas en el correo no es compatible con otros protocolos y clientes de correo.

Es posible que Protección frente a amenazas en el correo no siempre pueda obtener acceso de *nivel de protocolo* a los mensajes (por ejemplo, al usar la solución Microsoft Exchange). Por este motivo, Protección frente a amenazas en el correo incluye una [extensión para Microsoft Office Outlook](#). La extensión permite analizar mensajes en el *nivel del cliente de correo*. La extensión Protección frente a amenazas en el correo es compatible con operaciones con Outlook 2010, 2013, 2016 y 2019.

El componente Protección frente a amenazas en el correo no analiza los mensajes si el programa de correo se abre en un navegador.

Cuando se detecta un archivo malicioso en un adjunto, Kaspersky Endpoint Security modifica el nombre del asunto del mensaje a: [El mensaje necesita su participación en el procesamiento] <asunto del mensaje> o [Se ha procesado el mensaje] <asunto del mensaje>.

Configuración del componente Protección frente a amenazas en el correo

Parámetro	Descripción
<b>Nivel de seguridad</b> (disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)	<p>Para Protección frente a amenazas en el correo, Kaspersky Endpoint Security aplica diferentes grupos de ajustes. Estos grupos de parámetros guardados en la aplicación se denominan <i>niveles de seguridad</i>.</p> <ul style="list-style-type: none"><li>• <b>Alta.</b> Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo analiza los mensajes más exhaustivamente. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico avanzado. El nivel de seguridad de correo Máximo se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo electrónico gratuito desde una red doméstica sin protección centralizada del correo electrónico.</li><li>• <b>Recomendado.</b> El nivel de seguridad de correo electrónico que proporciona el equilibrio perfecto entre el rendimiento de Kaspersky Endpoint Security y la seguridad del correo electrónico. El componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico entrantes y salientes, y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico de correo.</li><li>• <b>Baja.</b> Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección frente a amenazas en el correo solamente analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza archivos adjuntos en mensajes de correo electrónico. Con este nivel de seguridad, el componente Protección frente a amenazas en el correo analiza los mensajes de correo electrónico a una velocidad máxima y con un uso mínimo de recursos del sistema operativo. Se recomienda el nivel de seguridad de correo Mínimo para su uso en un</li></ul>

	entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una LAN empresarial con protección centralizada del correo electrónico.
<b>Acción al detectar una amenaza</b>	<p><b>Desinfectar; eliminar si la desinfección falla.</b> Cuando se detecta un objeto infectado en un mensaje entrante o saliente, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security eliminará el objeto infectado. Kaspersky Endpoint Security añade información sobre la acción realizada al asunto del mensaje: [Se ha procesado el mensaje] &lt;asunto del mensaje&gt;.</p> <p><b>Desinfectar; bloquear si la desinfección falla.</b> Cuando se detecta un objeto infectado en un mensaje entrante, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario podrá acceder al mensaje con un archivo adjunto seguro. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security añade una advertencia al asunto del mensaje: [El mensaje necesita su participación en el procesamiento] &lt;asunto del mensaje&gt;. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta un objeto infectado en un mensaje saliente, Kaspersky Endpoint Security intenta desinfectar el objeto. Si el objeto no se puede desinfectar, Kaspersky Endpoint Security bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.</p> <p><b>Bloquear.</b> Si se detecta un objeto infectado en un mensaje entrante, Kaspersky Endpoint Security añade una advertencia al asunto del mensaje: [El mensaje necesita su participación en el procesamiento] &lt;asunto del mensaje&gt;. El usuario podrá acceder al mensaje con el archivo adjunto original. Si se detecta un objeto infectado en un mensaje saliente, Kaspersky Endpoint Security bloqueará la transmisión del mensaje y el cliente de correo mostrará un error.</p>
<b>Cobertura de protección</b> <i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i>	<p>La <i>Cobertura de protección</i> incluye objetos que el componente comprueba cuando se ejecuta: Mensajes entrantes y salientes o Solo mensajes entrantes.</p> <p>Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar que los archivos infectados se envíen en archivos. También puede activar el análisis de mensajes salientes si desea evitar que se envíen archivos en formatos particulares, como archivos de audio y vídeo, por ejemplo.</p>
<b>Analizar tráfico POP3, SMTP, NNTP e IMAP</b>	La casilla de verificación activa o desactiva el análisis que realiza el componente Protección frente a amenazas en el correo del tráfico que se transfiere mediante los protocolos POP3, SMTP, NNTP e IMAP.
<b>Conectar el complemento de Microsoft Outlook</b>	<p>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.</p> <p>Si el correo se analiza usando la extensión para Microsoft Outlook, se recomienda usar el modo caché de Exchange. Para información más detallada sobre el Modo caché de Exchange y recomendaciones sobre su uso, consulte la <a href="#">Base de conocimientos de Microsoft</a>.</p>
<b>Análisis heurístico</b>	La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.

<p><i>(disponible solo en la Consola de administración (MMC) y en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>Cuando analiza archivos en busca de código malicioso, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. El número de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para este. El nivel de análisis heurístico garantiza un equilibrio entre la exhaustividad de la búsqueda de nuevas amenazas, la carga en los recursos del sistema operativo y la duración del análisis heurístico.</p>
<p><b>Analizar archivos adjuntos</b></p>	<p>Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo.</p> <div data-bbox="376 517 1493 815" style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Si durante el análisis, Kaspersky Endpoint Security detecta la contraseña de un archivo comprimido en el cuerpo del mensaje, la utilizará para buscar aplicaciones maliciosas en el contenido del archivo. En este caso, la contraseña no se guardará. Un archivo de descomprime durante el análisis. Si ocurre un error con la aplicación durante el proceso de descomprimir, puede eliminar manualmente los archivos descomprimidos que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tendrán el prefijo PR.</p> </div>
<p><b>Analizar archivos adjuntos con formatos de Microsoft Office</b></p>	<p>Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.</p>
<p><b>No analizar archivos comprimidos de más de N MB</b></p>	<p>Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en el correo excluye del análisis los archivos adjuntos de los mensajes de correo electrónico si su tamaño supera el valor especificado. Si se desactiva la casilla de verificación, el componente Protección frente a amenazas en el correo analiza archivos adjuntos de cualquier tamaño.</p>
<p><b>No comprobar archivos durante más de N seg</b></p>	<p>Si se selecciona la casilla de verificación, el tiempo asignado para analizar los archivos adjuntos a los mensajes de correo electrónico se limita al período especificado.</p>
<p><b>Filtrado de adjuntos</b></p>	<div data-bbox="376 1541 1493 1630" style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>El filtrado de adjuntos no se aplica a los mensajes de correo electrónico salientes.</p> </div> <p><b>Desactivar el filtrado.</b> Si se selecciona esta opción, el componente Protección frente a amenazas en el correo no filtra archivos que están adjuntos a mensajes de correo electrónico.</p> <p><b>Renombrar los adjuntos de los tipos seleccionados.</b> Si se selecciona esta opción, el componente Protección frente a amenazas en el correo cambia el último carácter de la extensión en archivos adjuntos de los tipos especificados con el símbolo de barra baja (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.</p> <p><b>Eliminar los adjuntos de los tipos seleccionados.</b> Si se selecciona esta opción, el componente Protección frente a amenazas en el correo elimina los archivos adjuntos de los tipos especificados.</p>



Puede especificar los tipos de archivos adjuntos para eliminar de los mensajes de correo electrónico en la lista de máscaras de archivos.

## Protección frente a amenazas en la red

El componente Protección frente a amenazas en la red analiza el tráfico de red entrante en busca de actividad habitual en los ataques de red. Cuando Kaspersky Endpoint Security detecta un intento de ataque de red en el equipo del usuario, bloquea la conexión de red con el equipo atacante. Las bases de datos de Kaspersky Endpoint Security ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos. La lista de ataques de red que detecta el componente Protección frente a amenazas en la red se actualiza durante [las actualizaciones de módulos de aplicaciones y bases de datos](#).

Configuración del componente Protección frente a amenazas en la red

Parámetro	Descripción
<b>Tratar el análisis de puerto y el desbordamiento de red como ataques</b>	<p><i>Inundación de red</i> es un ataque a los recursos de red de una organización (como servidores web). Este ataque consiste en enviar una gran cantidad de solicitudes para sobrecargar el ancho de banda de los recursos de la red. Cuando esto sucede, los usuarios no pueden acceder a los recursos de red de la organización.</p> <p>Un ataque de tipo "Port scan" consiste en el análisis de puertos UDP, TCP, puertos y servicios de red en el equipo. Este ataque permite al atacante identificar el grado de vulnerabilidad del equipo antes de realizar tipos de ataques de red más peligrosos. Los ataques de tipo "Port scan" también permiten al atacante identificar el sistema operativo en el equipo y seleccionar los ataques de red apropiados para este sistema operativo.</p> <p>Cuando esta casilla está activada, Kaspersky Endpoint Security supervisa el tráfico de red para detectar estos ataques. Si se detecta un ataque, la aplicación notifica al usuario y envía el evento correspondiente a Kaspersky Security Center. La aplicación proporciona información sobre el equipo atacante, que es necesaria para emprender acciones de respuesta frente a amenazas.</p> <p>Puede activar la detección de este tipo de ataques en caso de que algunas de sus aplicaciones permitidas realicen operaciones típicas de este tipo de ataques. Esto ayudará a evitar falsas alarmas.</p>
<b>Añadir un equipo atacante a la lista de equipos bloqueados durante N min</b>	<p>Si se selecciona la casilla de verificación, el componente Protección frente a amenazas en la red añade al equipo atacante a la lista de bloqueados. Esto quiere decir que el componente Protección frente a amenazas en la red bloquea la conexión de red del equipo atacante después del primer intento de ataque de red durante el período de tiempo especificado. Este bloqueo protege automáticamente al equipo del usuario frente a posibles ataques de red desde la misma dirección en el futuro. El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 32 768 minutos.</p> <p>Puede ver la lista de rechazados en la ventana de la <a href="#">herramienta Monitor de red</a>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>Kaspersky Endpoint Security borra la lista de rechazados al reiniciar la aplicación y cuando se cambian los ajustes de Protección frente a amenazas en la red.</p></div>
<b>Exclusiones</b>	<p>La lista contiene direcciones IP para las que Protección frente a amenazas en la red no bloquea los ataques de la red.</p> <p>La aplicación no registra ningún dato sobre los ataques de red provenientes de las direcciones IP de la lista de exclusiones.</p>

## Protección contra spoofing de MAC

Los *ataques de spoofing de MAC* consisten en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Como resultado, un atacante puede redirigir los datos enviados a un dispositivo a otro dispositivo y obtener acceso a esos datos. Kaspersky Endpoint Security le permite saber si se detecta uno de ataques MAC Spoofing y bloquearlo.

## Firewall

Firewall bloquea las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local. Firewall también controla la actividad de red de las aplicaciones en el equipo. Esto le permite proteger su red de área local corporativa del robo de identidad y otros ataques. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus, el servicio en la nube Kaspersky Security Network y *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. De forma automática, el firewall crea las reglas de red necesarias para que funcionen la aplicación y el Agente de red. Como resultado, el firewall abre varios puertos en el ordenador. Los puertos se abren según la función del ordenador (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en el ordenador, consulte la [Ayuda de Kaspersky Security Center](#).

## Reglas de red

Puede configurar las reglas de la red en los siguientes niveles:

- *Reglas de paquetes de red.* Las reglas de paquetes de red imponen restricciones a los paquetes de red, con independencia de la aplicación. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security tiene reglas de paquetes de red predefinidas con permisos recomendados por los expertos de Kaspersky.
- *Reglas de red de la aplicación.* Las reglas de red de la aplicación imponen restricciones sobre la actividad de red de una aplicación concreta. No solo influyen en las características del paquete de red, sino también en la aplicación concreta a la que va dirigida la aplicación concreta o que emitió este paquete de red.

El componente [Prevención de intrusiones en el host](#) proporciona el acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de *derechos de aplicación*.

Durante el primer inicio de la aplicación, Firewall realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.  
Se le recomienda [participar en Kaspersky Security Network](#) para ayudar a Firewall a trabajar con más eficacia.
3. Coloca la aplicación en uno de los *grupos de confianza*: De confianza/Restricción mínima/Restricción máxima/No confiable.

Los [grupos de confianza definen los derechos](#) que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la [configuración del componente Prevención de intrusiones en el host](#). Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea la actividad de red de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega el uso de cualquier conexión de red.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

## Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más alta sea la posición de una regla en la lista, mayor prioridad tendrá. Si se añade actividad de red a varias reglas, Firewall regula la actividad de red en función de la regla con la prioridad más alta.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si tanto las reglas de paquetes de red como las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se gestiona de acuerdo con las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan de la siguiente manera: una regla de red para aplicaciones incluye reglas de acceso basadas en el estado de la red: *publica*, *local* o *de confianza*. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega cualquier actividad de red en redes de cualquier estado de forma predeterminada. Si se especifica una regla de red para una aplicación individual (aplicación principal), los subprocesos de otras aplicaciones se ejecutarán de acuerdo con la regla de red de la aplicación principal. Si no hay una regla de red para la aplicación, los subprocesos se ejecutarán de acuerdo con la regla de acceso a la red del grupo de confianza de la aplicación.

Por ejemplo, ha prohibido cualquier actividad de red en redes de todos los estados para todas las aplicaciones, excepto el navegador X. Si inicia la instalación del navegador Y (subproceso) desde el navegador X (aplicación principal), el instalador del navegador Y accederá a la red y descargará los archivos necesarios. Después de la instalación, se negarán las conexiones de red al navegador Y de acuerdo con la configuración del Firewall. Para prohibir la actividad de red del instalador del navegador Y como un subproceso, debe asignar una regla de red para el instalador del navegador Y.

## Estados de conexión de red

Firewall le permite controlar la actividad de la red en función del estado de la conexión de red. Kaspersky Endpoint Security recibe el estado de conexión de red del sistema operativo del equipo. El estado de la conexión de red en el sistema operativo lo establece el usuario al configurar la conexión. Puede [cambiar el estado de la conexión de red en la configuración de Kaspersky Endpoint Security](#). Firewall supervisará la actividad de la red en función del estado de la red en la configuración de Kaspersky Endpoint Security, y no en del sistema operativo.

La conexión de red puede tener uno de los siguientes tipos de estado:

- **Red pública.** La red no está protegida por aplicaciones antivirus, firewalls ni filtros (como la red wifi de una cafetería). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos mediante carpetas compartidas y acceso remoto al escritorio de este equipo. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.

Firewall asigna el estado *Red pública* a Internet de forma predeterminada. No se puede cambiar el estado de Internet.

- **Red local.** Red para usuarios con acceso restringido a archivos e impresoras en este equipo (como una red de área local corporativa o red doméstica).
- **Red de confianza.** Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.

Configuración del componente Firewall

Parámetro	Descripción
<b>Reglas de paquetes de red</b>	<p>Tabla con una lista de reglas de paquetes de red. Las reglas de paquetes de red sirven para imponer restricciones a los paquetes de red, con independencia de la aplicación. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado.</p> <p>La tabla enumera las reglas de paquetes de red preconfiguradas que recomienda Kaspersky para una protección óptima del tráfico de red de equipos que se ejecutan con los sistemas operativos Microsoft Windows.</p> <p>Firewall establece la prioridad de cada regla de paquetes de red. Firewall procesa las reglas de paquetes de red en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba abajo. Cuando se detecta una conexión de red, Firewall busca la primera regla de paquetes pertinente y la aplica a la actividad de red, que se permitirá o bloqueará según corresponda. Las reglas posteriores que también sean aplicables a la conexión de red se desestimarán.</p> <p>Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones.</p>
<b>Conexiones de red</b>	<p>Esta tabla contiene información sobre las conexiones de red que Firewall detecta en el equipo.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>El estado <i>Red pública</i> se asigna a Internet de forma predeterminada. No se puede cambiar el estado de Internet.</p> </div>
<b>Reglas de red</b>	<p><b>Aplicaciones</b></p> <p>Tabla de aplicaciones que controla el componente Firewall. Las aplicaciones se asignan a grupos de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security usa al controlar la actividad de red de las aplicaciones.</p> <p>Puede seleccionar una aplicación de una lista única de todas las aplicaciones instaladas en equipos bajo la influencia de una directiva y añadir la aplicación a un grupo de confianza.</p> <p><b>Reglas de red</b></p> <p>Tabla de reglas de red para aplicaciones que forman parte de un grupo de confianza. De acuerdo con estas reglas, Firewall regula la actividad de red de aplicaciones.</p> <p>La tabla muestra las reglas de red predefinidas que recomiendan los expertos de Kaspersky. Estas reglas de red se han añadido para proteger de manera óptima el tráfico de red de los equipos que ejecutan sistemas operativos Windows. No se puede eliminar las reglas de red predefinidas.</p>

## Prevención de ataques de BadUSB

Algunos virus modifican el firmware de los dispositivos USB para engañar al sistema operativo y que detecte el dispositivo USB y lo identifique como teclado. Como resultado, el virus puede ejecutar comandos en su cuenta de usuario para descargar software malicioso, por ejemplo.

El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.

Cuando un dispositivo USB se conecta al equipo y el sistema operativo lo identifica como un teclado, la aplicación solicita al usuario que introduzca desde este teclado un código numérico generado por la aplicación, o bien que utilice el [teclado en pantalla si está disponible](#) (vea la figura a continuación). Este procedimiento se conoce como autorización del teclado.

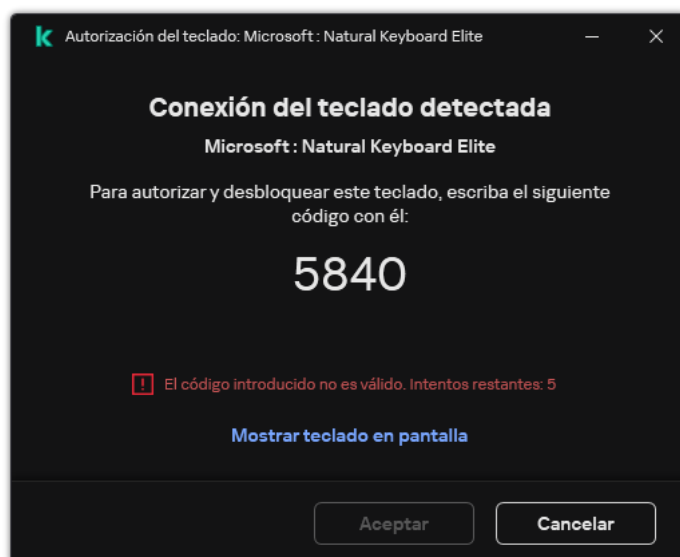
Si se ha introducido el código correctamente, la aplicación guarda los parámetros de identificación (los VID y PID del teclado y el número del puerto al cual se ha conectado) en la lista de teclados autorizados. No será necesario volver a realizar la autorización del teclado cuando se vuelva a conectar el teclado o después de que se reinicie el sistema operativo.

Si el teclado autorizado se conecta al equipo a través de un puerto USB diferente, la aplicación volverá a mostrar la solicitud de autorización.

Si se introduce el código numérico de forma incorrecta, la aplicación generará un nuevo código. Puede [configurar el número de intentos para introducir el código numérico](#). Si el código numérico se introduce de forma incorrecta muchas veces o si se cierra la ventana de autorización del teclado (ver la figura a continuación), la aplicación bloquea las acciones de ese teclado. Cuando se cumple el período de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación solicita al usuario que realice de nuevo el procedimiento de autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea los teclados que no se hayan autorizado.

El componente Prevención de ataques de BadUSB no se instala de forma predeterminada. Si necesita el componente Prevención de ataques de BadUSB, puede añadir el componente a las propiedades del [paquete de instalación](#) antes de instalar la aplicación o [cambiar sus componentes disponibles](#) después de instalarla.



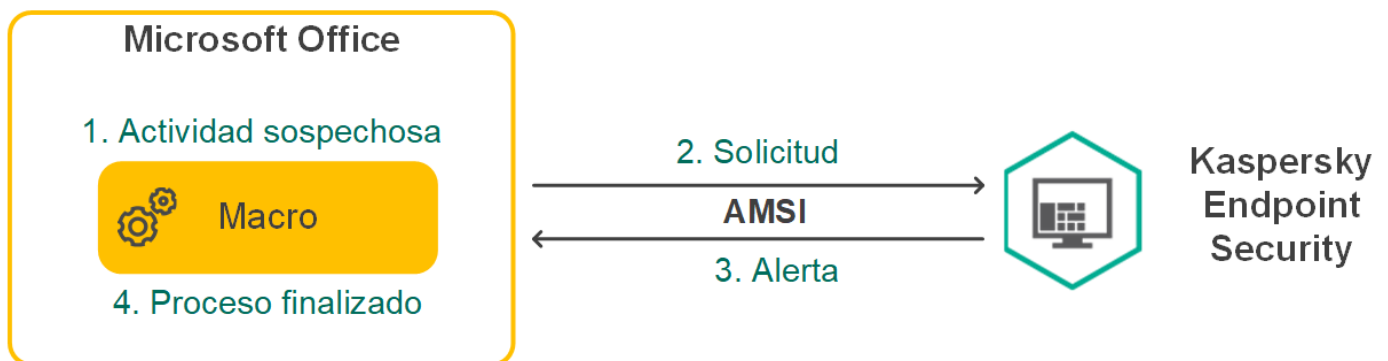
Configuración del componente Prevención de ataques de BadUSB

Parámetro	Descripción
<b>Prohibir el uso del teclado en pantalla para la autorización de dispositivos USB</b>	Si se selecciona, la aplicación bloquea el uso del teclado en pantalla para autorizar el dispositivo USB con el que no se puede introducir un código de autorización.
<b>Número máximo de intentos de autorización del dispositivo</b>	Bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite 5 intentos para introducir el código de autorización, el dispositivo USB se bloquea después del quinto intento fallido. Kaspersky Endpoint Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este período, puede tener 5 intentos para introducir el código de autorización.
<b>Tiempo de espera al alcanzar el número máximo de intentos</b>	Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos para introducir el código de autorización. Los valores válidos son de 1 a 180 (minutos).

## Protección AMSI

El componente de protección AMSI está diseñado para ser compatible con 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 más detalles sobre AMSI, consulte la [documentación de Microsoft](#).

La protección AMSI únicamente puede detectar una amenaza y notificar a una aplicación de terceros sobre dicha amenaza detectada. La aplicación de terceros, después de recibir una notificación de una amenaza, no permite realizar acciones maliciosas (por ejemplo, finaliza su proceso).



Ejemplo del funcionamiento de AMSI

El componente de protección AMSI puede rechazar una solicitud de una aplicación de terceros si, por ejemplo, esta aplicación sobrepasa el número máximo de solicitudes dentro de un intervalo específico. Cuando esto ocurre, Kaspersky Endpoint Security envía información al respecto al Servidor de administración. El componente Protección AMSI no rechaza las solicitudes de aquellas aplicaciones de terceros para las cuales la [integración continua con el componente de protección AMSI](#) está activada.

La protección AMSI está disponible para los siguientes sistemas operativos para estaciones de trabajo y servidores:

- Windows 10 Home/Pro/Pro for Workstations/Education/Enterprise;
- Windows 11;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter;
- Windows Server 2022.

#### Configuración de Protección AMSI

Parámetro	Descripción
<b>Analizar archivos</b>	Analizar archivos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros formatos de archivo.
<b>Analizar paquetes de distribución</b>	Use esta casilla para activar o desactivar el análisis de paquetes de distribución de terceros.
<b>Analizar archivos en formatos de Microsoft Office</b>	Analizar archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los archivos con formato de Office también incluyen objetos OLE.
<b>No descomprimir archivos compuestos de gran tamaño</b>	Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security no escanea archivos compuestos cuyo tamaño exceda el valor especificado.  Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.  Kaspersky Endpoint Security analiza archivos grandes que se extraen de archivos independientemente de si la casilla de verificación está marcada o no.

## Prevención de exploits

El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malicioso. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

#### Configuración del componente Prevención de exploits

Parámetro	Descripción

<b>Al detectar vulnerabilidades</b>	<p><b>Bloquear operación.</b> Si este elemento está seleccionado, al detectar una vulnerabilidad de seguridad, Kaspersky Endpoint Security bloquea el funcionamiento de la vulnerabilidad y crea una entrada de registro con información relevante.</p> <p><b>Notificar.</b> Si este elemento está seleccionado, cuando Kaspersky Endpoint Security detecte una vulnerabilidad registrará un evento que contenga información sobre la vulnerabilidad y añadirá información sobre esta vulnerabilidad a <a href="#">la lista de amenazas activas</a>.</p>
<b>Activar protección de la memoria de los procesos del sistema</b>	<p>Si se activa este interruptor, Kaspersky Endpoint Security bloquea los procesos externos que intentan acceder a la memoria de los procesos del sistema.</p>

## Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones de su equipo y ofrece esta información a otros componentes de protección mejorar su rendimiento. El componente Detección de comportamientos utiliza firmas de patrones de actividad peligrosa (Behavior stream signatures, BSS) para aplicaciones. Si la actividad de la aplicación coincide con una BSS Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security basada en bases de datos de reglas heurísticas ofrece protección proactiva al equipo.

Parámetros del componente Detección de comportamientos

Parámetro	Descripción
<b>Al detectar actividad de software malicioso</b>	<ul style="list-style-type: none"> <li>• <b>Eliminar el archivo.</b> Seleccione este elemento para que, cuando se detecte actividad maliciosa, Kaspersky Endpoint Security elimine el archivo ejecutable de la aplicación maliciosa y cree una copia de seguridad del archivo en Copias de seguridad.</li> <li>• <b>Finalizar la aplicación.</b> Seleccione este elemento para que, cuando se detecte actividad maliciosa, Kaspersky Endpoint Security finalice la aplicación.</li> <li>• <b>Notificar.</b> Seleccione este elemento para que, si se detecta actividad maliciosa de parte de una aplicación, Kaspersky Endpoint Security no finalice la aplicación, sino que añada información sobre esta actividad maliciosa a la lista de amenazas activas.</li> </ul>
<b>Activar protección de carpetas compartidas frente a cifrado externo</b>	<p>Si se activa el interruptor, Kaspersky Endpoint Security analiza la actividad de las carpetas compartidas. Si esta actividad coincide con un tipo de comportamiento típico del cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.</p> <div data-bbox="359 1691 1497 1816" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security impide el cifrado externo solo de los archivos ubicados en unidades con el sistema de archivos NTFS y no cifrados por el sistema EFS.</p> </div> <ul style="list-style-type: none"> <li>• <b>Notificar.</b> Si selecciona este elemento, cuando se detecte un intento de modificar los archivos de una carpeta compartida, Kaspersky Endpoint Security añadirá información sobre el hecho a la lista de amenazas activas.</li> <li>• <b>Bloquear conexión durante N min.</b> Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un intento de modificar archivos en carpetas compartidas, bloquea la actividad de red del equipo que intenta modificar los archivos y crea copias de seguridad de los archivos modificados.</li> </ul>



	<p>Si el componente Motor de reparación está activado y la opción <b>Bloquear conexión durante N minutos</b> está seleccionada, se restauran los archivos modificados a partir de las copias de seguridad.</p>
<b>Exclusiones</b>	<p>Lista de equipos cuyos intentos de cifrar carpetas compartidas no se supervisarán.</p> <p>Para aplicar la lista de equipos excluidos de la protección de carpetas compartidas contra el cifrado externo, deberá activar la opción "Auditar inicio de sesión" en la directiva de auditoría de seguridad de Windows. De manera predeterminada, la opción "Auditar inicio de sesión" no está activada. Para obtener más información sobre la directiva de auditoría de seguridad de Windows, visite el <a href="#">sitio web de Microsoft</a>.</p>

## Prevención de intrusiones en el host

El componente Prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. El componente proporciona protección del equipo con la ayuda de bases de datos antivirus y el servicio en la nube Kaspersky Security Network.

El componente controla el funcionamiento de las aplicaciones mediante el uso de *derechos de las aplicaciones*. Los derechos de las aplicaciones incluyen los siguientes parámetros de acceso:

- Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro)
- Acceso a datos personales (como archivos y aplicaciones)

La actividad de red de las aplicaciones está controlada por el [Firewall](#) utilizando las *reglas de red*.

Durante el primer inicio de la aplicación, el componente Prevención de intrusiones en el host realiza las siguientes acciones:

1. Comprueba la seguridad de la aplicación utilizando las bases de datos antivirus descargadas.
2. Comprueba la seguridad de la aplicación en Kaspersky Security Network.

Se le recomienda [participar en Kaspersky Security Network](#) para ayudar al componente Prevención de intrusiones en el host a trabajar con más eficacia.

3. Coloca la aplicación en uno de los *grupos de confianza*: De confianza/Restricción mínima/Restricción máxima/No confiable.

Los [grupos de confianza definen los derechos](#) que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza para los componentes Firewall y Prevención de intrusiones en el host. No puede cambiar el grupo de confianza solo para Firewall o para Prevención de intrusiones en el host.

Si se negó a participar en KSN o no hay red, Kaspersky Endpoint Security coloca la aplicación en un grupo de confianza en función de la [configuración del componente Prevención de intrusiones en el host](#). Tras recibir la reputación de la aplicación de KSN, el grupo de confianza se puede cambiar automáticamente.

4. Bloquea las acciones de las aplicaciones según el grupo de confianza. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega el acceso a los módulos del sistema operativo.

La próxima vez que se inicie la aplicación, Kaspersky Endpoint Security comprobará la integridad de la aplicación. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si se ha modificado la aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.

Configuración del componente Prevención de intrusiones en el host

Parámetro	Descripción
Derechos de la aplicación	<p><b>Aplicaciones</b></p> <p>Tabla de aplicaciones que supervisa el componente Prevención de intrusiones en el host. Las aplicaciones se asignan a grupos de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones.</p> <p>Puede seleccionar una aplicación de una lista única de todas las aplicaciones instaladas en equipos bajo la influencia de una directiva y añadir la aplicación a un grupo de confianza.</p> <p>Los derechos de acceso a la aplicación se muestran en las siguientes tablas:</p> <ul style="list-style-type: none"><li>• <b>Archivos y Registro del sistema.</b> Esta tabla contiene los derechos que rigen el acceso de las aplicaciones de un grupo de confianza a los recursos del sistema operativo y a los datos personales.</li><li>• <b>Permisos.</b> Esta tabla contiene los derechos que rigen el acceso de las aplicaciones de un grupo de confianza a los procesos y recursos del sistema operativo.</li><li>• <b>Reglas de red.</b> Tabla de reglas de red para aplicaciones que forman parte de un grupo de confianza. De acuerdo con estas reglas, <a href="#">Firewall</a> regula la actividad de red de aplicaciones. La tabla muestra las reglas de red predefinidas que recomiendan los expertos de Kaspersky. Estas reglas de red se han añadido para proteger de manera óptima el tráfico de red de los equipos que ejecutan sistemas operativos Windows. No se puede eliminar las reglas de red predefinidas.</li></ul>
Recursos protegidos	<p><b>Nombre</b></p> <p>La tabla contiene los recursos del equipo clasificados. El componente Prevención de intrusiones en el host supervisa los intentos de otras aplicaciones para acceder a recursos de la tabla.</p> <p>Un recurso puede ser una categoría de registro, archivo, carpeta o clave de registro.</p> <p><b>Aplicaciones</b></p>

	<p>Tabla de aplicaciones que supervisa el componente Prevención de intrusiones en el host para el recurso seleccionado. Las aplicaciones se asignan a grupos de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones.</p>
<p><b>Grupo de confianza para aplicaciones que se lancen antes que Kaspersky Endpoint Security para Windows comience a funcionar</b></p>	<p>Un grupo de confianza en el que se ubicarán las aplicaciones que se inicien antes que Kaspersky Endpoint Security.</p>
<p><b>Actualizar derechos para aplicaciones anteriormente desconocidas usando la base de datos de KSN</b></p>	<p>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.</p>
<p><b>Confiar en aplicaciones firmadas digitalmente</b></p>	<p>Si se selecciona esta casilla de verificación, el componente Prevención de intrusiones en el host ubica las aplicaciones con la firma digital de los proveedores de confianza en el Grupo de confianza.</p> <p><i>Los proveedores de confianza son proveedores de software en los que confía Kaspersky. También puede <a href="#">añadir un certificado de proveedor al almacén de certificados de confianza de forma manual</a>.</i></p> <p>Si se desactiva esta casilla de verificación, el componente Prevención de intrusiones en el host no considera estas aplicaciones como de confianza y utiliza otros ajustes para determinar su grupo de confianza.</p>
<p><b>Elimina las reglas de aplicaciones que no se hayan iniciado durante más de (1 a 90 días)</b></p>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security elimina automáticamente información sobre la aplicación (grupo de confianza y derechos de acceso) si se cumplen las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>• Si coloca manualmente la aplicación en un grupo de confianza o configura sus derechos de acceso.</li> <li>• La aplicación no se ha iniciado durante el período de tiempo definido.</li> </ul> <p>Si el grupo de confianza y los derechos de una aplicación se han determinado automáticamente, Kaspersky Endpoint Security elimina la información sobre esta aplicación después de 30 días. No es posible cambiar el período de almacenamiento para la información de las aplicaciones ni desactivar la eliminación automática.</p> <p>La próxima vez que inicie esta aplicación, Kaspersky Endpoint Security vuelve a analizarla como si fuese la primera vez que se inicia.</p>
<p><b>Grupo de confianza para aplicaciones que no se pudieron añadir a grupos existentes</b></p>	<p>Los elementos en esta lista desplegable determinan a qué grupo de confianza Kaspersky Endpoint Security asignará una aplicación desconocida.</p> <p>Puede elegir uno de los siguientes elementos:</p> <ul style="list-style-type: none"> <li>• <b>Restricción mínima.</b></li> <li>• <b>Restricción máxima.</b></li> <li>• <b>No confiable.</b></li> </ul>

## Motor de reparación

El Motor de reparación permite a Kaspersky Endpoint Security anular acciones que han sido realizadas por el malware en el sistema operativo.

Al anular la actividad de malware en el sistema operativo, Kaspersky Endpoint Security tramita los siguientes tipos de actividad de malware:

- **Actividad de archivos**

Kaspersky Endpoint Security realiza las siguientes acciones:

- Elimina 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 modificado o eliminado.

- **Actividad del sistema**

Kaspersky Endpoint Security realiza las siguientes acciones:

- Finaliza los procesos iniciados por el malware.
- Finaliza los procesos en los que haya penetrado una aplicación maliciosa.
- No reanuda procesos que el malware haya suspendido.

- **Actividad de red**

Kaspersky Endpoint Security realiza las siguientes acciones:

- Bloquea la actividad de red del malware.
- Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.

La reversión de acciones puede iniciarse durante un [análisis antivirus](#) o a pedido de los componentes [Protección contra archivos peligrosos](#) y [Detección de comportamientos](#).

Deshacer las operaciones de un software malicioso (malware) afecta a un conjunto de datos definidos rigurosamente. La anulación no tiene efectos adversos en el sistema operativo ni en la integridad de los datos del equipo.

A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

*Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security podrá utilizar los servicios de KSN para conocer la categoría y la reputación de los archivos analizados u obtener información sobre la reputación de las direcciones web que se analicen.

El uso de Kaspersky Security Network es voluntario. La aplicación le invita a usar en KSN durante la configuración inicial de la aplicación. Los usuarios podrán reanudar o interrumpir su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el [sitio web de Kaspersky](#) contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. El archivo ksn\_<identificador del idioma>.txt, que forma parte del [kit de distribución](#) de la aplicación, contiene el texto de la Declaración de Kaspersky Security Network.

Para reducir la carga de los servidores de KSN, los expertos de Kaspersky pueden publicar actualizaciones para la aplicación que impidan temporalmente o restrinjan parcialmente la capacidad de enviar solicitudes a Kaspersky Security Network. Bajo estas condiciones, el estado de conexión a KSN cambia a *Habilitado con restricciones* en la interfaz local de la aplicación.

## Infraestructura de KSN

Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura de KSN:

- *KSN Global*. Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky Security Network y, a su vez, envían a Kaspersky información sobre los objetos que se detectan en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos de Kaspersky Security Network.
- *KSN privada*. Esta es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky obtener acceso a bases de datos de reputación de Kaspersky Security Network y a otros datos estadísticos sin enviar datos a KSN desde sus propios equipos. KSN Privada se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:
  - porque las estaciones de trabajo locales no tienen acceso a Internet;
  - porque, por motivos legales o debido a las políticas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

De forma predeterminada, Kaspersky Security Center usa KSN Global. Puede configurar el uso de KSN privada en la Consola de administración (MMC), en Kaspersky Security Center Web Console y en la [línea de comando](#). No se puede configurar el uso de KSN privada en Kaspersky Security Center Cloud Console.

Para más información sobre KSN Privada, consulte la documentación de Kaspersky Private Security Network.

## Proxy de KSN

Los equipos de los usuarios que gestionen el servidor de administración de Kaspersky Security Center pueden interactuar con KSN mediante el servicio de proxy de KSN.

El servicio de proxy de KSN ofrece las siguientes funcionalidades:

- El equipo del usuario puede consultar y enviar información a KSN, aunque no tenga acceso directo a Internet.
- El servicio 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.

Para obtener más información sobre el servicio Proxy de KSN, consulte la [Ayuda de Kaspersky Security Center](#).

### Parámetros de Kaspersky Security Network

Parámetro	Descripción
<b>Activar el modo ampliado de KSN</b>	<p>El <i>modo KSN ampliado</i> es un modo en el que Kaspersky Endpoint Security envía <a href="#">información adicional</a> a Kaspersky. Kaspersky Endpoint Security utiliza KSN para detectar amenazas independientemente de la posición del botón.</p>
<b>Activar modo nube</b>	<p><i>Modo nube</i> 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.</p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>Kaspersky Endpoint Security descarga la versión ligera de las bases de datos antivirus durante la siguiente actualización después de que se haya seleccionado la casilla.</p></div> <p>Si el interruptor está desactivado, Kaspersky Endpoint Security usa la versión completa de las bases de datos antivirus.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>Kaspersky Endpoint Security descarga la versión completa de las bases de datos antivirus durante la siguiente actualización después de que se haya desactivado la casilla.</p></div>
<b>Estado del equipo cuando los servidores de KSN no están disponibles</b>	<p>Los elementos de esta lista desplegable permiten indicar qué estado tendrá un equipo en Kaspersky Security Center cuando los servidores de KSN no estén disponibles.</p>

<p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	
<p><b>Usar Proxy de KSN</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>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.</p>
<p><b>Utilizar servidores de KSN cuando el proxy de KSN no esté disponible</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores KSN pueden ubicarse tanto en el lado de Kaspersky (cuando se utiliza KSN global) como en el lado de terceros (cuando se utiliza KSN privada).</p>

## Control Web

Control web permite regular el acceso de los usuarios a los recursos web. El componente ayuda a reducir tanto el volumen de tráfico como el tiempo que se malgasta en actividades no laborales. Cuando un usuario intenta abrir un sitio web que se ha restringido mediante Control web, Kaspersky Endpoint Security bloqueará el acceso o le mostrará una advertencia (vea la imagen más abajo).

Kaspersky Endpoint Security solo puede supervisar tráfico HTTP y HTTPS.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario [activar el análisis de conexiones cifradas](#).

## Métodos para regular el acceso a los sitios web

Control web permite configurar el acceso a los sitios web a través de estos criterios:

- **Categorías de sitios web.** Para categorizar los sitios web, la aplicación utiliza el servicio en la nube Kaspersky Security Network, el análisis heurístico y la base de datos de sitios web conocidos, que está incluida con las demás bases de datos de la aplicación. Por ejemplo, puede restringir el acceso de los usuarios a la categoría "Redes sociales" o a [otras categorías](#).

- **Tipo de datos.** Puede restringir el acceso 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 "Archivos de gráficos".

- **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 Office" solo para la categoría de sitios web "Correo electrónico basado en Web".

## Reglas de acceso a sitios web

Control web regula el acceso de los usuarios a los sitios web a través de *reglas de acceso*. Para cada una de estas reglas, puede configurar las siguientes opciones avanzadas:

- **Usuarios alcanzados por la regla.**  
Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.
- **Planificación de reglas.**  
Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

## Prioridad de las reglas de acceso

Cada regla tiene una prioridad. Cuanto más alta sea la posición de una regla en la lista, mayor prioridad tendrá. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web "Redes sociales" y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.





No se puede proporcionar la página web solicitada.

Dirección: <http://kaspersky.ru/>.

La regla kasp ha bloqueado la página web.

Razón: el recurso web pertenece a las categorías de contenido Sin determinar y a las categorías de tipos de datos Sin determinar.

Este recurso web está prohibido en la empresa. Si considera que el bloqueo es un error, o si necesita acceder a este recurso web, póngase en contacto con el administrador de la red corporativa local ([Solicitar acceso](#)).

Mensaje generado: 10/14/2020 4:05:34 AM



La página web solicitada puede no ser segura o estar prohibida por la directiva de la empresa.

Dirección: <http://kaspersky.ru/>.

La regla kasp ha bloqueado la página web.

Motivo: el recurso web pertenece a las categorías de contenido Sin determinar y a las categorías de tipo de datos Sin determinar.

Haga clic en el vínculo <http://kaspersky.ru/> para abrir la página web solicitada.

Haga clic en el vínculo [http://kaspersky.ru/\\*](http://kaspersky.ru/*) para obtener acceso a todo el contenido del sitio web en el que se encuentra la página web solicitada.

Haga clic en el vínculo [\\*/\\*.kaspersky.ru/\\*](*/*.kaspersky.ru/*) para obtener acceso a todos los dominios existentes de nivel inferior o igual al que está marcado con \\*\*\".

Se concederá acceso a los recursos web enumerados anteriormente en la sesión actual de la aplicación.

Si ha recibido esta advertencia por error, póngase en contacto con el administrador de la red corporativa local ([Solicitar acceso](#)).

Mensaje generado: 10/14/2020 4:06:16 AM

#### Mensajes de Control web

#### Configuración del componente Control web

Parámetro	Descripción
Reglas de acceso a recursos web	Lista con las reglas de acceso a recursos web. Cada regla tiene una prioridad. Cuanto más alta sea la posición de una regla en la lista, mayor prioridad tendrá. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han añadido a más de una regla.
Regla predeterminada	La <i>regla predeterminada</i> regula el acceso a los recursos web que no están contemplados en ninguna otra regla. Están disponibles las siguientes opciones: <ul style="list-style-type: none"> <li>• <b>Autorizar todo lo que no esté especificado en la lista de reglas</b>, también conocido como modo de lista de rechazados para sitios web prohibidos.</li> <li>• <b>Prohibir todo lo que no esté especificado en la lista de reglas</b>, también conocido como modo de lista de admitidos para sitios web permitidos.</li> </ul>
Plantillas de	

<p><b>mensajes</b></p>	<ul style="list-style-type: none"> <li>• <b>Advertencia.</b> El campo de entrada consta de una plantilla del mensaje que se muestra si se activa una regla de advertencia sobre intentos de acceso a un recurso web no deseado.</li> <li>• <b>Mensaje sobre el bloqueo.</b> El campo de entrada contiene la plantilla del mensaje que aparece si se activa una regla que bloquee el acceso a un recurso web.</li> <li>• <b>Mensaje al administrador.</b> La plantilla del mensaje que se enviará al administrador de la LAN si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: <b>Mensaje al administrador por bloqueo del acceso a la página web.</b> La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida <b>Solicitudes de usuarios.</b> 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.</li> </ul>
<p><b>Registrar el acceso a páginas permitidas</b></p>	<p>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 <a href="#">registro local de Kaspersky Endpoint Security</a> y al registro de eventos de Windows. Para supervisar las actividades de los usuarios en Internet, deberá <a href="#">configurar los ajustes de almacenamiento de eventos</a>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Si opta por supervisar las actividades en línea de los usuarios, la carga del equipo podría aumentar cuando se necesite descifrar tráfico HTTPS.</p> </div>

## Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi). Esto le permite proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos.

### Niveles de acceso a dispositivos

Control de dispositivos controla el acceso a los siguientes niveles:

- **Tipo de dispositivo.** Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

Puede configurar el acceso a los dispositivos del siguiente modo:

- Autorizar – ✓.
- Bloquear – ✗.
- Depende del bus de conexión (excepto para wifi) – 🌈.
- Bloquear con excepciones (solo wifi) – 📄.

- **Bus de conexión.** Un *bus de conexión* es una interfaz usada para conectar dispositivos al equipo (por ejemplo, USB o FireWire). Por lo tanto, puede restringir la conexión de todos los dispositivos, por ejemplo, vía USB.



Puede configurar el acceso a los dispositivos del siguiente modo:

- Autorizar – ✓.
  - Bloquear – ⓧ.
- **Dispositivos de confianza.** Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

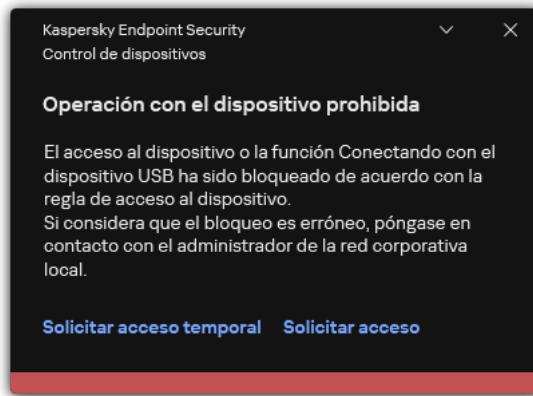
Puede añadir dispositivos de confianza según los siguientes datos:

- **Dispositivos por ID.** Cada dispositivo tiene un identificador exclusivo (ID de hardware o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. ID de dispositivo de ejemplo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.
- **Dispositivos por modelo.** Cada dispositivos tiene un ID de proveedor (VID) y un ID de producto (PID). Puede ver los ID en las propiedades del dispositivo usando herramientas del sistema operativo. Plantilla para introducir el VID y el PID: `VID_1234&PID_5678`. Añadir dispositivos por modelo es conveniente si utiliza dispositivos de un modelo concreto en su organización. De este modo, puede añadir todos los dispositivos de este modelo.
- **Dispositivos por máscara de ID.** Si utiliza varios dispositivos con ID similares, puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `WDC_C*`.
- **Dispositivos por máscara de modelo.** Si utiliza varios dispositivos con VID y PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza usando máscaras. El carácter `*` sustituye cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `VID_05AC & PID_*`.

Control de dispositivos regula el acceso de los usuarios a dispositivos usando [reglas de acceso](#). Control de dispositivos también le permite guardar eventos de conexión/desconexión de dispositivos. Para guardar eventos, tiene que configurar el registro de eventos en una directiva.

Cuando el acceso a un dispositivo dependa del bus de conexión (estado ) , Kaspersky Endpoint Security no guardará ningún evento relacionado con la conexión o desconexión del dispositivo. Para que Kaspersky Endpoint Security guarde eventos de conexión/desconexión, debe autorizar el acceso al tipo de dispositivo correspondiente (estado ) o añadir el dispositivo a la lista de dispositivos de confianza.

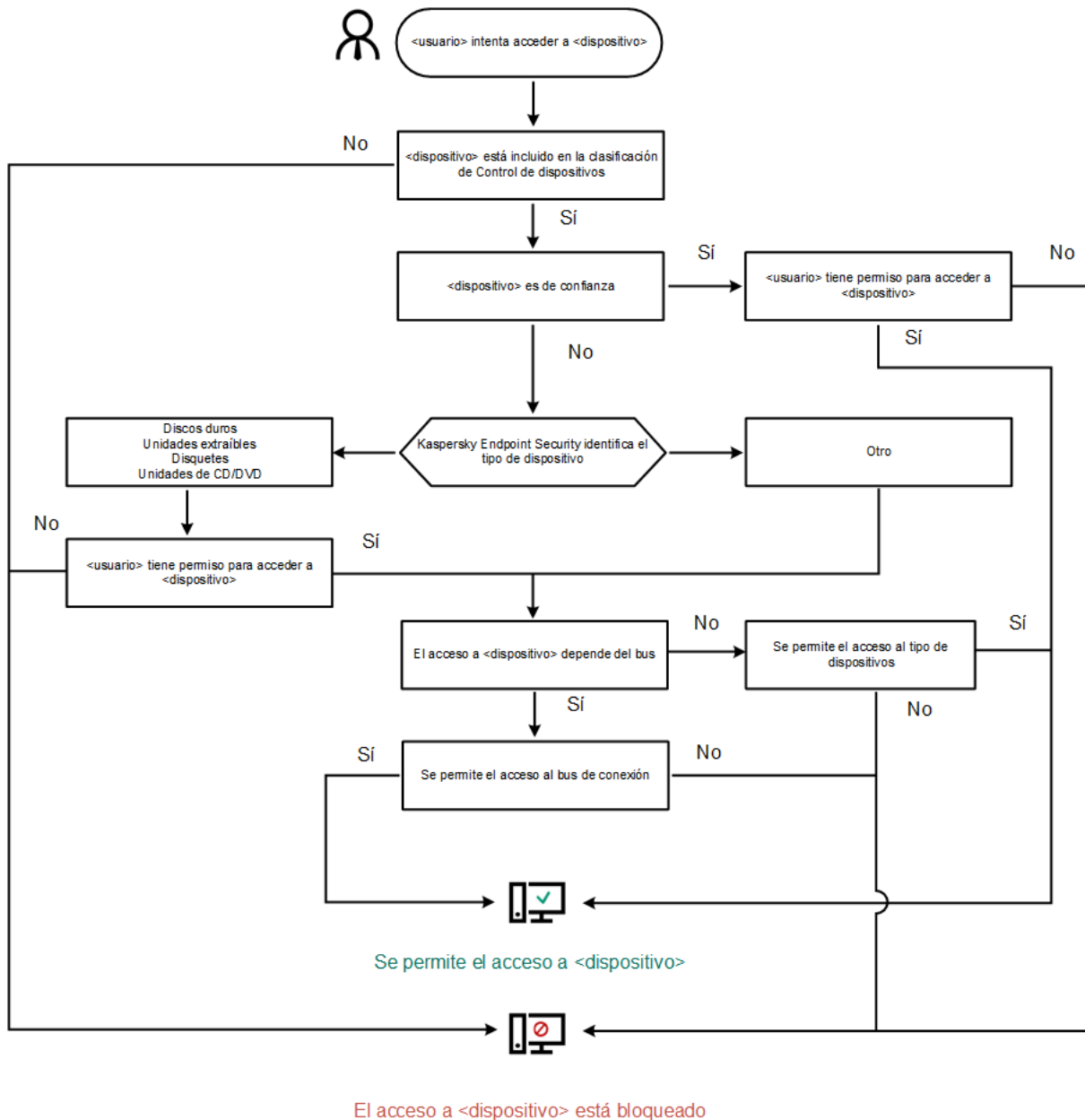
Cuando un dispositivo que está bloqueado por Control de dispositivos se conecte al equipo, Kaspersky Endpoint Security bloqueará el acceso y mostrará una notificación (véase la figura siguiente).



Notificación de Control de dispositivos

## Algoritmo de funcionamiento de Control de dispositivos

Kaspersky Endpoint Security toma una decisión sobre si permitir el acceso a un dispositivo después de que el usuario conecte un dispositivo al equipo de la siguiente imagen.



Algoritmo de funcionamiento de Control de dispositivos

Si conecta un dispositivo y se le permite acceder a él, puede editar la regla de acceso y bloquear la posibilidad de utilizarlo. Cuando alguien intente acceder al dispositivo nuevamente (por ejemplo, para ver la estructura de carpetas o para realizar una operación de lectura o escritura), Kaspersky Endpoint Security bloqueará el acceso. Un dispositivo sin sistema de archivos solo se bloquea la próxima vez que se conecta el dispositivo.

Si un usuario del equipo donde se ha instalado Kaspersky Endpoint Security debe solicitar el acceso a un dispositivo que el usuario cree que se bloqueó por equivocación, envíe al usuario las [instrucciones para solicitar acceso](#).

La configuración del componente Control de Dispositivos

Parámetro	Descripción
<b>Permitir solicitudes de acceso temporal</b>  <i>(disponible solo en la Consola de Kaspersky Security Center)</i>	<p>Si se selecciona la casilla de verificación, el botón <b>Solicitar acceso</b> está disponible a través de la interfaz local de Kaspersky Endpoint Security. Al hacer clic en este botón, se abre la ventana <b>Solicitar acceso al dispositivo</b>. En esta ventana, el usuario puede solicitar acceso temporal a un dispositivo bloqueado.</p>
<b>Dispositivos y redes wifi</b>	<p>Esta tabla muestra todos los tipos de dispositivos posibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso.</p>
<b>Buses de conexión</b>	<p>Una lista con todos los buses de conexión disponibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso.</p>
<b>Dispositivos de confianza</b>	<p>Una lista con los dispositivos de confianza y los usuarios que tienen acceso a esos dispositivos.</p>
<b>Anti-Bridging</b>	<p>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.</p> <p>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.</p> <p>Cuando una conexión activa y una conexión nueva son del mismo tipo (por ejemplo, wifi), Kaspersky Endpoint Security bloquea la conexión activa y permite que se establezca la conexión nueva.</p> <p>Cuando una conexión activa y una conexión nueva no son del mismo tipo (por ejemplo, adaptador de red y wifi), Kaspersky Endpoint Security bloquea la conexión de menor prioridad y autoriza la de mayor prioridad.</p> <p>Anti-Bridging puede operar con los siguientes tipos de dispositivos: adaptador de red, wifi y módem.</p>
<b>Plantillas de mensajes</b>	<ul style="list-style-type: none"> <li>• <b>Mensaje sobre el bloqueo.</b> 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.</li> </ul>

- **Mensaje al administrador.** Una plantilla del mensaje que se envía al administrador de la LAN cuando el usuario cree que el acceso al dispositivo está bloqueado o que se ha prohibido una operación con el contenido del dispositivo por error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: **Mensaje al administrador por bloqueo del acceso al dispositivo**. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida **Solicitudes de usuarios**. Si su organización no tiene implementado Kaspersky Security Center o no hay conexión con el Servidor de administración, la aplicación enviará un mensaje al administrador a la dirección de correo electrónico especificada.

## Control de aplicaciones

El Control de aplicaciones gestiona el inicio de aplicaciones en los equipos de los usuarios. Esto le permite implementar una directiva corporativa de seguridad al usar aplicaciones. El Control de aplicaciones también reduce el riesgo de infección del equipo al restringir el acceso a las aplicaciones.

La configuración del Control de aplicaciones consta de los siguientes pasos:

### 1. [Creación de categorías de aplicaciones.](#)

El administrador crea categorías de aplicaciones que el administrador quiere gestionar. Las categorías de aplicaciones están destinadas a todos los equipos de la red corporativa, independientemente de los grupos de administración. Para crear una categoría, puede usar los siguientes criterios: categoría KL (por ejemplo, *Navegadores*), hash de archivo, proveedor de aplicaciones y otros criterios.

### 2. [Crear reglas de Control de aplicaciones.](#)

El administrador crea reglas de Control de aplicaciones en la directiva para el grupo de administración. La regla incluye las categorías de aplicaciones y el estado de inicio de las aplicaciones de estas categorías: bloqueadas o permitidas.

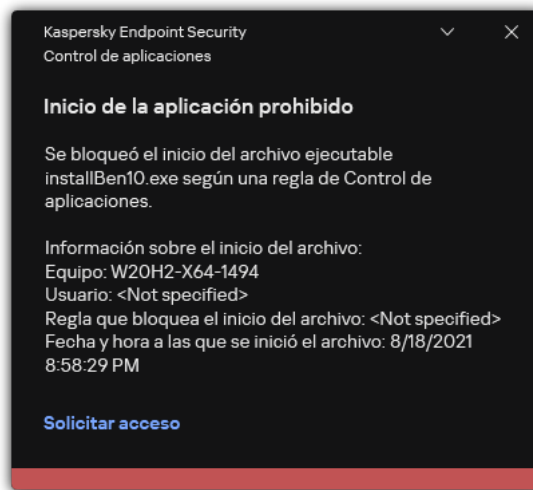
### 3. [Seleccionar el modo de Control de aplicaciones.](#)

El administrador elige el modo para trabajar con las aplicaciones que no estén incluidas en ninguna de las reglas (listas de aplicaciones admitidas y rechazadas).

Cuando un usuario intenta iniciar una aplicación prohibida, Kaspersky Endpoint Security bloqueará el inicio de dicha aplicación y mostrará una notificación (vea la figura a continuación).

Se proporciona un *modo de prueba* para comprobar la configuración de Control de aplicaciones. En este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite el inicio de aplicaciones, incluidas las prohibidas.
- Muestra una notificación sobre el inicio de una aplicación prohibida y añade información al informe en el equipo del usuario.
- Envía datos sobre el inicio de aplicaciones prohibidas a Kaspersky Security Center.



Notificación de Control de aplicaciones

## Modos de funcionamiento de Control de aplicaciones

El componente Control de aplicaciones funciona en dos modos:

- **Lista de rechazados.** En este modo, Control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de Control de aplicaciones.  
Este modo de Control de aplicaciones está activado de forma predeterminada.
- **Lista de permitidos.** En este modo, Control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de Control de aplicaciones.  
Si las reglas de autorización de Control de aplicaciones están totalmente configuradas, el componente bloquea el inicio de todas las aplicaciones nuevas que no haya verificado el administrador de la red de área local, mientras que autoriza el funcionamiento del sistema operativo y de las aplicaciones de confianza en las que los usuarios confían en su trabajo.  
Puede leer las [recomendaciones sobre la configuración de reglas de Control de aplicaciones en el modo de lista de admitidos](#).

El Control de aplicaciones puede configurarse para que funcione en estos modos tanto mediante la interfaz local de Kaspersky Endpoint Security como mediante Kaspersky Security Center.

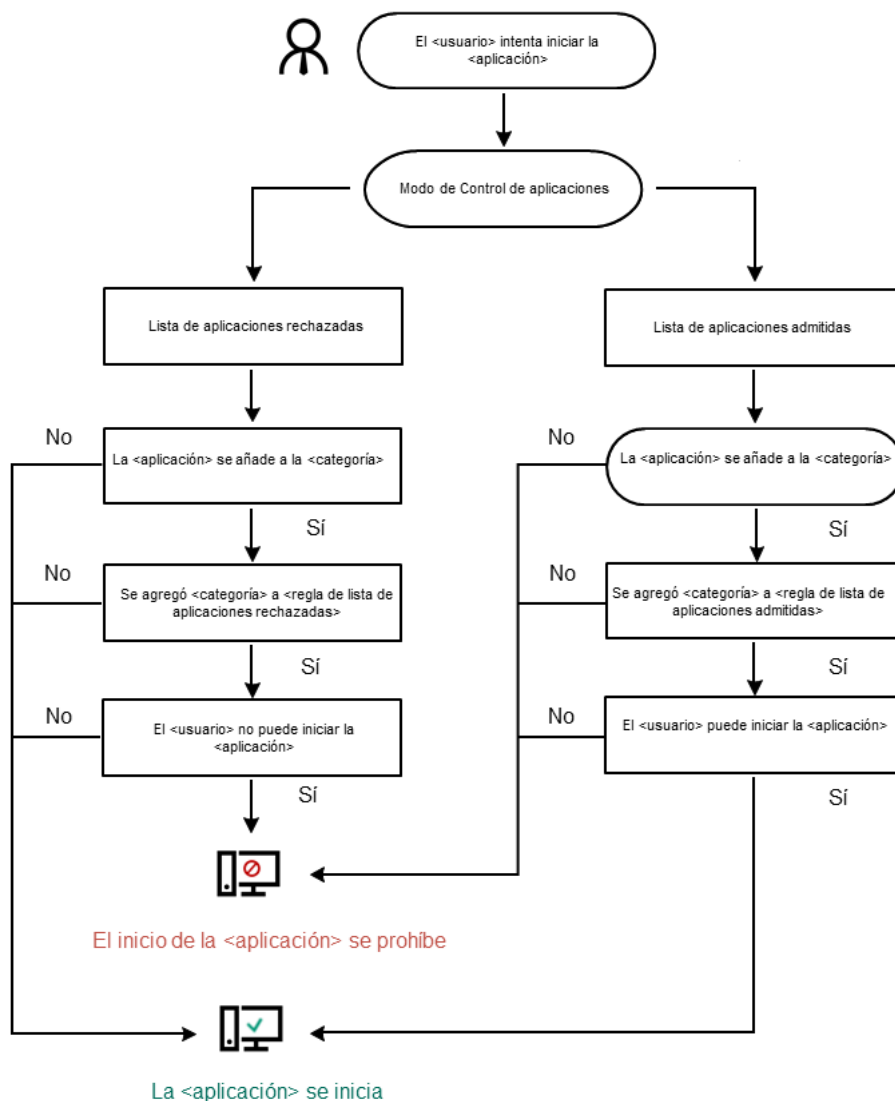
Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas que son necesarias para las siguientes tareas:

- [Creación de categorías de aplicaciones](#).  
Las reglas del componente Control de aplicaciones de la consola de administración de Kaspersky Security Center se basan en categorías de aplicaciones predeterminadas, y no en reglas de inclusión y exclusión, como sucede en la interfaz local de Kaspersky Endpoint Security.
- [Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN](#).

Por eso, se recomienda usar Kaspersky Security Center para configurar el funcionamiento del componente Control de aplicaciones.

## Algoritmo de funcionamiento de Control de aplicaciones

Kaspersky Endpoint Security utiliza un algoritmo para tomar una decisión sobre el inicio de una aplicación (vea la figura a continuación).



Algoritmo de funcionamiento de Control de aplicaciones

Parámetros del componente Control de aplicaciones

Parámetro	Descripción
<b>Modo de prueba</b>	Si se activa este interruptor, 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.
<b>Modo de Control de aplicaciones</b>	<p>Puede elegir una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• <b>Lista de rechazados.</b> Si se selecciona esta opción, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto las prohibidas por las condiciones de las reglas de bloqueo de Control de aplicaciones.</li> <li>• <b>Lista de permitidos.</b> Si se selecciona esta opción, Control de aplicaciones impide que los usuarios inicien las aplicaciones que no cumplen con las condiciones de las reglas de autorización de Control de aplicaciones.</li> </ul>



	<p>Cuando se selecciona el modo <b>Lista de permitidos</b>, se crean automáticamente dos reglas de Control de aplicaciones:</p> <ul style="list-style-type: none"> <li>• <b>Golden Image.</b></li> <li>• <b>Actualizadores de confianza.</b></li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>No puede modificar la configuración ni eliminar las reglas creadas automáticamente. Puede activar o desactivar estas reglas.</p> </div>
<p><b>Controlar la carga de los módulos DLL (incrementa significativamente la carga del sistema)</b></p>	<p>Si se selecciona, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. La información sobre el módulo de DLL y la aplicación que cargó dicho módulo se registra en el informe.</p> <div style="background-color: #ffe6e6; padding: 10px; margin-top: 10px;"> <p>Si planea activar el control sobre los controladores y módulos DLL que se carguen, asegúrese de que, en la configuración Control de aplicaciones, esté activada la regla <b>Golden Image</b> predeterminada u otra regla que contenga la categoría KL "Certificados de confianza" y garantice que los controladores y módulos DLL de confianza se carguen antes de que se inicie Kaspersky Endpoint Security. Activar la supervisión de la carga de los módulos DLL y los controladores cuando la regla <b>Golden Image</b> esté desactivada puede causar inestabilidad en el sistema operativo.</p> </div> <p>Kaspersky Endpoint Security solamente supervisa los controladores y módulos DLL que se carguen desde el momento en que se selecciona la casilla de verificación. Después de seleccionar la casilla de verificación, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security.</p>
<p><b>Plantillas de mensajes</b></p>	<p><b>Mensaje sobre el bloqueo.</b> Plantilla del mensaje que aparece si se activa una regla de Control de aplicaciones que impide el inicio de una aplicación.</p> <p><b>Mensaje al administrador.</b> Plantilla del mensaje que un usuario puede enviar al administrador de la red de área local corporativa si el usuario cree que la aplicación se ha bloqueado por error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: <b>Mensaje al administrador por bloqueo del inicio de la aplicación</b>. La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida <b>Solicitudes de usuarios</b>. 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.</p>

## Control de anomalías adaptativo

Este componente está disponible solo para Kaspersky Endpoint Security for Business Advanced y Kaspersky Total Security for Business. Para obtener más información sobre Kaspersky Endpoint Security for Business, visite el [sitio web de Kaspersky](#).

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos en una red de la empresa. El Control de anomalías adaptativo utiliza un conjunto de reglas para supervisar el comportamiento inusual (por ejemplo, la regla *Inicio de Microsoft PowerShell desde la aplicación Office*). Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad maliciosa. Puede configurar el modo en que el Control de anomalías adaptativo gestiona cada regla y, por ejemplo, permitir la ejecución de scripts de PowerShell que automatizan determinadas tareas de flujo de trabajo. Kaspersky Endpoint Security actualiza el conjunto de reglas junto con las bases de datos de la aplicación. Las actualizaciones de los conjuntos de reglas deben [confirmarse manualmente](#).

## Parámetros del Control de anomalías adaptativo

Para configurar el Control de anomalías adaptativo se tienen que realizar los pasos siguientes:

### 1. Autoaprendizaje del Control de anomalías adaptativo.

Después de habilitar el Control de anomalías adaptativo, sus reglas funcionan en el *modo de autoaprendizaje*. Durante el aprendizaje, el Control de anomalías adaptativo supervisa la activación de reglas y envía eventos de activación a Kaspersky Security Center. Cada regla tiene su propia duración del modo de autoaprendizaje. La duración del modo de autoaprendizaje es establecida por los expertos de Kaspersky. Por lo general, el modo de autoaprendizaje está activo durante dos semanas.

Si una regla no se ha activado nunca durante el autoaprendizaje, el Control de anomalías adaptativo considerará las acciones asociadas a esta regla como no típicas. Kaspersky Endpoint Security bloqueará todas las acciones asociadas a esa regla.

Si se activó una regla durante el autoaprendizaje, Kaspersky Endpoint Security registra los eventos en el [informe de activación de las reglas](#) y en el repositorio de **Activación de reglas en el estado Aprendizaje inteligente**.

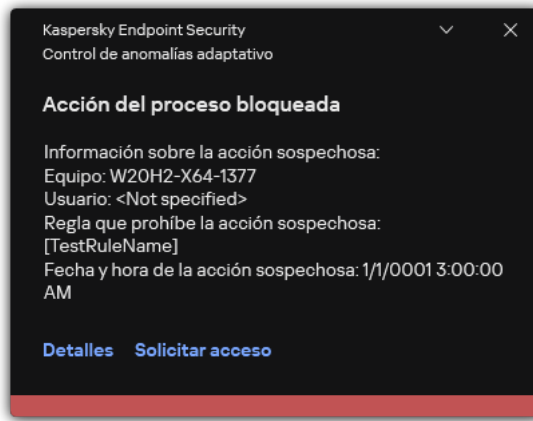
### 2. Analizar el informe de activación de las reglas.

El administrador analiza el [informe de activación de las reglas](#) o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. A continuación, el administrador puede seleccionar el comportamiento del Control de anomalías adaptativo cuando se active la regla para bloquearlo o permitirlo. El administrador también puede seguir supervisando el funcionamiento de la regla y ampliar su duración durante el modo de autoaprendizaje. Si el administrador no realiza ninguna acción, la aplicación también seguirá funcionando en el modo de autoaprendizaje. El plazo de aprendizaje se reiniciará.

El Control de anomalías adaptativo se configura en tiempo real. El Control de anomalías adaptativo se configura a través de los siguientes canales:

- El Control de anomalías adaptativo empieza a bloquear automáticamente las acciones asociadas con las reglas que no se activaron nunca en el modo de autoaprendizaje.
- Kaspersky Endpoint Security añade nuevas reglas o elimina las obsoletas.
- El administrador configura el funcionamiento del Control de anomalías adaptativo tras revisar el informe de activación de las reglas o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**. Se recomienda comprobar el informe de activación de las reglas o los contenidos del repositorio de **Activación de reglas en el estado Aprendizaje inteligente**.

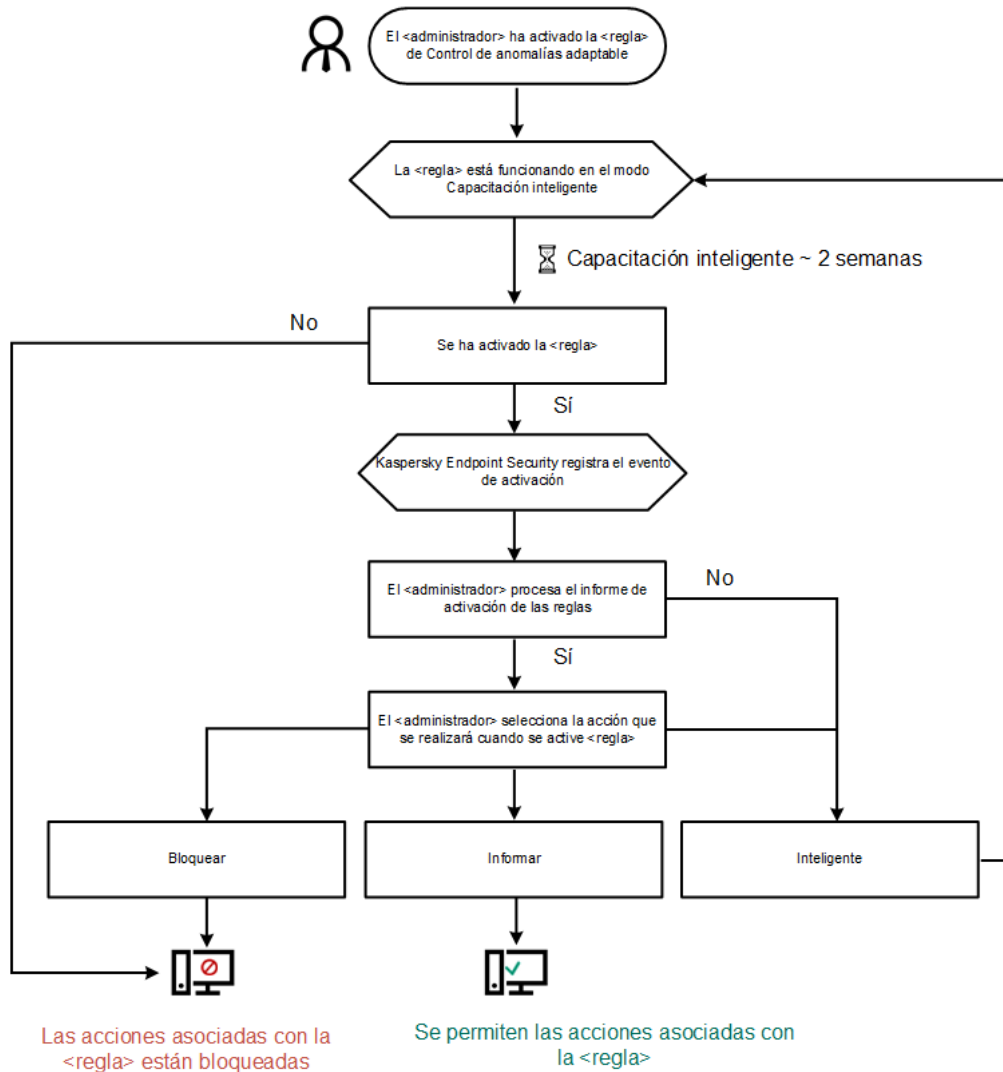
Cuando una aplicación maliciosa intenta realizar una acción, Kaspersky Endpoint Security bloqueará dicha acción y mostrará una notificación (vea la figura a continuación).



Notificación del Control de anomalías adaptativo

## Algoritmo de funcionamiento del Control de anomalías adaptativo

Kaspersky Endpoint Security decide si se autoriza o se bloquea una acción que esté asociada con una regla de acuerdo al siguiente algoritmo (consulte la siguiente figura).



Algoritmo de funcionamiento del Control de anomalías adaptativo

Parámetros del componente Control de anomalías adaptativo

Parámetro	Descripción

<p><b>Informe de estado de reglas de Control de anomalías adaptativo</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Este informe contiene información sobre el estado de las reglas de detección del Control de anomalías adaptativo (por ejemplo, la regla <i>Inactivo</i> o <i>Bloquear</i>). Este informe se genera para todos los grupos de administración.</p>
<p><b>Informe de reglas activadas del Control de anomalías adaptativo</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Este informe contiene información sobre las acciones no típicas detectadas al usar el Control de anomalías adaptativo. Este informe se genera para todos los grupos de administración.</p>
<p><b>Reglas</b></p>	<p>Tabla de reglas del Control de anomalías adaptativo Los especialistas de Kaspersky crean las reglas sobre la base de los escenarios habituales de actividad potencialmente maliciosa.</p>
<p><b>Plantillas</b></p>	<ul style="list-style-type: none"> <li>• <b>Mensaje sobre el bloqueo.</b> Plantilla del mensaje que se muestra a un usuario cuando se activa una regla del Control de anomalías adaptativo que bloquea una acción no típica.</li> <li>• <b>Mensaje al administrador.</b> Plantilla del mensaje que un usuario puede enviar al administrador de la red corporativa local si el usuario considera que el bloqueo es un error. Después de que el usuario solicite acceso, Kaspersky Endpoint Security envía un evento a Kaspersky Security Center: <b>Mensaje al administrador por bloqueo de la actividad de aplicaciones.</b> La descripción del evento contiene un mensaje para el administrador con variables sustituidas. Puede ver estos eventos en la consola de Kaspersky Security Center usando la selección de eventos predefinida <b>Solicitudes de usuarios.</b> 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.</li> </ul>

## Sensor de Endpoint

Kaspersky Endpoint Security 11.4.0 no incluye Sensor de Endpoint.

Puede administrar el Endpoint Sensor en Kaspersky Security Center Web Console y en la Consola de administración de Kaspersky Security Center. No se puede administrar el Endpoint Sensor en Kaspersky Security Center Cloud Console.

*Endpoint Sensor* está diseñado para interactuar con la Plataforma antiataques dirigidos de Kaspersky. *Kaspersky Anti Targeted Attack Platform* es una solución diseñada para detener a tiempo amenazas sofisticadas, como ataques dirigidos, amenazas persistentes avanzadas (APT) y ataques de día cero, entre otras. Kaspersky Anti Targeted Attack Platform incluye dos bloques funcionales: Kaspersky Anti Targeted Attack (en adelante también llamado "KATA") y Kaspersky Endpoint Detection and Response (en adelante también llamado "KEDR"). Puede comprar KEDR por separado. Para obtener información acerca de la solución, consulte la [Ayuda de Kaspersky Anti Targeted Attack Platform](#).

La administración de Endpoint Sensor tiene las siguientes limitaciones:

- Puede configurar Endpoint Sensor en una directiva siempre que la versión de Kaspersky Endpoint Security instalada en el equipo sea de la 11.0.0 a la 11.3.0. Para obtener más información sobre cómo configurar Endpoint Sensor utilizando la directiva, consulte los [artículos de ayuda de las versiones anteriores de Kaspersky Endpoint Security](#).
- Si la versión de Kaspersky Endpoint Security instalada en el equipo es la 11.4.0 o posterior, no podrá configurar Endpoint Sensor en la directiva.

Endpoint Sensor se instala en los equipos cliente. Una vez instalado, vigila de forma constante los procesos, las conexiones de red activas y los archivos que se modifican en esos equipos. El componente remite entonces la información al servidor de KATA.

La funcionalidad del componente está disponible con estos sistemas operativos:

- Windows 7 Service Pack 1 Home/Professional/Enterprise;
- Windows 8.1 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](#).

## Kaspersky Sandbox

Kaspersky Endpoint Security 11.7.0 ahora tiene un agente incorporado para la integración con la solución Kaspersky Sandbox. La solución Kaspersky Sandbox detecta y bloquea automáticamente las amenazas avanzadas en los equipos. Kaspersky 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. Kaspersky Sandbox analiza objetos en servidores especiales con imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows (servidores de Kaspersky Sandbox). Para obtener más información acerca de la solución, consulte la [Ayuda de Kaspersky Sandbox](#).

El componente solo se puede administrar mediante Kaspersky Security Center Web Console. No puede administrar este componente mediante la Consola de administración (MMC).

#### Configuración del componente Kaspersky Sandbox

Parámetro	Descripción
<b>Certificado TLS del servidor</b>	Para configurar una conexión de confianza con los servidores de Kaspersky Sandbox, debe preparar un certificado TLS. A continuación, debe añadir el certificado a los servidores de Kaspersky Sandbox y la directiva de Kaspersky Endpoint Security. Para obtener información sobre cómo preparar el certificado y añadirlo a los servidores, consulte la <a href="#">Ayuda de Kaspersky Sandbox</a> .
<b>Tiempo de espera</b>	Tiempo de espera de conexión para el servidor de Kaspersky Sandbox. Una vez transcurrido el tiempo de espera configurado, Kaspersky Endpoint Security envía una solicitud al siguiente servidor. Puede aumentar el tiempo de espera de conexión de Kaspersky Sandbox 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.
<b>Cola de peticiones de Kaspersky Sandbox</b>	Tamaño de la carpeta de cola de solicitudes. Cuando se accede a un objeto en el equipo (ejecutable iniciado o documento abierto, por ejemplo, en formato DOCX o PDF), Kaspersky Endpoint Security también puede enviar el objeto para que Kaspersky Sandbox lo analice. Si hay varias solicitudes, Kaspersky Endpoint Security crea una cola de solicitudes. De forma predeterminada, el tamaño de la carpeta de cola de solicitudes está limitado a 100 MB. Una vez que se alcanza el tamaño máximo, Kaspersky Sandbox deja de añadir nuevas solicitudes a la cola y envía el evento correspondiente a Kaspersky Security Center. Puede configurar el tamaño de la carpeta de cola de solicitudes en función de la configuración de su servidor.
<b>Servidores Kaspersky Sandbox</b>	Configuración de la conexión del servidor de Kaspersky Sandbox. Los servidores utilizan imágenes virtuales desplegadas de los sistemas operativos de Microsoft Windows para ejecutar objetos que se deben analizar. Puede introducir una dirección IP (IPv4 o IPv6) o un nombre de dominio completo.
<b>Acción al detectar una amenaza</b>	<p><b>Mover la copia a la cuarentena, eliminar objeto.</b> Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la cuarentena.</p> <p><b>Ejecutar análisis de áreas críticas.</b> Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea <a href="#">Análisis de áreas críticas</a>. De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.</p> <p><b>Crear una tarea de análisis de IOC.</b> Si se selecciona esta opción, Kaspersky Endpoint Security crea la tarea de <a href="#">análisis de IOC</a> automáticamente (tarea de análisis de IOC autónoma). Para esta tarea, puede configurar el modo de ejecución, la cobertura del análisis y la acción al detectar un IOC: eliminar objeto, ejecutar la tarea de <a href="#">análisis de áreas críticas</a>. Para modificar otros parámetros de la tarea de <a href="#">análisis de IOC</a>, vaya a la configuración de la tarea.</p>
<b>Cobertura de análisis de IOC</b>	<b>Áreas críticas de archivos.</b> Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC solo en áreas críticas de archivos del equipo: memoria del núcleo y sectores de arranque.

	<b>Áreas de archivos en las unidades de sistema del equipo.</b> Si se selecciona esta opción, Kaspersky Endpoint Security realiza un análisis de IOC en la unidad de sistema del equipo.
<b>Ejecutar la tarea de análisis IOC</b>	<p><b>Manual.</b> Modo de ejecución en el que puede iniciar la tarea de <i>análisis de IOC</i> manualmente a la hora que elija.</p> <p><b>Luego de detectar la amenaza.</b> Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea de <i>análisis de IOC</i> automáticamente cada vez que se detecta una amenaza.</p> <p><b>Ejecutar solo cuando el equipo está inactivo.</b> Modo de ejecución en el que Kaspersky Endpoint Security ejecuta la tarea de <i>análisis de IOC</i> si el protector de pantalla está activo o la pantalla está bloqueada. Si el usuario desbloquea el equipo, Kaspersky Endpoint Security pausa la tarea. Esto significa que la tarea puede tardar varios días en completarse.</p>

## Endpoint Detection and Response

Kaspersky Endpoint Security 11.7.0 ahora tiene un agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante también "EDR Optimum"). Kaspersky Endpoint Security 11.8.0 ahora tiene un agente integrado para la solución Kaspersky Endpoint Detection and Response Expert (en adelante también "EDR Expert"). *Kaspersky Endpoint Detection and Response* es una variedad de soluciones para proteger la infraestructura de TI corporativa de las amenazas cibernéticas avanzadas. La funcionalidad de las soluciones combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware y ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. EDR Expert ofrece más funcionalidades de supervisión y respuesta a las amenazas que EDR Optimum. Para obtener más información sobre las soluciones, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Detection and Response examina y analiza el desarrollo de amenazas e informa al *personal de seguridad* o al *Administrador* del posible ataque, para permitir una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana separada. *Detalles de la alerta* es una herramienta para ver toda la información recolectada sobre una amenaza detectada. Detalles de la alerta incluye, por ejemplo, el historial de archivos que aparecen en el equipo. Para obtener más información sobre la administración de los detalles de la alerta, consulte la [Ayuda de Kaspersky Endpoint Detection and Response Optimum](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

Puede configurar el componente EDR Optimum en Web Console y Cloud Console. La configuración de componente para EDR Expert está disponible solo en Cloud Console.

### Configuración de Endpoint Detection and Response

Parámetro	Descripción
<b>Aislamiento de red</b>	<p>Aislamiento automático del equipo de la red en respuesta a amenazas detectadas.</p> <p>Cuando el aislamiento de red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones TCP/IP nuevas en el equipo. La aplicación deja solo las siguientes conexiones activas:</p> <ul style="list-style-type: none"> <li>• Conexiones enumeradas en exclusiones de aislamiento de red.</li> <li>• Conexiones iniciadas por los servicios de Kaspersky Endpoint Security.</li> <li>• Conexiones iniciadas por el agente de administración de Kaspersky Security Center.</li> </ul>
<b>Desbloquear automáticamente</b>	El aislamiento de red se puede desactivar automáticamente después de un tiempo especificado o manualmente. De forma predeterminada, Kaspersky Endpoint Security

<b>el equipo aislado en N horas</b>	desactiva el aislamiento de red 5 horas después del inicio del aislamiento.
<b>Exclusiones de aislamiento de red</b>	<p>Lista de reglas para las exclusiones del aislamiento de red. Las conexiones de red que coinciden con las reglas no se bloquean en los equipos cuando el aislamiento de red está activado.</p> <p>Para configurar las Exclusiones de aislamiento de red, puede usar una lista de <i>perfiles de red estándar</i>. De forma predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones manualmente.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si el aislamiento de red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center.</p> </div>
<b>Prevención de ejecución</b>	Controle la ejecución de archivos ejecutables y scripts y la apertura de archivos en formato Office. Por ejemplo, puede evitar la ejecución de aplicaciones que se consideran inseguras en el equipo seleccionado. La prevención de ejecución es compatible con <a href="#">un conjunto de extensiones de archivos</a> y <a href="#">un conjunto de intérpretes de script</a> .
<b>Acción al ejecutar o abrir un objeto prohibido</b>	<p><b>Bloquear y escribirlo en el informe.</b> En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Windows y en el registro de eventos de Kaspersky Security Center.</p> <p><b>Solo eventos del registro.</b> 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.</p>
<b>Normas de prevención de la ejecución</b>	Lista de reglas de prevención de ejecución de objetos. Una <i>regla de prevención de ejecución</i> es un conjunto de criterios que se consideran al realizar bloqueos. La aplicación identifica archivos por sus rutas o sumas de comprobación calculadas mediante algoritmos hash MD5 y SHA256.

## 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



Después de que se hayan cifrado los discos duros del sistema, en el siguiente inicio de sesión en el equipo, el usuario debe autenticarse en el [Agente de autenticación](#) antes de que se pueda acceder a los discos duros y cargar el sistema operativo. Esto requiere la introducción de la contraseña del token o la tarjeta inteligente conectada al equipo, o bien el nombre de usuario y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local que utilice la tarea [Administrar cuentas del agente de autenticación](#). Estas cuentas se basan en las cuentas de Microsoft Windows con las que los usuarios inician sesión en el sistema operativo. También puede usar la [tecnología de inicio de sesión único \(SSO\)](#), que le permite iniciar sesión automáticamente en el sistema operativo utilizando el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

La autenticación de usuario en Agente de autenticación se puede realizar de dos maneras:

- Introduzca el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local con las herramientas de Kaspersky Security Center.
- Introduzca la contraseña de un token o una tarjeta inteligente conectados al equipo.

El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, no se podrá agregar el archivo del certificado electrónico al comando.

## Cifrado de unidad BitLocker

*BitLocker* es una tecnología de cifrado integrada en los sistemas operativos Windows. Kaspersky Endpoint Security le permite controlar y gestionar BitLocker utilizando Kaspersky Security Center. BitLocker cifra los volúmenes lógicos. BitLocker no se puede utilizar para el cifrado de unidades extraíbles. Para obtener más detalles sobre BitLocker, consulte la [documentación de Microsoft](#).

BitLocker proporciona almacenamiento seguro de claves de acceso utilizando un módulo de plataforma segura. Un *módulo de plataforma segura (TPM)* es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del ordenador e interactúa con todos los otros componentes del sistema a través del bus de hardware. Utilizar el módulo TPM es el modo más seguro de almacenar las claves de acceso de BitLocker, ya que TPM proporciona verificación de integridad del sistema antes del inicio. Sigue pudiendo cifrar unidades en un equipo sin un módulo TPM. En este caso, la clave de acceso se cifrará con una contraseña. BitLocker utiliza los siguientes métodos de autenticación:

- TPM.
- TPM y PIN.
- Contraseña.

Después de cifrar una unidad, BitLocker crea una clave maestra. Kaspersky Endpoint Security envía la clave maestra a Kaspersky Security Center para que pueda [restaurar el acceso al disco](#), por ejemplo, si un usuario ha olvidado la contraseña.

Si un usuario cifra un disco con BitLocker, Kaspersky Endpoint Security enviará [información sobre el cifrado de disco a Kaspersky Security Center](#). Sin embargo, Kaspersky Endpoint Security no enviará la clave maestra a Kaspersky Security Center, por lo que será imposible restaurar el acceso al disco utilizando Kaspersky Security Center. Para que BitLocker funcione correctamente con Kaspersky Security Center, [descifre la unidad](#) y [vuelva a cifrarla](#) utilizando una directiva. Puede descifrar una unidad de manera local o usar una directiva.

Después de cifrar el disco duro del sistema, el usuario debe pasar por el procedimiento de autenticación de BitLocker para iniciar el sistema operativo. Después del procedimiento de autenticación, BitLocker permitirá que los usuarios inicien sesión. BitLocker no admite la tecnología Single Sign-On (SSO).

Si está utilizando directivas de grupo de Windows, desactive la administración de BitLocker en la configuración de directivas. La configuración de directivas de Windows puede entrar en conflicto con la configuración de directivas de Kaspersky Endpoint Security. Al cifrar una unidad, pueden producirse errores.

#### Configuración del componente Cifrado de disco de Kaspersky

Parámetro	Descripción
<b>Modo de cifrado</b>	<p><b>Cifrar todos los discos duros.</b> Si se selecciona este elemento, la aplicación cifra todos los discos duros cuando se aplica la directiva.</p> <p>Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo con la aplicación instalada.</p> <p><b>Descifrar todos los discos duros.</b> Si se selecciona este elemento, la aplicación descifra todas las unidades de disco duro cifradas previamente cuando se aplica la directiva.</p> <p><b>Dejar sin modificar</b> Si se selecciona este elemento, la aplicación revierte el estado de todas las unidades de disco duro cuando se aplica la directiva. Si se cifró la unidad de disco, permanecerá cifrada. Si se descifró, permanecerá descifrada. Este elemento está seleccionado de forma predeterminada.</p>
<b>Durante el cifrado, crear automáticamente cuentas del Agente de autenticación para usuarios de Windows</b>	<p>Si esta casilla de verificación está seleccionada, la aplicación creará cuentas de agente de autenticación según la lista de cuentas de usuario de Windows en el equipo. De forma predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario ha iniciado sesión en el sistema operativo durante los últimos 30 días.</p>
<b>Configuración de la creación de la cuenta del Agente de autenticación</b>	<p><b>Todas las cuentas del equipo.</b> Si se selecciona esta casilla de verificación, durante la ejecución de la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas del Agente de autenticación para todas las cuentas que han estado activas alguna vez en el equipo.</p> <p><b>Todas las cuentas de dominio en el equipo.</b> Si se selecciona esta casilla de verificación, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas del Agente de autenticación para todas las cuentas que pertenecen a un dominio en particular y que han estado activas alguna vez en el equipo.</p> <p><b>Todas las cuentas locales en el equipo.</b> Si se selecciona esta casilla de verificación, durante la ejecución de la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas del Agente de autenticación para todas las cuentas locales que han estado activas alguna vez en el equipo.</p> <p><b>Administrador local.</b> Si se selecciona esta casilla de verificación, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas de administrador local.</p> <p><b>Administrador del equipo.</b> Si se selecciona esta casilla de verificación, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea una cuenta del Agente de autenticación para la cuenta cuyas propiedades en Active Directory muestran que es una cuenta de administración.</p>

	<p><b>Cuenta activa.</b> Si se selecciona esta casilla de verificación, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea automáticamente una cuenta del Agente de autenticación para la cuenta del equipo que está activa durante la tarea de cifrado.</p>
<p><b>Crear automáticamente cuentas del Agente de autenticación para todos los usuarios de este equipo al iniciar sesión</b></p>	<p>Si esta casilla de verificación está seleccionada, la aplicación verifica la información sobre las cuentas de usuario de Windows en el equipo antes de iniciar el Agente de autenticación. Si Kaspersky Endpoint Security detecta una cuenta de usuario de Windows que no tiene una cuenta de Agente de autenticación, la aplicación creará una nueva cuenta para acceder a las unidades cifradas. La nueva cuenta del Agente de autenticación tendrá la siguiente configuración predeterminada: inicio de sesión protegido con contraseña únicamente y cambio de contraseña en la primera autenticación. Por lo tanto, no es necesario <a href="#">agregar manualmente cuentas del Agente de autenticación</a> mediante la tarea <i>Administrar cuentas del Agente de autenticación</i> para equipos con unidades ya cifradas.</p>
<p><b>Guardar el nombre de usuario introducido en el Agente de autenticación</b></p>	<p>Si se selecciona la casilla de verificación, la aplicación guarda el nombre de la cuenta del Agente de Autenticación. No se le solicitará introducir el nombre de la cuenta la próxima vez que intente realizar una autorización en el Agente de autenticación con la misma cuenta.</p>
<p><b>Cifrar únicamente el espacio en disco utilizado</b></p>	<p>Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado.</p> <div data-bbox="424 958 1493 1151" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Activar o desactivar la función <b>Cifrar solo el espacio en disco utilizado (SO Windows 8 y versiones posteriores)</b> después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado.</p> </div> <p>Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden.</p> <p>Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente.</p> <div data-bbox="424 1420 1493 1648" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables.</p> </div> <p>Esta casilla de verificación está desactivada de forma predeterminada.</p>
<p><b>Utilizar Legacy USB Support</b></p>	<p>Esta casilla de verificación activa o desactiva la función Legacy USB Support. <i>Legacy USB Support</i> es una función BIOS/UEFI que le permite usar dispositivos USB (como un token de seguridad) durante la fase de inicio del equipo antes de iniciar el sistema operativo (modo BIOS). Legacy USB Support no afecta a la compatibilidad con dispositivos USB después del inicio del sistema operativo.</p> <p>Si la casilla está seleccionada, se activará la compatibilidad con dispositivos USB durante el primer inicio del equipo.</p>

	<p>Cuando la función Legacy USB Support está activada, el Agente de autenticación en el modo BIOS no permite trabajar con tokens a través de USB. Se recomienda usar esta opción solo cuando existe un problema de compatibilidad de hardware y solo para los equipos en los cuales se produce el problema.</p>
<b>Configuración de contraseña</b>	<p>Configuración de seguridad de la contraseña de la cuenta del Agente de autenticación. También puede activar el uso de la tecnología de inicio de sesión único (SSO).</p> <p>La tecnología SSO posibilita el uso de las mismas credenciales de la cuenta para acceder a unidades de disco duro cifradas e iniciar sesión en el sistema operativo.</p> <p>Si la casilla está seleccionada, debe introducir las credenciales de la cuenta para acceder a los discos duros cifrados y, luego, iniciar sesión automáticamente en el sistema operativo.</p> <p>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.</p>
<b>Textos de ayuda</b>	<p><b>Autenticación.</b> Texto de ayuda que aparece en la ventana del Agente de autenticación al introducir las credenciales de la cuenta.</p> <p><b>Cambiar contraseña.</b> Texto de ayuda que aparece en la ventana del Agente de autenticación al cambiar la contraseña de la cuenta del Agente de autenticación.</p> <p><b>Recuperar contraseña.</b> Texto de ayuda que aparece en la ventana del Agente de autenticación al recuperar la contraseña de la cuenta del Agente de autenticación.</p>

Configuración del componente Cifrado de unidad BitLocker

Parámetro	Descripción
<b>Modo de cifrado</b>	<p><b>Cifrar todos los discos duros.</b> Si se selecciona este elemento, la aplicación cifra todos los discos duros cuando se aplica la directiva.</p> <p>Si el equipo tiene varios sistemas operativos instalados, después del cifrado, solo podrá cargar el sistema operativo con la aplicación instalada.</p> <p><b>Descifrar todos los discos duros.</b> Si se selecciona este elemento, la aplicación descifra todas las unidades de disco duro cifradas previamente cuando se aplica la directiva.</p> <p><b>Dejar sin modificar</b> Si se selecciona este elemento, la aplicación revierte el estado de todas las unidades de disco duro cuando se aplica la directiva. Si se cifró la unidad de disco, permanecerá cifrada. Si se descifró, permanecerá descifrada. Este elemento está seleccionado de forma predeterminada.</p>
<b>Activar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en tabletas</b>	<p>Esta casilla de verificación activa o desactiva el uso de la autenticación que requiere la entrada de datos en un entorno de prearranque, incluso si la plataforma no tiene la capacidad de entrada de prearranque (por ejemplo, con los teclados de la pantalla táctil de las tabletas).</p> <p>La pantalla táctil de las tabletas no está disponible en el entorno de prearranque. Para completar la autenticación BitLocker en tabletas, el usuario debe conectar un teclado USB, por ejemplo.</p>

	<p>Si selecciona, se permite el uso de la autenticación que requiere la entrada de prearranque en las tabletas. Se recomienda utilizar esta configuración solo en dispositivos con herramientas alternativas de entrada de datos en un entorno de prearranque, como un teclado USB, además de los teclados de la pantalla táctil.</p> <p>Si se desactiva, el Cifrado de unidad BitLocker no es posible en tabletas.</p>
<p><b>Uso del cifrado basado en hardware</b></p>	<p>Si se selecciona, la aplicación utiliza el cifrado basado en hardware, lo que le permite aumentar la velocidad de cifrado y utilizar menos recursos del equipo.</p>
<p><b>Cifrar solo el espacio en disco utilizado (SO Windows 8 y versiones posteriores)</b></p>	<p>Esta casilla activa o desactiva la opción que limita el área de cifrado solo a los sectores del disco duro que están ocupados. Este límite le permite reducir el tiempo de cifrado.</p> <div data-bbox="427 533 1493 725" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Activar o desactivar la función <b>Cifrar solo el espacio en disco utilizado (SO Windows 8 y versiones posteriores)</b> después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado.</p> </div> <p>Si se selecciona, solo se cifran las partes del disco duro ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden.</p> <p>Si se desactiva, se cifra todo el disco duro, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente.</p> <div data-bbox="427 994 1493 1223" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Se recomienda esta opción para nuevos discos duros cuyos datos no se han modificado ni eliminado. Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables.</p> </div> <p>Esta casilla de verificación está desactivada de forma predeterminada.</p>
<p><b>Parámetros de autenticación</b></p>	<p><b>Usar contraseña (SO Windows 8 y versiones posteriores)</b></p> <p>Si se selecciona esta opción, Kaspersky Endpoint Security solicita una contraseña al usuario cada vez que este intenta acceder a la unidad cifrada.</p> <p>Se puede seleccionar cuando el módulo de plataforma segura (TPM) no se está utilizando.</p> <p><b>Usar el módulo de plataforma segura (TPM)</b></p> <p>Si se selecciona esta opción, BitLocker utiliza el módulo de plataforma segura (TPM).</p> <p>Un <i>módulo de plataforma segura (TPM)</i> es un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del ordenador e interactúa con todos los otros componentes del sistema a través del bus de hardware.</p> <div data-bbox="427 1845 1493 2038" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>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.</p> </div>

Un dispositivo equipado con un módulo de plataforma segura puede crear claves de cifrado que solo con dicho dispositivo se pueden descifrar. El módulo de plataforma segura cifra las claves de cifrado con su propia clave raíz de almacenamiento. La clave raíz de almacenamiento se guarda en el módulo de plataforma segura, lo que proporciona un nivel adicional de protección contra los intentos de piratear las claves de cifrado.

Esta acción está seleccionada de forma predeterminada.

Puede establecer una capa de protección adicional para acceder a la clave de cifrado, y cifrar la clave con una contraseña o PIN:

- **Utilizar PIN para el TPM.** Si esta casilla de verificación está seleccionada, un usuario puede utilizar un código PIN para obtener acceso a una clave de cifrado almacenada en el módulo de plataforma segura (TPM). Si la casilla no está seleccionada, se prohíbe a los usuarios utilizar códigos PIN. Para acceder a la clave de cifrado, un usuario debe introducir la contraseña. Puede permitir que el usuario utilice un PIN optimizado. El *PIN optimizado* permite utilizar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.
- **Usar el módulo de plataforma segura (TPM). Si no está disponible, use la contraseña.** Si se selecciona la casilla de verificación, el usuario podrá utilizar una contraseña para acceder a claves de cifrado cuando el módulo de plataforma segura (TPM) no esté disponible.

Si no se seleccionó la casilla de verificación y el módulo TPM no está disponible, no comenzará el cifrado de disco completo.

## Cifrado de archivos

Puede [compilar listas de archivos](#) por extensión o grupos de extensiones y listas de carpetas almacenadas en las unidades del equipo local, así como crear [reglas para el cifrado de los archivos creados por aplicaciones específicas](#). Después de aplicar una directiva, Kaspersky Endpoint Security cifra y descifra los archivos siguientes:

- archivos añadidos individualmente a listas para su cifrado y descifrado;
- archivos almacenados en carpetas añadidos a listas para su cifrado y descifrado;
- Archivos creados por aplicaciones separadas.

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

El cifrado de archivo tiene las siguientes características especiales:

- Kaspersky Endpoint Security cifra y descifra los archivos de las carpetas predeterminadas solo para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifra ni descifra los archivos de las carpetas predeterminadas de los perfiles de usuario en itinerancia, de los perfiles de usuario obligatorio, de los perfiles de usuario temporal ni de las carpetas redirigidas.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo o aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas se encuentran en la lista de exclusiones del cifrado:

- %WINDIR%;
- %PROGRAMFILES% y %PROGRAMFILES(X86)%;
- Archivos de registro de Windows.

No se puede ver ni modificar la lista de exclusiones del cifrado. Los archivos y las carpetas de la lista de exclusiones del cifrado se pueden añadir a la lista de cifrado, pero no se cifrarán durante el cifrado de archivos.

#### Configuración del componente Cifrado de archivos

Parámetro	Descripción
<b>Modo de cifrado</b>	<p><b>Dejar sin modificar</b> Si se selecciona este elemento, Kaspersky Endpoint Security no cambia los archivos ni las carpetas, los deja sin cifrar o sin descifrar.</p> <p><b>Según las reglas.</b> Si se selecciona este elemento, Kaspersky Endpoint Security cifra los archivos y las carpetas según las reglas de cifrado, descifra los archivos y las carpetas según las reglas de descifrado, y regula el acceso de las aplicaciones a los archivos cifrados según las reglas de aplicaciones.</p> <p><b>Descifrar todo.</b> Si se selecciona este elemento, Kaspersky Endpoint Security descifra todos los archivos y carpetas cifrados.</p>
<b>Reglas de cifrado</b>	<p>Esta pestaña muestra las reglas de cifrado para los archivos almacenados en las unidades locales. Puede añadir archivos de la siguiente manera:</p> <ul style="list-style-type: none"> <li>• <b>Carpetas predeterminadas.</b> Kaspersky Endpoint Security le permite añadir las siguientes áreas: <ul style="list-style-type: none"> <li><b>Documentos.</b> Los archivos en la carpeta estándar <i>Documentos</i> del sistema operativo y sus subcarpetas.</li> <li><b>Favoritos.</b> Los archivos en la carpeta estándar <i>Favoritos</i> del sistema operativo y sus subcarpetas.</li> <li><b>Escritorio.</b> Los archivos en la carpeta estándar <i>Escritorio</i> del sistema operativo y sus subcarpetas.</li> <li><b>Archivos temporales.</b> Archivos temporales relacionados con el funcionamiento de aplicaciones instaladas en el equipo. Por ejemplo, las aplicaciones de Microsoft Office crean archivos temporales que contienen copias de seguridad de documentos.</li> <li><b>Archivos de Outlook.</b> Archivos relacionados con el funcionamiento del cliente de correo Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de libretas de direcciones sin conexión (OAB) y archivos de libretas de direcciones personales (PAB).</li> </ul> </li> <li>• <b>Carpeta personalizada.</b> Puede introducir la ruta de la carpeta. Al añadir una ruta de carpeta, cumpla las siguientes reglas: <ul style="list-style-type: none"> <li>Use una variable de entorno (por ejemplo, %FOLDER%\UserFo1der\). Puede usar una variable de entorno solo una vez y solo al comienzo de la ruta.</li> <li>No use rutas relativas. Puede usar el conjunto \. . \ (p. ej., C:\Users\.. \UserFo1der\). El conjunto \. . \ indica la transición a la carpeta principal.</li> <li>No utilice los caracteres * y ?.</li> <li>No utilice rutas UNC.</li> <li>Utilice ; o , como carácter de separación.</li> </ul> </li> <li>• <b>Archivos por extensión</b> Puede seleccionar grupos de extensiones de la lista, como los <i>Archivos</i> del grupo de extensiones. También puede añadir la extensión del archivo de forma manual.</li> </ul>
<b>Reglas de descifrado</b>	<p>Esta pestaña muestra las reglas de descifrado para los archivos almacenados en las unidades locales.</p>

<b>Reglas para aplicaciones</b>	La pestaña muestra una tabla que contiene las reglas de acceso a archivos cifrados que afectan a las aplicaciones y las reglas de cifrado de los archivos que se crean o modifican mediante aplicaciones independientes.
<b>Configuración de contraseña para paquetes cifrados</b>	Requisitos de seguridad de la contraseña que se deben cumplir al crear paquetes cifrados.

## Cifrado de unidades extraíbles

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si una unidad extraíble con un sistema de archivos no compatible está conectada al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Para proteger los datos de las unidades extraíbles, puede usar los siguientes tipos de cifrado:

- Cifrado de disco completo (FDE).

Cifrado de toda la unidad extraíble, incluido el sistema de archivos.

No se puede acceder a datos cifrados fuera de la red corporativa. También es imposible acceder a datos cifrados dentro de la red corporativa si el equipo no está conectado a Kaspersky Security Center (p. ej., en un equipo "invitado").

- Cifrado de archivos (FLE).

Cifrado solo de los archivos en una unidad extraíble. El sistema de archivos permanece sin cambios.

El cifrado de archivos en unidades extraíbles proporciona la capacidad de acceder a datos fuera de la red corporativa mediante un modo especial llamado *[modo portátil](#)*.

Durante el cifrado, Kaspersky Endpoint Security crea una clave maestra. Kaspersky Endpoint Security guarda la clave maestra en los siguientes repositorios:

- Kaspersky Security Center.

- Equipo del usuario.

La clave maestra está cifrada con la clave secreta del usuario.

- Unidad extraíble.

La clave maestra está cifrada con la clave pública de Kaspersky Security Center.



Una vez que se completa el cifrado, se puede acceder a los datos de la unidad extraíble dentro de la red corporativa como si fuera una unidad extraíble convencional sin cifrar.

## Acceso a datos cifrados

Cuando se conecta una unidad extraíble con datos cifrados, Kaspersky Endpoint Security realiza las siguientes acciones:

1. Comprueba si hay una clave maestra en el almacenamiento local en el equipo del usuario.  
Si se encuentra la clave maestra, el usuario obtiene acceso a los datos en la unidad extraíble.  
Si la clave maestra no se encuentra, Kaspersky Endpoint Security realiza las siguientes acciones:
  - a. Envíe una solicitud a Kaspersky Security Center.  
Después de recibir la solicitud, Kaspersky Security Center envía una respuesta que contiene la clave maestra.
  - b. Kaspersky Endpoint Security guarda la clave maestra en el almacenamiento local en el equipo del usuario para operaciones posteriores con la unidad extraíble cifrada.
2. Descifre los datos.

## Características especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles tiene las siguientes características especiales:

- La directiva con la configuración preestablecida para el cifrado extraíble de la unidad se forma para un grupo específico de equipos administrados. Por lo tanto, el resultado de aplicar la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al que se conecta la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra archivos de solo lectura almacenados en las unidades extraíbles.
- Los siguientes tipos de dispositivo son compatibles como unidades extraíbles:
  - Medios de datos conectados por medio del puerto USB
  - Discos duros conectados por medio de los puertos USB y FireWire
  - Unidades SSD conectadas por medio de los puertos USB y FireWire

Configuración del componente Cifrado de unidades extraíbles

Parámetro	Descripción
<b>Administrar cifrado</b>	<b>Cifrar toda la unidad extraíble.</b> Si se selecciona este elemento, cuando se aplique la directiva con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará las unidades extraíbles sector a sector, incluidos sus sistemas de archivos.

**Cifrar todos los archivos** Si se selecciona este elemento, cuando se aplique la directiva con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará todos los archivos almacenados en las unidades extraíbles. Kaspersky Endpoint Security no vuelve a cifrar archivos que ya están cifrados. El contenido del sistema de archivos de una unidad extraíble, incluidos la estructura de carpetas y los nombres de archivos cifrados, no se cifrará y seguirá siendo accesible.

**Cifrar solo archivos nuevos** Si se selecciona este elemento, cuando se aplique la directiva con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará solamente los archivos que se han añadido a unidades extraíbles o que se han modificado tras la última aplicación de la directiva de Kaspersky Security Center. Conviene emplear este modo de cifrado cuando una unidad extraíble se utiliza tanto para fines personales como profesionales. Este modo de cifrado le permite mantener los antiguos archivos sin cambios y cifrar solamente los archivos que el usuario cree en un equipo de trabajo en el que se haya instalado Kaspersky Endpoint Security y se haya activado la funcionalidad de cifrado. Como resultado, el acceso a los archivos personales está siempre disponible, independientemente de si se ha instalado o no Kaspersky Endpoint Security con la funcionalidad de cifrado activada en el equipo.

**Descifrar toda la unidad extraíble.** Si se selecciona este elemento, cuando se aplique la directiva con la configuración de cifrado de unidades extraíbles especificada, Kaspersky Endpoint Security descifrará todos los archivos cifrados que se hayan almacenado en las unidades extraíbles, así como los sistemas de archivos de las unidades extraíbles, en caso de haberse cifrado previamente.

**Dejar sin modificar** Si se selecciona este elemento, la aplicación revierte el estado de todas las unidades de disco duro cuando se aplica la directiva. Si se cifró la unidad de disco, permanecerá cifrada. Si se descifró, permanecerá descifrada. Este elemento está seleccionado de forma predeterminada.

#### Modo portátil

Esta casilla de verificación activa o desactiva la preparación de una unidad extraíble para poder acceder a los archivos almacenados en esta unidad en aquellos equipos fuera de la red corporativa.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security solicita al usuario que especifique una contraseña antes de cifrar archivos en una unidad extraíble conforme a la aplicación de la directiva. La contraseña es obligatoria para acceder a los archivos cifrados de una unidad extraíble en aquellos equipos fuera de la red corporativa. Puede configurar la seguridad de la contraseña.

El modo portátil está disponible para los modos **Cifrar todos los archivos** o **Cifrar solo archivos nuevos**.

#### Cifrar solo el espacio en disco utilizado

Esta casilla de verificación activa o desactiva el modo de cifrado en el que solo se cifran los sectores ocupados del disco. Se recomienda este modo para nuevas unidades cuyos datos no se han modificado ni eliminado.

Si se selecciona, solo se cifran las partes de la unidad ocupadas por archivos. Kaspersky Endpoint Security cifra automáticamente los datos a medida que se añaden.

Si se desactiva, se cifra toda la unidad, incluidos los fragmentos restantes de los archivos que se han modificado o eliminado previamente.

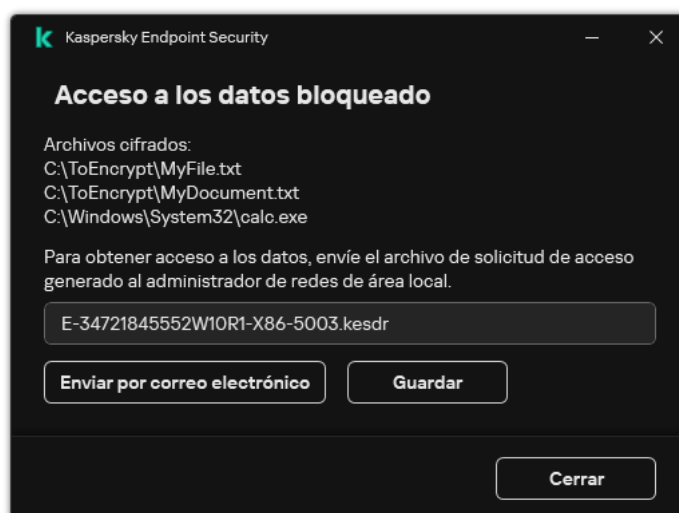
La habilidad de cifrar solo el espacio ocupado está disponible solo para el modo **Cifrar toda la unidad extraíble**.

Una vez iniciado el cifrado, la activación o desactivación de la función **Cifrar solo el espacio en disco utilizado** no cambiará esta configuración. Debe seleccionar o desactivar la casilla de verificación antes de iniciar el cifrado.

<b>Reglas de cifrado para los dispositivos seleccionados</b>	<p>Esta tabla contiene los dispositivos que tienen definidas reglas personalizadas de cifrado. Puede crear reglas de cifrado para unidades extraíbles específicas de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Añada una unidad extraíble de la lista de dispositivos de confianza para Control de dispositivos.</li> <li>• Añada manualmente una unidad extraíble: <ul style="list-style-type: none"> <li>• Por ID de dispositivo (ID de hardware o HWID)</li> <li>• Por modelo de dispositivo: ID de proveedor (VID) e ID de producto (PID)</li> </ul> </li> </ul>
<b>Permitir el cifrado de las unidades extraíbles en modo sin conexión</b>	<p>Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security cifra las unidades extraíbles incluso cuando no existe conexión a Kaspersky Security Center. En este caso, los datos requeridos para descifrar las unidades extraíbles se almacenan en el disco duro del equipo al cual está conectada la unidad extraíble y no se transmiten a Kaspersky Security Center.</p> <p>Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no cifra las unidades extraíbles cuando no existe conexión a Kaspersky Security Center.</p>
<b>Configuración de contraseñas en modo portátil</b>	<p>Configuración de seguridad de contraseña para el Administrador de archivos portátil.</p>

## Plantillas (cifrado de datos)

Después del cifrado de datos, Kaspersky Endpoint Security puede restringir el acceso a los datos, por ejemplo, debido a un cambio en la infraestructura de la organización y a un cambio en el Servidor de Administración de Kaspersky Security Center. Si un usuario no tiene acceso a los datos cifrados, puede solicitarle al administrador acceso a los datos. En otras palabras, el usuario tiene que enviar un archivo de solicitud de acceso al administrador. A continuación, el usuario tiene que cargar el archivo de respuesta recibido del administrador a Kaspersky Endpoint Security. Kaspersky Endpoint Security le permite solicitar el acceso a los datos del administrador por correo electrónico (vea la figura a continuación).



Solicitar acceso a los datos cifrados

Se proporciona una plantilla para informar de la falta de acceso a los datos cifrados. Por comodidad del usuario, puede completar los siguientes campos:

- **A.** Introduzca la dirección de correo electrónico del grupo de administradores con derechos sobre las características de cifrado de datos.
- **Asunto.** Introduzca el asunto del correo electrónico de la solicitud de acceso a archivos cifrados. Por ejemplo, puede añadir etiquetas para filtrar los mensajes.
- **Mensaje.** De ser necesario, cambie el contenido del mensaje. Puede utilizar variables para obtener los datos necesarios (por ejemplo, la variable %USER\_NAME%).

## Exclusiones

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza de manera independiente y tiene en cuenta las características de los objetos que se gestionan y de las aplicaciones que se instalan en el equipo. Puede que sea necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a ellos, si está seguro de que el objeto o la aplicación son inofensivos. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza, además de la zona de confianza general en una directiva.

### Exclusiones del análisis

Una *exclusión de análisis* es un conjunto de condiciones que se deben cumplir para que Kaspersky Endpoint Security no analice un objeto en busca de virus u otras amenazas.

Las exclusiones del análisis permiten utilizar de manera segura software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario. Aunque no poseen ninguna función maliciosa, dichas aplicaciones pueden ser aprovechadas por los intrusos. Para obtener más información sobre el software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos personales de un usuario, visite el [sitio web de la Enciclopedia de Kaspersky](#).

Es posible que Kaspersky Endpoint Security bloquee estas aplicaciones. Para evitar que se bloqueen, puede configurar las exclusiones del análisis para las aplicaciones en uso. Para ello, añada el nombre o la máscara de nombre que figura en la Enciclopedia de Kaspersky a la zona de confianza. Por ejemplo, a menudo se utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security identifica esta actividad como sospechosa y puede que la bloquee. Para evitar el bloqueo de la aplicación, cree una exclusión del análisis con el nombre o la máscara de nombre que se muestra en la Enciclopedia de Kaspersky.

Si la aplicación que recopila la información y la envía para procesarse se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar que esto ocurra, puede excluir la aplicación del análisis mediante la configuración de Kaspersky Endpoint Security como se describe en este documento.

Los siguientes componentes de aplicaciones y tareas que el administrador del sistema configure pueden utilizar exclusiones del análisis:

- [Detección de comportamiento](#).
- [Prevención de exploits](#).

- [Prevención de intrusiones en el host.](#)
- [Protección frente a amenazas en archivos.](#)
- [Protección frente a amenazas web.](#)
- [Protección frente a amenazas en el correo.](#)
- [Tareas de análisis.](#)

## Lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de red y archivos (incluida la actividad maliciosa), así como el acceso al registro del sistema, no supervisa Kaspersky Endpoint Security. De forma predeterminada, Kaspersky Endpoint Security analiza los objetos que el proceso de cualquier aplicación abre, ejecuta o guarda, y controla la actividad de todas las aplicaciones y el tráfico de red que generan. Sin embargo, una aplicación que se añadió a la lista de aplicaciones de confianza está excluida de los análisis de Kaspersky Endpoint Security.

Por ejemplo, si considera que los objetos que emplea el Bloc de notas estándar de Microsoft Windows son seguros sin necesidad de analizarlos, significa que confía en esta aplicación y que puede añadir el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza. Por tanto, el análisis no incluirá objetos que emplee esta aplicación.

Además, algunas acciones que Kaspersky Endpoint Security clasifica como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de diferentes aplicaciones. Por ejemplo, la interceptación de texto que se escribe mediante el teclado es un proceso rutinario para intercambiadores de disposición del teclado automáticos (como Punto Switcher). Para tener en cuenta los detalles de este tipo de aplicaciones y excluir su actividad del proceso de análisis, le recomendamos que las agregue a la lista de aplicaciones de confianza.

La exclusión de aplicaciones de confianza del proceso de análisis permite evitar conflictos de compatibilidad entre Kaspersky Endpoint Security y otros programas (por ejemplo, el problema de analizar dos veces el tráfico de red de un equipo de terceros, por parte de Kaspersky Endpoint Security y de otra aplicación antivirus) y también aumenta el rendimiento del equipo, que es fundamental cuando se emplean aplicaciones de servidor.

Al mismo tiempo, el archivo ejecutable y el proceso de la aplicación de confianza sí que se analizan en busca de virus y otro software malicioso (malware). Puede excluirse completamente una aplicación del análisis de Kaspersky Endpoint Security gracias a las exclusiones del análisis.

### Configuración de exclusiones

Parámetro	Descripción
<b>Tipos de objetos detectados</b>	<p>Independientemente de la configuración de la aplicación, Kaspersky Endpoint Security siempre detecta y bloquea virus, gusanos y troyanos. Pueden provocar daños significativos en el equipo.</p> <ul style="list-style-type: none"> <li>• <a href="#">Virus y gusanos</a> ⓘ</li> </ul>

**Subcategoría:** virus y gusanos (Viruses\_and\_Worms)

**Nivel de amenaza:** alto

Los gusanos y virus tradicionales ejecutan acciones que no autoriza el usuario. Pueden crear copias de ellos mismos, que son capaces de reproducirse.

### **Virus tradicionales**

Cuando un virus tradicional se introduce en un equipo, lo que hace es infectar un archivo, activarse, realizar acciones maliciosas y añadir copias de sí mismo a otros archivos.

Un virus tradicional se multiplica únicamente en los recursos locales del equipo; no puede penetrar en otros equipos por sí mismo. Solo puede pasar a otro equipo si añade una copia de sí mismo a un archivo almacenado en una carpeta compartida o un CD introducido, o si el usuario reenvía un mensaje de correo electrónico con un archivo infectado como adjunto.

Un código de virus tradicional puede penetrar en varias zonas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de secuencias de scripts* y *virus de macros*.

Los virus pueden infectar los archivos a través de una gran diversidad de técnicas. *Los virus de sobrescritura* escriben su código sobre el código del archivo que se infecta, con lo que borran su contenido. El archivo infectado deja de funcionar y no se puede restaurar. *Los virus parásitos* modifican los archivos y los dejan parcial o completamente funcionales. *Los virus compañeros* no modifican los archivos, pero crean duplicados. Cuando se abre un archivo infectado, se inicia un duplicado de él (lo que es un virus en realidad). También existen los siguientes tipos de virus: *virus de vínculos*, *virus para archivos OBJ*, *virus para archivos LIB*, *virus para código fuente* y muchos otros.

### **Gusano**

Como ocurre con los virus tradicionales, el código de los gusanos está diseñado para infiltrarse en un equipo, activarse y realizar acciones maliciosas. La denominación de los gusanos se debe a su capacidad para "arrastrarse" de un equipo a otro y para propagar copias a través de diversos canales sin el permiso del usuario.

La principal característica que permite distinguir entre varios tipos de gusanos es la forma en que se propagan. En la siguiente tabla, se ofrece una descripción general de varios tipos de gusanos, que se clasifican por el modo en que se propagan.

Formas de propagación de los gusanos

<b>Tipo</b>	<b>Nombre</b>	<b>Descripción</b>
<b>Email-Worm</b>	Email-Worm	Se propagan a través del correo electrónico.

		<p>Un mensaje de correo electrónico infectado contiene un archivo adjunto con una copia de un gusano o un enlace a un archivo que se ha cargado en un sitio que se puede haber pirateado o creado exclusivamente para dicho propósito. Al abrir el archivo adjunto, se activa el gusano. Al hacer clic en el enlace, descargar y, a continuación, abrir el archivo, el gusano también comienza a realizar sus acciones maliciosas. Después, continúa propagando copias de sí mismo y buscando otras direcciones de correo electrónico, a las que envía mensajes infectados.</p>
<b>Gusano de mensajería instantánea</b>	Gusanos de cliente de MI	<p>Se propagan a través de clientes de MI.</p> <p>Por lo general, dichos gusanos envían mensajes que contienen un enlace a un archivo con una copia del gusano en un sitio web; para ello usan las listas de contactos del usuario. Cuando el usuario descarga y abre el archivo, el gusano se activa.</p>
<b>Gusano IRC</b>	Gusanos de chat de Internet	<p>Se propagan a través de Internet Relay Chats, sistemas de servicios que permiten la comunicación con otros usuarios a través de Internet en tiempo real.</p> <p>Estos gusanos publican un archivo con una copia de ellos mismos o un enlace a un archivo en un chat de Internet. Cuando el usuario descarga y abre el archivo, el gusano se activa.</p>
<b>Net-Worm</b>	Gusanos de red	<p>Estos gusanos se propagan a través de redes de equipos.</p> <p>A diferencia de otros tipos de gusanos, un gusano de red tradicional se propaga sin intervención del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red especialmente creado (exploit) que contiene el código del gusano o una parte de este. Si un equipo "vulnerable" se encuentra en la red, recibe dicho paquete de red. Cuando el gusano penetra completamente en el equipo, se activa.</p>
<b>Gusano de P2P</b>	Gusanos de redes de uso compartido de archivos	<p>Se propagan a través de las redes de uso compartido de archivos entre pares.</p> <p>Para penetrar en una red P2P, el gusano se copia en una carpeta de uso compartido de archivos, que se ubica normalmente en el equipo del usuario. La red P2P muestra información sobre este archivo para que el usuario pueda "encontrar" el archivo infectado en la red al igual que cualquier otro archivo y, a continuación, descargarlo y abrirlo.</p>

		Los gusanos más sofisticados simulan el protocolo de red de una red P2P determinada: devuelven respuestas positivas a consultas de búsqueda y ofrecen sus copias para descargarlas.
<b>Gusano</b>	Otros tipos de gusanos	<p>Entre otros tipos de gusanos, se incluyen:</p> <ul style="list-style-type: none"> <li>• Gusanos que propagan copias de sí mismos a través de recursos de red. Con las funciones del sistema operativo, pueden analizar las carpetas disponibles de la red, conectarse a equipos en Internet e intentar obtener acceso completo a sus unidades de disco. A diferencia de los tipos de gusanos descritos previamente, los otros tipos de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano.</li> <li>• Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono móvil a otro).</li> </ul>

- [Trojanos \(incluye ransomware\)](#)<sup>?</sup>



## Subcategoría: Troyanos

**Nivel de amenaza:** alto

A diferencia de los gusanos y los virus, los troyanos no se replican. Por ejemplo, se introducen en un equipo a través del correo electrónico o un navegador cuando el usuario visita una página web infectada. Los troyanos se inician con intervención del usuario. Comienzan a realizar acciones maliciosas inmediatamente después de que se inician.

Los distintos troyanos se comportan de forma diferente en los equipos infectados. Las funciones principales de los troyanos consisten en bloquear, modificar o destruir información, y desactivar equipos o redes. Los troyanos también pueden recibir o enviar archivos, ejecutarlos, mostrar mensajes en la pantalla, solicitar páginas web, descargar e instalar programas y reiniciar el equipo.

Los piratas usan conjuntos de diversos troyanos con frecuencia.

Los distintos tipos de comportamiento de los troyanos se describen en la tabla siguiente.

Tipos de comportamiento de los troyanos en un equipo infectado

Tipo	Nombre	Descripción
<b>Trojan-ArcBomb</b>	Troyanos: "archivos bomba"	<p>Al descomprimirlos, estos archivos aumentan de tamaño de tal forma que el funcionamiento del equipo se ve afectado.</p> <p>Cuando el usuario intenta descomprimir un archivo de esas características, es posible que el equipo se vea ralentizado o se congele; el disco duro puede llenarse de datos "vacíos". Los "archivos bomba" son especialmente peligrosos para los servidores de correo y archivos. Si el servidor usa un sistema automático para procesar la información entrante, un "archivo bomba" puede detener el servidor.</p>
<b>Backdoor</b>	Troyanos para administración remota	<p>Se considera que son los troyanos más peligrosos. En sus funciones, se parecen a las aplicaciones de administración remota que se instalan en los equipos.</p> <p>Estos programas se instalan en un equipo sin que el usuario se dé cuenta de ello, lo que permite que el intruso administre el equipo de forma remota.</p>
<b>Troyano</b>	Troyanos	<p>Incluyen las siguientes aplicaciones maliciosas:</p> <ul style="list-style-type: none"><li>• <b>Troyanos tradicionales.</b> Estos programas solo ejecutan las</li></ul>

		<p>funciones principales de los troyanos: bloqueo, modificación o destrucción de información y desactivación de equipos o redes. No cuentan con funciones avanzadas, a diferencia de otros tipos de troyanos descritos en la tabla.</p> <ul style="list-style-type: none"> <li>• <b>Troyanos versátiles.</b> Estos programas tienen funciones avanzadas comunes en varios tipos de troyanos.</li> </ul>
<b>Trojan-Ransom</b>	Troyanos de rescate	<p>Toman como "rehén" la información del usuario para modificarla, bloquearla o afectar al funcionamiento del equipo de modo que el usuario pierda la capacidad de usar la información. El intruso pide un rescate al usuario y le promete enviar una aplicación que restaure el rendimiento del equipo y los datos que estaban almacenados en él.</p>
<b>Trojan-Clicker</b>	Troyanos de clic	<p>Acceden a las páginas web desde el equipo del usuario, ya sea enviando comandos a un navegador o cambiando las direcciones web que se especifican en los archivos del sistema operativo.</p> <p>Con estos programas, los intrusos perpetrarán ataques de red y aumentarán las visitas al sitio web mediante un mayor número de visualizaciones de anuncios publicitarios.</p>
<b>Trojan-Downloader</b>	Descargador de troyanos	<p>Acceden a la página web del intruso, descargan otras aplicaciones maliciosas desde ella y las instalan en el equipo del usuario. Pueden contener el nombre de archivo de la aplicación maliciosa que se va a descargar o recibirla desde la página web a la que se accede.</p>
<b>Trojan-Dropper</b>	Troyanos lanzadera	<p>Contienen otros troyanos que instalan en el disco duro y después se instalan.</p> <p>Los intrusos pueden usar programas del tipo Trojan Dropper para los siguientes propósitos:</p> <ul style="list-style-type: none"> <li>• Instalar una aplicación maliciosa sin que el usuario se dé cuenta: los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (pueden, por ejemplo, advertir</li> </ul>

		<p>sobre la existencia de un archivo dañado o sobre incompatibilidades con el sistema operativo).</p> <ul style="list-style-type: none"> <li>• Para proteger a otra aplicación maliciosa y evitar que se detecte: no todo el software antivirus puede detectar una aplicación maliciosa en una aplicación del tipo Trojan Dropper.</li> </ul>
<b>Trojan-Notifier</b>	Troyanos de notificación	<p>Le informan al atacante que el equipo infectado está accesible y le envían información: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso a través del correo electrónico o el FTP, mediante la página web del intruso o de otro modo.</p> <p>Los programas del tipo Trojan Notifier se usan normalmente como conjuntos compuestos de varios troyanos. Notifican al intruso de que se han instalado correctamente otros troyanos en el equipo del usuario.</p>
<b>Trojan-Proxy</b>	Proxies de troyanos	<p>Permiten al intruso acceder de forma anónima a las páginas web mediante el equipo del usuario; se usan normalmente para enviar correo no deseado.</p>
<b>Trojan-PSW</b>	Software de robo de contraseñas	<p>El software de robo de contraseñas es un tipo de troyano que roba cuentas de usuario, como datos de registro de software. Estos troyanos buscan datos confidenciales en los archivos del sistema y en el Registro, y los envían al "agresor" por correo electrónico, el FTP o mediante acceso a la página web del intruso, o de cualquier otro modo.</p> <p>Algunos de estos troyanos están clasificados en los distintos tipos que se describen en la tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan en Internet (Trojan-GameThief).</p>
<b>Trojan-Spy</b>	Troyanos espía	<p>Espían a los usuarios con el fin de recopilar información sobre las acciones que el usuario lleva a cabo cuando utiliza el equipo. Pueden interceptar los datos que el usuario introduce en el teclado, tomar</p>

		instantáneas o recopilar listas de aplicaciones activas. Una vez que reciben la información, la transfieren al intruso a través de correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo.
<b>Trojan-DDoS</b>	Troyanos atacantes de redes	<p>Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS). Con frecuencia, los piratas infectan diversos equipos con estos programas, de modo que puedan usar los equipos para atacar un solo servidor a la vez.</p> <p>Los programas de DoS perpetran los ataques desde un solo equipo con conocimiento del usuario. Los programas DDoS (Distributed DoS) perpetran los ataques distribuidos desde varios equipos sin que el usuario del equipo infectado lo perciba.</p>
<b>Trojan-IM</b>	Troyanos que roban información de los usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de usuarios de programas de mensajería instantánea. Transfieren los datos al intruso mediante correo electrónico o FTP, accediendo a la página web del intruso o de otro modo.
<b>Rootkit</b>	Rootkits	Enmascaran otras aplicaciones maliciosas y su actividad, con lo que prolongan la persistencia de las aplicaciones en el sistema operativo. Además, pueden ocultar archivos, procesos en la memoria infectada del equipo o claves del registro que ejecutan aplicaciones maliciosas. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones del equipo del usuario y otros equipos de la red.
<b>Trojan-SMS</b>	Troyanos con formato de mensajes SMS	Infectan teléfonos móviles a través del envío de mensajes a números de teléfono de tarificación especial.
<b>Trojan-GameThief</b>	Troyanos que roban información de los usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, para después enviar estos datos al intruso mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo.
<b>Trojan-Banker</b>	Troyanos que roban cuentas	Roban datos de cuentas bancarias o de sistemas de dinero electrónico y

	bancarias	envían la información al hacker mediante su página web, por correo electrónico, por FTP o usando otros medios.
<b>Trojan-Mailfinder</b>	Troyanos que recopilan direcciones de correo electrónico	Recopilan direcciones de correo electrónico almacenadas en un equipo y las envían al intruso por correo electrónico o FTP, mediante el acceso a la página web del intruso o de cualquier otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado.

- [Herramientas maliciosas](#) 

## Subcategoría: Herramientas maliciosas

### Nivel de peligrosidad: medio

A diferencia de otros tipos de software malicioso (malware), las herramientas maliciosas no llevan a cabo acciones inmediatamente después de que se inicien. Se pueden almacenar e iniciar de forma segura en el equipo del usuario. Los intrusos usan con frecuencia las funciones de estos programas para crear virus, gusanos y troyanos; perpetrar ataques de red en servidores remotos; piratear equipos o llevar a cabo otras acciones maliciosas.

Varias funciones de herramientas maliciosas se agrupan por los tipos descritos en la tabla siguiente.

Funciones de herramientas maliciosas

Tipo	Nombre	Descripción
<b>Constructor</b>	Constructores	Permiten la creación de nuevos virus, gusanos y troyanos. Algunos constructores cuentan incluso con una interfaz de ventanas estándar en la que el usuario puede seleccionar el tipo de aplicación maliciosa que creará, la forma de contrarrestar los depuradores y otras funciones.
<b>DoS</b>	Ataques de red	Envían diversas solicitudes desde el equipo del usuario a un servidor remoto. El servidor carece de los recursos necesarios para procesar todas las solicitudes, con lo que deja de funcionar (Denegación de servicio o, simplemente, DoS).
<b>Exploit</b>	Exploits	Un exploit es un conjunto de datos o un código de programa que usa las vulnerabilidades de la aplicación en la que se procesa para llevar a cabo una acción maliciosa en un equipo. Por ejemplo, un exploit puede escribir o leer archivos, así como solicitar páginas web "infectadas".

		<p>Los exploits utilizan las vulnerabilidades de distintas aplicaciones o servicios de red. Disfrazado como paquete de red, un exploit se transfiere a través de la red a diversos equipos. Busca equipos con servicios de red vulnerables. Un exploit en un archivo DOC usa las vulnerabilidades de un editor de textos. Puede comenzar a ejecutar las acciones preprogramadas por el pirata cuando el usuario abra el archivo infectado. Un exploit incrustado en un mensaje de correo electrónico busca vulnerabilidades en cualquier cliente de correo electrónico. Puede empezar a realizar acciones maliciosas en cuanto el usuario abra el mensaje infectado en este cliente de correo electrónico.</p> <p>Los Net-Worms se propagan por las redes mediante exploits. Los exploits <i>Nuker</i> son paquetes de red que desactivan equipos.</p>
<b>FileCryptor</b>	Cifradores	Cifran otras aplicaciones maliciosas para ocultarlas frente a las aplicaciones antivirus.
<b>Flooder</b>	Programas para contaminar redes	<p>Envían un gran número de mensajes a través de canales de red. Este tipo de herramientas incluye, por ejemplo, los programas que "contaminan" Internet Relay Chats.</p> <p>Las herramientas de tipo Flooder no incluyen programas que "contaminan" los canales que usa el correo electrónico, los clientes de MI y los sistemas de comunicación móvil. Estos programas se distinguen como los distintos tipos que se describen en esta tabla (Email-Flooder, IM-Flooder y SMS-Flooder).</p>
<b>HackTool</b>	Herramientas de pirateo	Permiten hackear el equipo en el que están instalados o atacar a otro equipo (por ejemplo, añadiendo nuevas cuentas de sistema sin el permiso del usuario o borrando los registros del sistema para ocultar los rastros de su presencia en el sistema operativo). Este tipo de herramientas incluye sniffers, que incluyen funciones maliciosas, como la interceptación de contraseñas. Los sniffers son programas que permiten la visualización del tráfico de la red.
<b>Hoax</b>	Hoaxes	Avisan al usuario con mensajes parecidos a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario que el disco se ha formateado, aunque no haya sucedido en realidad.

<b>Spoofeer</b>	Herramientas de spoofing	Envían mensajes y solicitudes de red con una dirección de remitente falsa. Los intrusos usan herramientas del tipo Spoofeer para pasar como los verdaderos remitentes del mensaje, por ejemplo.
<b>VirTool</b>	Herramientas que modifican aplicaciones maliciosas	Permiten la modificación de otros programas de software malicioso (malware) para ocultarlos de las aplicaciones antivirus.
<b>Email-Flooder</b>	Programas que "contaminan" direcciones de correo electrónico	Envían diversos mensajes a varias direcciones de correo electrónico y las "contaminan" de ese modo. Un gran volumen de mensajes entrantes impide a los usuarios ver los mensajes útiles en la bandeja de entrada.
<b>IM-Flooder</b>	Programas que "contaminan" el tráfico de clientes de MI	Inundan a los usuarios de clientes de MI con mensajes. El gran volumen de mensajes impide que los usuarios vean los mensajes entrantes útiles.
<b>SMS-Flooder</b>	Programas que "contaminan" el tráfico con mensajes SMS	Envían un gran número de mensajes SMS a teléfonos móviles.

- [Software publicitario](#) 

**Subcategoría:** software publicitario (adware)

**Nivel de amenaza:** medio

El software publicitario (adware) muestra información publicitaria al usuario. El software publicitario (adware) muestra anuncios publicitarios en la interfaz de otros programas y dirige las búsquedas a páginas web de publicidad. Algunos de ellos recopilan información de marketing del usuario y la envían al desarrollador. Esta información puede incluir los nombres de los sitios web que visita el usuario o el contenido de sus búsquedas. A diferencia de los programas del tipo Trojan-Spy, el software publicitario (adware) envía esta información al desarrollador con el permiso del usuario.

- [Marcadores automáticos \(auto-dialers\)](#) 



**Subcategoría:** Software legal que pueden utilizar los delincuentes para dañar su equipo o datos personales.

**Nivel de peligrosidad:** medio

La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de Internet para FTP, HTTP y Telnet.

No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
<b>Client-IRC</b>	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).
<b>Marcadores</b>	Marcadores automáticos (auto-dialers)	Pueden establecer conexión telefónica a través de un módem en modo oculto.
<b>Descargador</b>	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
<b>Monitor</b>	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
<b>PSWTool</b>	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
<b>RemoteAdmin</b>	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisar y gestionarlo. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos.

		Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
<b>Server-FTP</b>	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
<b>Server-Proxy</b>	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>Server-Telnet</b>	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.
<b>Server-Web</b>	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
<b>RiskTool</b>	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
<b>NetTool</b>	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
<b>Client-P2P</b>	Clientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
<b>Client-SMTP</b>	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>WebToolbar</b>	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
<b>FraudTool</b>	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran

		mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.
--	--	---

- Detectar otro software que los intrusos pueden usar para dañar su equipo o sus datos personales 

**Subcategoría:** Software legal que pueden utilizar los delincuentes para dañar su equipo o datos personales.

**Nivel de peligrosidad:** medio

La mayoría de estas aplicaciones son muy útiles, por lo que hay muchos usuarios que las utilizan. Entre estas aplicaciones se incluyen los clientes IRC, marcadores automáticos, programas de descarga de archivos, monitores de actividad de sistemas informáticos, herramientas de contraseña y servidores de Internet para FTP, HTTP y Telnet.

No obstante, si los intrusos obtienen acceso a estos programas o si los instalan en el equipo del usuario, las funciones de la aplicación se pueden usar para infringir la seguridad.

Dichas aplicaciones difieren en sus funciones; los tipos se describen en la siguiente tabla.

Tipo	Nombre	Descripción
<b>Client-IRC</b>	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar a través de Internet Relay Chats. Los intrusos los usan para propagar el software malicioso (malware).
<b>Marcadores</b>	Marcadores automáticos (auto-dialers)	Pueden establecer conexión telefónica a través de un módem en modo oculto.
<b>Descargador</b>	Programas de descargas	Pueden descargar archivos de páginas web en modo oculto.
<b>Monitor</b>	Programas de supervisión	Permiten supervisar la actividad en el equipo en el que se instalan (ver qué aplicaciones están activas y cómo intercambian datos con las aplicaciones que instaladas en otros equipos).
<b>PSWTool</b>	Restauradores de contraseñas	Permiten ver y restaurar contraseñas olvidadas. Los intrusos se instalan en los equipos de los usuarios en secreto con el mismo propósito.
<b>RemoteAdmin</b>	Programas de administración remota	Los usan de forma generalizada los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisar y gestionarlo. Los intrusos se implantan en secreto en los equipos de los usuarios con el mismo objetivo: supervisar y administrar equipos remotos.

		Los programas legales de administración remota difieren de los troyanos del tipo puerta trasera para administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo de forma independiente y autoinstalarse; los programas legales no la tienen.
<b>Server-FTP</b>	Servidores FTP	Funcionan como servidores FTP. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del FTP.
<b>Server-Proxy</b>	Servidores proxy	Funcionan como servidores proxy. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>Server-Telnet</b>	Servidores Telnet	Funcionan como servidores telnet. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través de telnet.
<b>Server-Web</b>	Servidores web	Funcionan como servidores web. Los intrusos se instalan en el equipo del usuario para abrir un acceso remoto a él a través del HTTP.
<b>RiskTool</b>	Herramientas para trabajar en un equipo local	Ofrecen al usuario opciones adicionales cuando se trabaja en el equipo del usuario. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas, así como finalizar procesos activos.
<b>NetTool</b>	Herramientas de red	Ofrecen al usuario opciones adicionales cuando se trabaja en otros equipos de la red. Con estas herramientas, se pueden reiniciar, detectar puertos abiertos e iniciar aplicaciones que estén instaladas en otros equipos.
<b>Client-P2P</b>	Cientes de redes P2P	Permiten el trabajo en redes de punto a punto. Pueden usarlas los intrusos para propagar software malicioso (malware).
<b>Client-SMTP</b>	Cientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos se instalan en el equipo del usuario para enviar correo no deseado con el nombre del usuario.
<b>WebToolbar</b>	Barras de herramientas web	Añaden barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
<b>FraudTool</b>	Seudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen falsos programas antivirus que muestran

		mensajes sobre la detección de software malicioso (malware). No obstante, en realidad, no encuentran ni desinfectan nada.
--	--	---

- [Objetos comprimidos cuya compresión puede usarse para proteger código malicioso](#) 

Kaspersky Endpoint Security analiza objetos comprimidos y el módulo de descompresión de los archivos SFX (autoextraíbles).

Para ocultar archivos peligrosos de las aplicaciones antivirus, los intrusos los archivan usando compresores especiales o creando archivos comprimidos varias veces.

Los analistas de virus de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

Si Kaspersky Endpoint Security detecta este tipo compresor en un archivo, es muy probable que dicho archivo contenga una aplicación maliciosa o una aplicación que los delincuentes pueden utilizar para dañar el equipo o sus datos personales.

Kaspersky Endpoint Security identifica los siguientes tipos de programas:

- *Archivos comprimidos que pueden causar daños*: se utilizan para comprimir malware, como virus, gusanos y troyanos.
- *Archivos comprimidos varias veces* (nivel de amenaza medio): han comprimido tres veces el objeto usando uno o varios programas compresores.

- [Objetos comprimidos varias veces](#) 

Kaspersky Endpoint Security analiza objetos comprimidos y el módulo de descompresión de los archivos SFX (autoextraíbles).

Para ocultar archivos peligrosos de las aplicaciones antivirus, los intrusos los archivan usando compresores especiales o creando archivos comprimidos varias veces.

Los analistas de virus de Kaspersky han identificado los compresores más conocidos entre los piratas informáticos.

Si Kaspersky Endpoint Security detecta este tipo compresor en un archivo, es muy probable que dicho archivo contenga una aplicación maliciosa o una aplicación que los delincuentes pueden utilizar para dañar el equipo o sus datos personales.

Kaspersky Endpoint Security identifica los siguientes tipos de programas:

- *Archivos comprimidos que pueden causar daños*: se utilizan para comprimir malware, como virus, gusanos y troyanos.
- *Archivos comprimidos varias veces* (nivel de amenaza medio): han comprimido tres veces el objeto usando uno o varios programas compresores.

## Exclusiones

Esta tabla contiene información sobre las exclusiones del análisis.

Para excluir objetos de los análisis, puede usar los siguientes métodos:

- Especificar la ruta al archivo o la carpeta que desea excluir.
- Introducir el hash del objeto que desea excluir.
- Usar máscaras:
  - El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en la unidad C:, pero no en las subcarpetas
  - Dos caracteres `**` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT que se encuentren en la carpeta llamada `Carpeta` y en cualquiera de sus subcarpetas. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
  - El carácter `?` (signo de interrogación), que toma el lugar de cualquier carácter único, excepto los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Carpeta` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

	<ul style="list-style-type: none"> <li>• Introduzca el nombre del objeto según la clasificación de la <a href="#">Enciclopedia de Kaspersky</a> (por ejemplo, Email-Worm, Rootkit o RemoteAdmin). Se pueden usar máscaras con el carácter <code>?</code> (sustituye cualquier carácter único) y el carácter <code>*</code> (sustituye cualquier número de caracteres). Por ejemplo, si se especifica la máscara <code>Cliente*</code>, Kaspersky Endpoint Security excluye los objetos <code>Client-IRC</code>, <code>Client-P2P</code> y <code>Client-SMTP</code> de los análisis.</li> </ul>
<b>Aplicaciones de confianza</b>	<p>Esta tabla enumera las aplicaciones de confianza cuya actividad no supervisa Kaspersky Endpoint Security cuando está en funcionamiento.</p> <p>El componente Control de aplicaciones regula el inicio de cada una de las aplicaciones independientemente de si la aplicación está incluida en la tabla de aplicaciones de confianza.</p>
<b>Fusionar valores al heredar</b>  <i>(disponible solo en la Consola de Kaspersky Security Center)</i>	<p>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.</p> <p>Si la casilla de verificación está seleccionada, los elementos de la lista de la directiva principal de Kaspersky Security Center se muestran en las directivas secundarias. De esta manera, puede, por ejemplo, crear una lista consolidada de aplicaciones de confianza para toda la organización.</p> <p>Los elementos de lista heredados de una directiva secundaria no se pueden eliminar ni editar. Los elementos de la lista de exclusiones de análisis y la lista de aplicaciones de confianza que se fusionan durante la herencia se pueden eliminar y editar solo en la directiva principal. Puede añadir, modificar o eliminar elementos de la lista en las directivas de nivel inferior.</p> <p>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.</p> <p>Si la casilla de verificación no está seleccionada, los elementos de las listas no se combinan al heredar la configuración de las directivas de Kaspersky Security Center.</p>
<b>Permitir el uso de exclusiones locales/Permitir el uso de aplicaciones locales de confianza</b>  <i>(disponible solo en la Consola de Kaspersky Security Center)</i>	<p><i>Exclusiones locales y aplicaciones de confianza locales (zona de confianza local):</i> 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 <a href="#">crear sus propias listas locales de exclusiones y aplicaciones de confianza</a>, además de la zona de confianza general en una directiva.</p> <p>Si la casilla de verificación está seleccionada, un usuario puede crear una lista local de exclusiones de análisis y una lista local de aplicaciones de confianza. Un administrador puede usar Kaspersky Security Center para ver, añadir, editar o eliminar elementos de la lista en las propiedades del equipo.</p> <p>Si la casilla de verificación está desmarcada, un usuario puede acceder solo a las listas generales de exclusiones de análisis y aplicaciones de confianza generadas en la directiva. Si se generaron listas locales, después de desactivar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los objetos enumerados de los análisis.</p>
<b>Almacén de confianza de certificados del sistema</b>	<p>Si se selecciona uno de las tiendas de certificados de sistemas de confianza, Kaspersky Endpoint Security excluye de los análisis las aplicaciones firmadas con una firma digital de confianza. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al Grupo de <i>confianza</i>.</p>



Si se selecciona **No utilizar**, Kaspersky Endpoint Security analiza las aplicaciones independientemente de si tienen o no una firma digital. Kaspersky Endpoint Security coloca una aplicación en un grupo de confianza en función del nivel de peligro que presente dicha aplicación para el equipo.

## Configuración de la aplicación

En este paso, configure los siguientes ajustes generales de la aplicación:

- Modo de funcionamiento
- Autoprotección
- Rendimiento
- Información de depuración
- Estado del equipo cuando la configuración está aplicada

### Configuración de la aplicación

Parámetro	Descripción
<b>Ejecutar Kaspersky Endpoint Security para Windows al iniciarse el equipo</b>	<p>Cuando se selecciona la casilla de verificación, Kaspersky Endpoint Security se inicia después de la carga del sistema operativo, lo que permite proteger el equipo durante la sesión completa.</p> <p>Cuando se desactiva la casilla de verificación, Kaspersky Endpoint Security no se inicia tras la carga del sistema operativo hasta que el usuario lo inicia de forma manual. La protección del equipo se desactiva y los datos del usuario pueden verse expuestos a amenazas.</p>
<b>Usar tecnología de Desinfección avanzada (requiere varios recursos informáticos)</b>	<p>Cuando la casilla está seleccionada y se detecta actividad maliciosa en el sistema operativo, aparece una notificación emergente en la pantalla. En su notificación, Kaspersky Endpoint Security permite al usuario realizar la desinfección avanzada del equipo. Una vez que el usuario aprueba este procedimiento, Kaspersky Endpoint Security neutraliza la amenaza. Una vez completado el proceso de desinfección avanzada, Kaspersky Endpoint Security reinicia el equipo. La tecnología de desinfección avanzada emplea un número considerable de recursos del equipo, lo que puede ralentizar el resto de las aplicaciones.</p> <p>Cuando la aplicación se encuentra en proceso de detectar una infección activa, es posible que algunas funcionalidades del sistema operativo no estén disponibles. La disponibilidad del sistema operativo se restablece tras la finalización de la Desinfección avanzada y el reinicio del ordenador.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Si Kaspersky Endpoint Security se instala en un equipo en el que se ejecuta Windows para servidores, Kaspersky Endpoint Security no muestra la notificación. Por lo tanto, el usuario no puede seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe <a href="#">activar la tecnología de Desinfección avanzada</a> en la configuración de la aplicación y <a href="#">activar la Desinfección avanzada de inmediato</a> en la configuración de la tarea <i>Análisis antivirus</i>. Luego, debe iniciar la tarea <i>Análisis antivirus</i>.</p> </div>
<b>Usar</b>	Si se selecciona esta casilla, el Servidor de administración de Kaspersky Security

<p><b>Kaspersky Security Center como servidor proxy para la activación</b></p> <p><i>(disponible solo en la Consola de Kaspersky Security Center)</i></p>	<p>Center se usa como servidor proxy al activar la aplicación.</p>
<p><b>Activar la autoprotección</b></p>	<p>Cuando se selecciona esta casilla de verificación, Kaspersky Endpoint Security impide la modificación o eliminación de los archivos de la aplicación el disco duro, los procesos de memoria y las entradas en el Registro del sistema.</p>
<p><b>Autorizar la administración de la configuración de Kaspersky Endpoint Security a través de aplicaciones de control remoto</b></p>	<p>Si la casilla de verificación está seleccionada, las aplicaciones de administración remota de confianza (como TeamViewer, LogMeln Pro y Remotely Anywhere) pueden modificar la configuración de Kaspersky Endpoint Security.</p> <p>Las aplicaciones de administración remota que no son de confianza tienen prohibido modificar la configuración de Kaspersky Endpoint Security incluso cuando la casilla de verificación está seleccionada.</p>
<p><b>Activar el control remoto de servicios</b></p>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security permite administrar los servicios de aplicaciones desde un equipo remoto. Cuando se intenta administrar los servicios de aplicaciones de forma remota, aparece una notificación en la barra de tareas de Microsoft Windows, encima del icono de la aplicación (a menos que el usuario haya desactivado el servicio de notificaciones).</p>
<p><b>Posponer tareas planificadas al funcionar con batería</b></p>	<p>Si se selecciona la casilla de verificación, se activa el modo de conservación de energía. Kaspersky Endpoint Security pospone las tareas planificadas. Las tareas de análisis y actualización podrán iniciarse manualmente cuando sea necesario.</p>
<p><b>Facilitar recursos para otras aplicaciones</b></p>	<p>Cuando Kaspersky Endpoint Security realiza tareas planificadas, puede provocar un aumento en la carga de trabajo de la CPU y los subsistemas del disco, lo que ralentiza el rendimiento de otras aplicaciones.</p> <p>Cuando se selecciona la casilla de verificación, Kaspersky Endpoint Security suspende las tareas planificadas si detecta un aumento en la carga y libera recursos del sistema operativo para las aplicaciones del usuario.</p>
<p><b>Activar escritura de volcado</b></p>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security escribe volcados cuando se producen fallos generales.</p> <p>Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no escribe volcados. La aplicación también elimina los archivos de volcado existentes del disco duro del equipo.</p>
<p><b>Activar la protección de los archivos de volcado y de rastreo</b></p>	<p>Si se activa esta casilla, podrán acceder a los archivos de volcado el administrador del sistema, el administrador local y el usuario que haya habilitado la creación de dichos archivos. Solo el sistema y los administradores locales pueden acceder a los archivos de trazas.</p> <p>Si se desactiva, cualquier usuario puede acceder a los archivos de volcado y de trazas.</p>
<p><b>Estado del</b></p>	<p>Opciones para mostrar, en Web Console, los estados de los equipos cliente con</p>

**equipo cuando la configuración está aplicada**

*(disponible solo en la Consola de Kaspersky Security Center)*

Kaspersky Endpoint Security instalado cuando ocurran errores al aplicar una directiva o ejecutar una tarea. Los estados disponibles son *Sin inconvenientes*, *Advertencia* y *Crítico*.

## Informes y almacenamiento

### Informes

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la ejecución de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se registra en informes.

Los informes se almacenan en la carpeta C:\ProgramData\Kaspersky Lab\KES\Report.

### Copia de seguridad

*Copias de seguridad* almacena copias de seguridad de los archivos que se modificaron o eliminaron durante la desinfección. Una *copia de seguridad* es una copia del archivo creada antes de que el archivo se desinfectara o se eliminara. Las copias de seguridad de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

Las copias de seguridad de los archivos se almacenan en la carpeta C:\ProgramData\Kaspersky Lab\KES\QB.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. El usuario cuya cuenta se usó para instalar la Kaspersky Endpoint Security tiene derechos de acceso limitado a esta carpeta.

Kaspersky Endpoint Security no ofrece la posibilidad de configurar permisos de acceso de usuario a copias de seguridad de los archivos.

### Cuarentena

La *cuarentena* es un almacén local especial en el equipo donde se envían los archivos infectados por virus o los archivos no desinfectables. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security usa la cuarentena solo cuando trabaja con las soluciones Kaspersky Sandbox y Kaspersky Endpoint 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](#) y la [Ayuda de Kaspersky Endpoint Detection and Response Expert](#).

La cuarentena solo se puede configurar mediante Web Console. También puede usar Web Console para administrar objetos en cuarentena (restaurar, eliminar, añadir, etc.). Puede restaurar objetos localmente en el equipo mediante la [línea de comandos](#).

Kaspersky Endpoint Security utiliza la cuenta del sistema (SYSTEM) para poner archivos en cuarentena.

#### Configuración de informes y almacenes

Parámetro	Descripción
<b>Conservar informes un máximo de N días</b>	Si la casilla de verificación está seleccionada, los informes se conservarán solo durante el tiempo definido como máximo. El período máximo predeterminado del almacenamiento de informes es de 30 días. Después de dicho período de tiempo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.
<b>Limitar el tamaño del archivo del informe a N MB</b>	Si la casilla de verificación está seleccionada, el tamaño máximo del archivo de informes se limitará al valor definido. De forma predeterminada, el tamaño máximo de archivo es de 1024 MB. Para evitar superar el tamaño máximo de archivo de informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo de informe cuando se alcance el tamaño máximo en el archivo de informe.
<b>Conservar objetos un máximo de N días</b>	Si la casilla de verificación está seleccionada, los archivos se conservarán solo durante el tiempo definido como máximo. El período máximo predeterminado del almacenamiento de archivos es de 30 días. Cuando venza el período máximo de almacenamiento, Kaspersky Endpoint Security eliminará los archivos más antiguos de Copia de seguridad.
<b>Limitar el tamaño de la copia de seguridad a N MB</b>	Si la casilla de verificación está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. De forma predeterminada, el tamaño máximo de archivo es de 100 MB. Cuando se alcanza el valor definido, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos para evitar que el límite se exceda.
<b>Limitar el tamaño de Cuarentena a N MB</b> <i>(disponible solo en Web Console)</i>	Tamaño máximo de cuarentena en MB. Por ejemplo, puede establecer el tamaño máximo de la cuarentena en 200 MB. Cuando la cuarentena alcanza el tamaño máximo, 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 deja de colocar nuevos objetos en cuarentena. Debe vaciar manualmente la Cuarentena.
<b>Notificar cuando el almacenamiento de la Cuarentena alcance el N por ciento</b> <i>(disponible solo en Web Console)</i>	Valor umbral de la cuarentena. Por ejemplo, puede establecer el umbral de la cuarentena en 50 %. Cuando la cuarentena alcanza el umbral, Kaspersky Endpoint Security envía el evento correspondiente a Kaspersky Security Center y publica el evento en el Registro de eventos de Windows. Mientras tanto, la aplicación continúa poniendo en cuarentena nuevos objetos.
<b>Transferencia de datos al Servidor de administración</b> <i>(disponible solo en Kaspersky Security Center)</i>	Categorías de eventos de los equipos cliente cuya información debe transmitirse al Servidor de administración.

Puede configurar los parámetros del servidor proxy utilizado para conectarse a Internet y actualizar las bases de datos antivirus, seleccionar el modo de vigilancia para los puertos de red y configurar la función de análisis de conexiones cifradas.

#### Opciones de red

Parámetro	Descripción
<b>Limitar el tráfico de las conexiones de uso medido</b>	<p>Si está seleccionada esta casilla de verificación, la aplicación reduce su propio tráfico de red cuando la conexión a Internet es limitada. Kaspersky Endpoint Security identifica la conexión a Internet móvil de alta velocidad como limitada e identifica la conexión wifi como ilimitada.</p> <p>Las redes con reconocimiento del coste funcionan en equipos con Windows 8 o posterior.</p>
<b>Insertar scripts en el tráfico web para interactuar con las páginas web</b>	<p>Si se activa la casilla de verificación, Kaspersky Endpoint Security inyecta un script de interacción con la página web en el tráfico web. Este script garantiza que el componente de Control web pueda funcionar correctamente. El script permite el registro de eventos de Control web. Sin este script, no se puede activar la <a href="#">supervisión de la actividad de Internet del usuario</a>.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>
<b>Servidor proxy</b>	<p>Configuración del servidor proxy que los usuarios de equipos cliente usan para ingresar a Internet. Kaspersky Endpoint Security utiliza estos parámetros para determinados componentes de protección, como los de actualización de bases de datos y módulos de la aplicación.</p> <p>Para la configuración automática del servidor proxy, Kaspersky Endpoint Security utiliza el protocolo WPAD (Web Proxy Auto-Discovery Protocol). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, Kaspersky Endpoint Security usa la dirección especificada en la configuración del navegador Microsoft Internet Explorer.</p>
<b>No usar servidor proxy para direcciones locales</b>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security no utiliza un servidor proxy al realizar una actualización desde una carpeta compartida.</p>
<b>Puertos vigilados</b>	<p><b>Supervisar todos los puertos de red.</b> En este modo de supervisión de puertos de red, los componentes de protección (Protección frente a amenazas en archivos, Protección frente a amenazas web y Protección frente a amenazas en el correo) supervisan los flujos de datos que se transmiten a través de los puertos de red abiertos del equipo.</p> <p><b>Vigilar solo los puertos de red seleccionados.</b> En este modo de supervisión de puertos de red, los componentes de protección controlan los puertos seleccionados del equipo y la actividad de red de las aplicaciones seleccionadas. La lista de puertos de red que normalmente se utilizan para transmitir correo electrónico y otras clases de tráfico se configura siguiendo las recomendaciones de los expertos de Kaspersky.</p> <p><b>Supervisar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky.</b> Esto utiliza una lista de aplicaciones predefinidas cuyos puertos de red son supervisados por Kaspersky Endpoint Security. Por ejemplo, esta lista incluye Google Chrome, Adobe Reader, Java y otras aplicaciones.</p> <p><b>Supervisar todos los puertos de las aplicaciones especificadas.</b> Esto utiliza una lista de aplicaciones cuyos puertos de red son supervisados por Kaspersky Endpoint Security.</p>

<p><b>Análisis de conexión cifrada</b></p>	<p>Kaspersky Endpoint Security analiza el tráfico de red cifrado que se transmite a través de los siguientes protocolos:</p> <ul style="list-style-type: none"> <li>• SSL 3.0</li> <li>• TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.</li> </ul> <p>Kaspersky Endpoint Security admite los siguientes modos de análisis de conexión cifrada:</p> <ul style="list-style-type: none"> <li>• <b>No analizar las conexiones cifradas.</b> Kaspersky Endpoint Security no tendrá acceso al contenido de sitios web cuyas direcciones comiencen con <code>https://</code>.</li> <li>• <b>Analizar las conexiones cifradas cuando lo soliciten los componentes de protección.</b> Kaspersky Endpoint Security analizará el tráfico cifrado solo cuando los componentes Protección frente a amenazas en archivos, Protección frente a amenazas en el correo y Control web lo soliciten.</li> <li>• <b>Analizar conexiones cifradas siempre.</b> Kaspersky Endpoint Security analizará el tráfico de red cifrado incluso cuando los componentes de protección están desactivados.</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por <a href="#">aplicaciones de confianza para las que el análisis de tráfico está desactivado</a>. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza solo en la interfaz de Kaspersky Endpoint Security. No puede ver la lista en la Consola de Kaspersky Security Center.</p> </div>
<p><b>Cuando se visite un dominio cuyo certificado no sea de confianza</b></p>	<ul style="list-style-type: none"> <li>• <b>Autorizar.</b> Cuando se elige esta opción y se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security permite que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para advertirle que acceder a ese dominio en particular no es recomendable e indicarle por qué. La página contiene un enlace para obtener acceso al recurso web solicitado. Una vez que el usuario hace clic en el enlace, dispone de una hora para visitar otros recursos alojados en el mismo dominio sin que Kaspersky Endpoint Security le advierta sobre la falta de confianza en el certificado.</li> </ul> <p><b>Bloquear conexión.</b> Cuando se elige esta opción y se visita un dominio cuyo certificado no es de confianza, Kaspersky Endpoint Security impide que se establezca la conexión de red. Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para explicarle por qué ese dominio en particular se ha bloqueado.</p>
<p><b>Si se presentan errores al analizar una conexión cifrada</b></p>	<ul style="list-style-type: none"> <li>• <b>Bloquear conexión.</b> Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red.</li> <li>• <b>Agregar dominio a exclusiones.</b> Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security añade el dominio con el que se presentó el problema a la lista de dominios con errores de análisis y deja de controlar el tráfico de red cifrado que se genera al visitarlo. La lista de dominios con errores de análisis de conexiones cifradas solo puede consultarse a través de la</li> </ul>

	<p>interfaz local de la aplicación. Para borrar el contenido de la lista, deberá seleccionar <b>Bloquear conexión</b>.</p>
<p><b>Bloquear conexiones SSL 2.0 (recomendado)</b></p>	<p>Cuando la casilla está activada, Kaspersky Endpoint Security bloquea las conexiones de red que se establecen con el protocolo SSL 2.0.</p> <p>Cuando la casilla no está activada, Kaspersky Endpoint Security no bloquea las conexiones de red que se establecen con el protocolo SSL 2.0 ni controla el tráfico que se transmite por ellas.</p>
<p><b>Descifrar conexiones cifradas con sitios web que utilizan certificados de EV</b></p>	<p>Los certificados de EV (certificados de validación extendida) confirman la autenticidad de los sitios web y mejoran la seguridad de la conexión. Cuando un sitio web cuente con un certificado de EV, verá un candado en la barra de direcciones del navegador. Es posible, además, que la barra de direcciones esté total o parcialmente sombreada en verde.</p> <p>Cuando esta casilla está activada, Kaspersky Endpoint Security descifra y controla las conexiones cifradas con sitios web que usan un certificado de EV.</p> <p>Cuando esta casilla no está activada, Kaspersky Endpoint Security no tiene acceso al contenido del tráfico HTTPS. Esto significa que la aplicación únicamente puede controlar el tráfico HTTPS sobre la base de la dirección del sitio web (por ejemplo, <code>https://google.com</code>).</p> <p>Cuando visite un sitio web con certificado de EV por primera vez, la conexión cifrada se descifrará independientemente de que la casilla esté o no activada.</p>
<p><b>Direcciones de confianza</b></p>	<p>Esto utiliza una lista de direcciones web que Kaspersky Endpoint Security omite del análisis de conexiones de red cifradas. Puede introducir un nombre de dominio o una dirección IP. Kaspersky Endpoint Security admite el carácter <code>*</code> para introducir una máscara en el nombre de dominio.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security no es compatible con las máscaras para direcciones IP. Puede introducir un rango de direcciones IP en la interfaz de la aplicación local (por ejemplo, <code>198.51.100.0/24</code>). No puede introducir un rango de direcciones IP en la consola de Kaspersky Security Center.</p> </div> <p>Ejemplos:</p> <ul style="list-style-type: none"> <li><code>domain.com</code>: el registro incluye las siguientes direcciones: <code>https://domain.com</code>, <code>https://www.domain.com</code>, <code>https://domain.com/page123</code>. El registro es exclusivo de subdominios (por ejemplo, <code>subdomain.domain.com</code>).</li> <li><code>subdomain.domain.com</code>: el registro incluye las siguientes direcciones: <code>https://subdomain.domain.com</code>, <code>https://subdomain.domain.com/page123</code>. El registro es exclusivo del dominio <code>domain.com</code>.</li> <li><code>*.domain.com</code>: el registro incluye las siguientes direcciones: <code>https://movies.domain.com</code>, <code>https://images.domain.com/page123</code>. El registro es exclusivo del dominio <code>domain.com</code>.</li> </ul>
<p><b>Aplicaciones de confianza</b></p>	<p>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 <code>*</code> y <code>?</code> al introducir una máscara.</p>

**Utilice el almacén de certificados seleccionado para analizar las conexiones cifradas en las aplicaciones de Mozilla**

*(disponible solo en la interfaz de Kaspersky Endpoint Security)*

Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security analiza el tráfico cifrado en el navegador Mozilla Firefox y el cliente de correo Thunderbird. Es posible que se bloquee el acceso a algunos sitios web a través del protocolo HTTPS.

Para analizar el tráfico en el navegador Mozilla Firefox y el cliente de correo Thunderbird, debe [activar el Análisis de conexiones cifradas](#). Si el Análisis de conexiones cifradas está desactivado, Kaspersky Endpoint Security no analiza el tráfico en el navegador Mozilla Firefox ni en el cliente de correo Thunderbird.

Kaspersky Endpoint Security utiliza el certificado raíz de Kaspersky para descifrar y analizar el tráfico cifrado. Puede seleccionar la tienda de certificados que contendrá el certificado raíz de Kaspersky.

- **Usar el almacén de certificados de Windows (recomendado).** El certificado raíz de Kaspersky se añade a esta tienda durante la instalación de Kaspersky Endpoint Security.
- **Usar la tienda de certificados de Mozilla.** Mozilla Firefox y Thunderbird utilizan sus propias tiendas de certificados. Si se selecciona la tienda de certificados de Mozilla, debe añadir manualmente el certificado raíz de Kaspersky a esta tienda a través de las propiedades del navegador.

## Interfaz

Puede configurar los ajustes de la interfaz de la aplicación.

Configuración de la interfaz

Parámetro	Descripción
<b>Interacción con el usuario</b> <i>(disponible solo en la Consola de Kaspersky Security Center)</i>	<p><b>Con la interfaz simplificada.</b> La ventana principal de la aplicación no estará disponible en el equipo cliente; únicamente se mostrará un <a href="#">icono en el área de notificación de Windows</a>. El usuario podrá <a href="#">interactuar con Kaspersky Endpoint Security en forma limitada</a> a través del menú contextual de este icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.</p> <p><b>Con la interfaz completa.</b> En un equipo cliente, se podrá acceder tanto a la ventana principal de Kaspersky Endpoint Security como al <a href="#">icono ubicado en el área de notificaciones de Windows</a>. 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.</p> <p><b>Ocultar la sección Supervisión de la actividad de aplicaciones.</b> En el equipo cliente, en la ventana principal de Kaspersky Endpoint Security, el botón <b>Supervisión de la actividad de aplicaciones</b> no está disponible. <i>Supervisión de la Actividad de Aplicaciones</i> es una herramienta diseñada para ver información sobre la actividad de las aplicaciones en el equipo de un usuario en tiempo real.</p> <p><b>Sin interfaz.</b> No habrá ninguna indicación en el equipo cliente de que Kaspersky Endpoint Security está en funcionamiento. El <a href="#">icono del área de notificación de Windows</a> no estará disponible y tampoco se mostrará ninguna notificación.</p>
<b>Configuración de notificación</b>	<p>Tabla con la configuración de las notificaciones sobre eventos con distinto nivel de importancia que pueden producirse durante el funcionamiento de un componente, una tarea o toda una aplicación. Kaspersky Endpoint Security muestra notificaciones que informan de estos eventos en la pantalla, las envía por correo electrónico o las registra.</p>



<b>Parámetros de notificaciones por correo</b>	Parámetros del servidor SMTP con el que se enviarán las notificaciones de los eventos registrados mientras la aplicación esté en funcionamiento.
<b>Mostrar el estado de la aplicación en el área de notificaciones</b>	Categorías de eventos de la aplicación que provocan un cambio (🔒 o 📧) en el <a href="#">icono de Kaspersky Endpoint Security</a> ubicado en el área de notificación de la barra de tareas de Microsoft Windows. Dichos eventos también dan lugar a una notificación emergente.
<b>Notificaciones del estado de la base de datos de antivirus local</b>	Ajustes de las notificaciones sobre bases de datos de antivirus obsoletas utilizadas por la aplicación.
<b>Protección con contraseña</b>	<p>Cuando este interruptor está activado y el usuario intenta realizar una acción alcanzada por la función de protección con contraseña, Kaspersky Endpoint Security solicita la contraseña en cuestión. La cobertura de la protección con contraseña se compone de las acciones que se han prohibido (por ejemplo, la desactivación de los componentes de protección) y las cuentas de usuario para las que se han prohibido tales acciones.</p> <p>Cuando habilite la protección con contraseña, Kaspersky Endpoint Security le pedirá que establezca la contraseña que se necesitará para realizar operaciones.</p>
<b>Recursos web del Soporte Técnico</b>  <i>(disponible solo en la Consola de Kaspersky Security Center)</i>	Lista de enlaces a recursos web que contienen información sobre el Soporte técnico de Kaspersky Endpoint Security. Los enlaces añadidos se muestran en la ventana <b>Soporte</b> de la interfaz local de Kaspersky Endpoint Security en lugar de los enlaces predeterminados.
<b>Mensaje al usuario</b>  <i>(disponible solo en la Consola de Kaspersky Security Center)</i>	Mensaje que se muestra en la ventana <b>Soporte</b> de la interfaz local de Kaspersky Endpoint Security.

## Administrar configuración

Puede guardar la configuración actual de Kaspersky Endpoint Security en un archivo y usarla para configurar rápidamente la aplicación en un equipo diferente. También puede utilizar un archivo de configuración al implementar la aplicación a través de Kaspersky Security Center 12 con un [paquete de instalación](#). Puede restaurar la configuración predeterminada en cualquier momento.

Los ajustes de administración de la configuración de la aplicación solo están disponibles en la interfaz de Kaspersky Endpoint Security.

Configuración	Descripción
<b>Importar</b>	Extraer la configuración de la aplicación de un archivo en formato CFG y aplicarla.
<b>Exportar</b>	Guardar la configuración actual de la aplicación a un archivo en formato CFG.
<b>Restaurar</b>	Puede restaurar la configuración recomendada por Kaspersky para Endpoint Security en cualquier momento. Cuando se restablece la configuración, el nivel de seguridad <b>Recomendado</b> se establece para todos los componentes de protección.

## Actualización de las bases de datos y módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

Las actualizaciones regulares requieren una licencia efectiva. Si no hay ninguna licencia actual, solamente podrá realizar una actualización una vez.

El origen principal de actualizaciones para Kaspersky Endpoint Security son los servidores de actualizaciones de Kaspersky.

Su equipo debe estar conectado a Internet para descargar satisfactoriamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. De forma predeterminada, los parámetros de conexión a Internet se determinan automáticamente. Si utiliza un servidor proxy, debe ajustar la configuración del servidor proxy.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTP.

Mientras se lleva a cabo la actualización, se descargan e instalan los siguientes objetos en su equipo:

- **Bases de datos de Kaspersky Endpoint Security.** La protección del equipo se proporciona por medio de bases de datos que contienen firmas de virus y otras amenazas, así como información sobre la forma de neutralizarlas. Los componentes de protección emplean esta información a la hora de buscar y neutralizar archivos infectados en el equipo. Las bases de datos se actualizan constantemente con registros de nuevas amenazas y métodos para combatirlas. Por tanto, es recomendable que actualice la base de datos con regularidad.  
Además de las bases de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de protección interceptar el tráfico de la red.
- **Módulos de la aplicación.** Aparte de las bases de datos de Kaspersky Endpoint Security, también puede actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación sirve para solucionar vulnerabilidades en Kaspersky Endpoint Security, añade nuevas funciones o mejora las existentes.

Durante una actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con los de la versión actualizada en el origen de actualizaciones. Si los módulos de la aplicación y las bases de datos actuales son diferentes de sus respectivas versiones actualizadas, la parte de las actualizaciones que falte se instala en su equipo.

Los archivos de ayuda contextual se pueden actualizar junto con las actualizaciones de los módulos de la aplicación.

Si las bases de datos no están actualizadas, puede que el tamaño del paquete de actualización sea considerable, lo que provocaría un tráfico de Internet adicional (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en la ventana principal de la aplicación o en la información sobre herramientas que ve cuando pasa el cursor sobre el icono de la aplicación en el área de notificación.

La información sobre los resultados de la actualización y sobre todos los eventos se producen durante la ejecución de la tarea de actualización se registra en el [informe de Kaspersky Endpoint Security](#).

Configuración de actualización de base de datos y módulo de aplicación

Parámetro	Descripción
<b>Programación de la actualización de bases de datos</b>	<p><b>Automáticamente.</b> En este modo, Kaspersky Endpoint Security comprueba el origen de actualizaciones con cierta frecuencia en busca de nuevos paquetes de actualización. La frecuencia de las comprobaciones para ver si hay paquetes de actualización aumenta durante los brotes de virus y disminuye cuando no hay brotes. Tras detectar un paquete de actualización nuevo, Kaspersky Endpoint Security lo descarga e instala las actualizaciones en su equipo.</p> <p><b>Manual.</b> Este modo de ejecución de la tarea de actualización permite iniciar la tarea de actualización de forma manual.</p> <p><b>Según programación.</b> En este modo de ejecución de la tarea de actualización, Kaspersky Endpoint Security ejecuta la tarea de actualización en función de la planificación especificada. Si está seleccionado este modo de ejecución de la tarea de actualización, también puede iniciar la tarea de actualización de Kaspersky Endpoint Security manualmente.</p>
<b>Ejecutar tareas no realizadas</b>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security inicia la tarea de actualización omitida lo antes posible. La tarea de actualización se puede omitir, por ejemplo, si el equipo se apagó en el momento de inicio de la tarea de actualización.</p> <p>Si se desactiva esta casilla de verificación, Kaspersky Endpoint Security no inicia las tareas de actualización omitidas. En lugar de ello, ejecuta la siguiente tarea de actualización de acuerdo con la planificación actual.</p>
<b>Origen de actualizaciones</b>	<p>Un <i>origen de actualizaciones</i> es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security.</p> <p>Las fuentes de las actualizaciones incluyen el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky y carpetas locales y en red.</p> <p>La lista predeterminada de orígenes de actualizaciones incluye los servidores de actualizaciones de Kaspersky Security Center y Kaspersky. Puede añadir a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security no es compatible con las actualizaciones de los servidores HTTPS a menos que sean servidores de actualizaciones de Kaspersky.</p> </div> <p>Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno después de otro, empieza desde el inicio de la lista y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible.</p>
<b>Ejecutar actualizaciones</b>	<p>De forma predeterminada, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta se ha utilizado para iniciar la sesión en el sistema</p>

<p><b>de bases de datos como</b></p>	<p>operativo. Sin embargo, Kaspersky Endpoint Security se podría actualizar desde un origen de actualizaciones al que el usuario no pueda acceder debido a la falta de los permisos necesarios (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o un origen de actualizaciones para el que no se haya configurado la autenticación del servidor proxy. En la configuración de Kaspersky Endpoint Security, puede especificar un usuario que tenga esos permisos e iniciar la tarea de actualización de Kaspersky Endpoint Security con la cuenta de ese usuario.</p>
<p><b>Descargar actualizaciones de los módulos de la aplicación</b></p>	<p>Esta casilla de verificación activa o desactiva las descargas de las actualizaciones de los módulos de la aplicación y las actualizaciones de la base de datos de antivirus.</p> <p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security informa al usuario sobre actualizaciones disponibles de los módulos de la aplicación e incluye actualizaciones de estos en el paquete de actualización mientras ejecuta la tarea. La manera en la que se aplican las actualizaciones de los módulos de la aplicación está determinada por la configuración siguiente:</p> <ul style="list-style-type: none"> <li>• <b>Instalar actualizaciones críticas y aprobadas.</b> Si se selecciona esta opción, cuando las actualizaciones de los módulos de la aplicación están disponibles, Kaspersky Endpoint Security instala automáticamente las actualizaciones críticas y todas las demás únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center.</li> <li>• <b>Instalar solo actualizaciones aprobadas.</b> Si se selecciona esta opción, cuando están disponibles las actualizaciones de los módulos de la aplicación, Kaspersky Endpoint Security las instala únicamente después de que se apruebe su instalación de forma local a través de la interfaz de la aplicación o Kaspersky Security Center. Esta opción está seleccionada de forma predeterminada.</li> </ul> <p>Si se desactiva la casilla de verificación, Kaspersky Endpoint Security no informa al usuario sobre actualizaciones disponibles de los módulos de la aplicación ni incluye actualizaciones de estos en el paquete de actualización mientras ejecuta la tarea.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia de usuario final, la aplicación instala las actualizaciones después de que se hayan aceptado dichos términos.</p> </div> <p>Esta casilla de verificación está seleccionada de forma predeterminada.</p>
<p><b>Copiar las actualizaciones a la carpeta</b></p>	<p>Si se selecciona esta casilla, Kaspersky Endpoint Security copia el paquete de actualización en la carpeta compartida especificada bajo la casilla. Después, el resto de los equipos de su LAN pueden acceder al paquete de actualización a través de esta carpeta compartida. Reduce el tráfico de Internet dado que el paquete de actualización se descarga únicamente una vez. La carpeta especificada por defecto es C:\ProgramData\Kaspersky Lab\KES\Update distribution\.</p>
<p><b>Servidor proxy para actualizaciones</b> <i>(disponible solo en la interfaz de Kaspersky Endpoint Security)</i></p>	<p>Configuración del servidor proxy para el acceso a Internet de los usuarios de los equipos de clientes para actualizar los módulos de la aplicación y las bases de datos.</p> <p>Para la configuración automática del servidor proxy, Kaspersky Endpoint Security utiliza el protocolo WPAD (Web Proxy Auto-Discovery Protocol). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, Kaspersky Endpoint Security usa la dirección del servidor especificada en la configuración del navegador Microsoft Internet Explorer.</p>
<p><b>No usar servidor proxy para</b></p>	<p>Si se selecciona la casilla de verificación, Kaspersky Endpoint Security no utiliza un servidor proxy al realizar una actualización desde una carpeta compartida.</p>

**direcciones  
locales**

*(disponible solo  
en la interfaz de  
Kaspersky  
Endpoint  
Security)*

## Apéndice 2. Grupos de confianza de aplicaciones

Kaspersky Endpoint Security clasifica todas las aplicaciones que se inician en el equipo en grupos de confianza. Dicha clasificación se realiza en grupos de confianza en función del nivel de peligro que las aplicaciones presentan para el sistema operativo.

Los grupos de confianza son los siguientes:

- **De confianza.** Este grupo incluye aplicaciones para las que se cumplen una o varias de las siguientes condiciones:
  - Aplicaciones firmadas digitalmente por proveedores de confianza.
  - Aplicaciones registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto aplicaciones en el grupo De confianza.

No hay operaciones prohibidas para dichas aplicaciones.

- **Restricción mínima.** Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - Aplicaciones no firmadas digitalmente por proveedores de confianza.
  - Aplicaciones no registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto aplicaciones en el grupo Restricción mínima.

Dichas aplicaciones están sujetas a restricciones mínimas de acceso a los recursos del sistema operativo.

- **Restricción máxima.** Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - Aplicaciones no firmadas digitalmente por proveedores de confianza.
  - Aplicaciones no registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
  - El usuario ha puesto aplicaciones en el grupo Restricción máxima.

Dichas aplicaciones están sujetas a un nivel alto de restricción en el acceso a los recursos del sistema operativo.

- **No confiable.** Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - Aplicaciones no firmadas digitalmente por proveedores de confianza.

- Aplicaciones no registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network.
- El usuario ha puesto aplicaciones en el grupo No confiable.

Para estas aplicaciones, todas las operaciones están bloqueadas.

## Apéndice 3. Extensiones de archivo para el análisis rápido de unidades extraíbles

com: archivo ejecutable de una aplicación no superior a 64 KB

exe: archivo ejecutable o archivo comprimido autoextraíble

sys: archivo del sistema de Microsoft Windows

prg: texto de programas como dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin: archivo binario

bat: archivo de lotes

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para DOS), OS/2

dpl: biblioteca comprimida de Borland Delphi

dll: biblioteca de enlaces dinámicos

scr: pantalla de presentación en Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto Microsoft OLE (Object Linking and Embedding)

tsp: programa ejecutable en modo de tiempo fraccionado

drv: controlador de dispositivo

vx: controlador de dispositivo virtual de Microsoft Windows

pif: archivo de información de programa

lnk: archivo de acceso directo de Microsoft Windows

reg: archivo clave para el Registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de instalación para Microsoft Windows, Windows NT y ciertas aplicaciones

cla: clase Java

vbs: script Visual Basic®

vbe: extensión de vídeo del BIOS

js, jse: texto de origen JavaScript

htm: documento hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta: programa hipertexto para Microsoft Internet Explorer®

asp: secuencia de comandos Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script PHP integrado en archivos HTML

wsh: archivo de configuración de Microsoft Windows Script Host

wsf: script Microsoft Windows

the: papel tapiz del escritorio de Microsoft Windows 95

hlp: archivo de Ayuda de Microsoft Windows

eml: mensaje de correo de Microsoft Office Outlook Express

nws: mensaje de noticias de Microsoft Outlook Express

msg: mensaje de correo de Microsoft Mail

plg: mensaje de correo

mbx: mensajes de correo de Microsoft Office Outlook guardado

doc\*: documentos de Microsoft Office Word, como doc (Microsoft Office Word), docx (Microsoft Office Word 2007 con compatibilidad con XML) y docm (Microsoft Office Word 2007 con compatibilidad para macros)

dot\*: plantilla de documento de Microsoft Office Word, como: dot para plantillas de documento de Microsoft Office Word; dotx para plantillas de documento Microsoft Office Word 2007, y dotm para plantilla de documento Microsoft Office Word 2007 con soporte para macros

fpm: programa de bases de datos, archivo de inicio para Microsoft Visual FoxPro

rtf: documento en formato de texto enriquecido (Rich Text Format)

shs: fragmento de identificador de objeto de recorte de Shell de Windows

dwg: base de datos de dibujos de AutoCAD®

msi: paquete de instalación de Microsoft Windows Installer

otm: proyecto VBA para Microsoft Office Outlook

pdf: documento Adobe Acrobat

swf: objeto empaquetado Shockwave® Flash

jpg, jpeg: formato gráfico para imágenes comprimidas

emf: formato de metadatos ampliado

ico: archivo de icono

ov?: Archivos ejecutables de Microsoft Office Word

xl\*: documentos de Microsoft Office Excel y archivos como: xla, la extensión para Microsoft Office Excel; xlc para diagramas; xlt para plantillas de documentos; xlsx para libros de trabajo de Microsoft Office Excel 2007; xltm para libros de trabajo de Microsoft Office Excel 2007 con compatibilidad para macros; xlsb para libros de trabajo de Microsoft Office Excel 2007 en formato binario (no XML); xltx para plantillas de Microsoft Office Excel 2007; xlsx para plantillas de Microsoft Office Excel 2007 con compatibilidad para macros, y xlsm para complementos de Microsoft Office Excel 2007 con compatibilidad para macros

pp\*: documentos y archivos de Microsoft Office PowerPoint®, como: pps para diapositivas de Microsoft Office PowerPoint; ppt para presentaciones; pptx para presentaciones de Microsoft Office PowerPoint 2007; pptm para presentaciones de Microsoft Office PowerPoint 2007 con compatibilidad para macros; potx para plantillas de presentación de Microsoft Office PowerPoint 2007; potm para plantillas de presentación de Microsoft Office PowerPoint 2007 con compatibilidad para macros; ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007; ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 con compatibilidad para macros, y ppam para complementos de Microsoft Office PowerPoint 2007 con compatibilidad para macros

md\*: documentos y archivos de Microsoft Office Access® como mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: diapositivas Microsoft PowerPoint 2007

sldm: diapositivas Microsoft PowerPoint 2007 con soporte para macros

thmx: tema Microsoft Office 2007

## Apéndice 4. Tipos de archivo para el filtrado de adjuntos Protección frente a amenazas en el correo

Recuerde que el formato real de un archivo puede no corresponder al formato indicado por su extensión.

Si activa el filtro de archivos adjuntos a mensajes de correo electrónico, el componente Protección frente a amenazas en el correo podría eliminar o cambiar el nombre de los archivos con las siguientes extensiones:

com: archivo ejecutable de una aplicación no superior a 64 KB

exe: archivo ejecutable o archivo comprimido autoextraíble



sys: archivo del sistema de Microsoft Windows

prg: texto de programas como dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin: archivo binario

bat: archivo de lotes

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para DOS), OS/2

dpl: biblioteca comprimida de Borland Delphi

dll: biblioteca de enlaces dinámicos

scr: pantalla de presentación en Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto Microsoft OLE (Object Linking and Embedding)

tsp: programa ejecutable en modo de tiempo fraccionado

drv: controlador de dispositivo

vxm: controlador de dispositivo virtual de Microsoft Windows

pif: archivo de información de programa

lnk: archivo de acceso directo de Microsoft Windows

reg: archivo clave para el Registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de instalación para Microsoft Windows, Windows NT y ciertas aplicaciones

cla: clase Java

vbs: script Visual Basic®

vbe: extensión de vídeo del BIOS

js, jse: texto de origen JavaScript

htm: documento hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta: programa hipertexto para Microsoft Internet Explorer®

asp: secuencia de comandos Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script PHP integrado en archivos HTML

wsh: archivo de configuración de Microsoft Windows Script Host

wsf: script Microsoft Windows

the: papel tapiz del escritorio de Microsoft Windows 95

hlp: archivo de Ayuda de Microsoft Windows

eml: mensaje de correo de Microsoft Office Outlook Express

nws: mensaje de noticias de Microsoft Outlook Express

msg: mensaje de correo de Microsoft Mail

plg: mensaje de correo

mbx: mensajes de correo de Microsoft Office Outlook guardado

doc\*: documentos de Microsoft Office Word, como doc (Microsoft Office Word), docx (Microsoft Office Word 2007 con compatibilidad con XML) y docm (Microsoft Office Word 2007 con compatibilidad para macros)

dot\*: plantilla de documento de Microsoft Office Word, como: dot para plantillas de documento de Microsoft Office Word; dotx para plantillas de documento Microsoft Office Word 2007, y dotm para plantilla de documento Microsoft Office Word 2007 con soporte para macros

fpm: programa de bases de datos, archivo de inicio para Microsoft Visual FoxPro

rtf: documento en formato de texto enriquecido (Rich Text Format)

shs: fragmento de identificador de objeto de recorte de Shell de Windows

dwg: base de datos de dibujos de AutoCAD®

msi: paquete de instalación de Microsoft Windows Installer

otm: proyecto VBA para Microsoft Office Outlook

pdf: documento Adobe Acrobat

swf: objeto empaquetado Shockwave® Flash

jpg, jpeg: formato gráfico para imágenes comprimidas

emf: formato de metadatos ampliado

ico: archivo de icono

ov?: Archivos ejecutables de Microsoft Office Word

xl\*: documentos de Microsoft Office Excel y archivos como: xla, la extensión para Microsoft Office Excel; xlc para diagramas; xlt para plantillas de documentos; xlsx para libros de trabajo de Microsoft Office Excel 2007; xltm para libros de trabajo de Microsoft Office Excel 2007 con compatibilidad para macros; xlsb para libros de trabajo de Microsoft Office Excel 2007 en formato binario (no XML); xltx para plantillas de Microsoft Office Excel 2007; xslm para plantillas de Microsoft Office Excel 2007 con compatibilidad para macros, y xlam para complementos de Microsoft Office Excel 2007 con compatibilidad para macros

pp\*: documentos y archivos de Microsoft Office PowerPoint®, como: pps para diapositivas de Microsoft Office PowerPoint; ppt para presentaciones; pptx para presentaciones de Microsoft Office PowerPoint 2007; pptm para presentaciones de Microsoft Office PowerPoint 2007 con compatibilidad para macros; potx para plantillas de presentación de Microsoft Office PowerPoint 2007; potm para plantillas de presentación de Microsoft Office PowerPoint 2007 con compatibilidad para macros; ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007; ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 con compatibilidad para macros, y ppam para complementos de Microsoft Office PowerPoint 2007 con compatibilidad para macros

md\*: documentos y archivos de Microsoft Office Access® como mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: diapositivas Microsoft PowerPoint 2007

sldm: diapositivas Microsoft PowerPoint 2007 con soporte para macros

thmx: tema Microsoft Office 2007

## Apéndice 5. Configuración de red para la interacción con servicios externos

Kaspersky Endpoint Security utiliza la siguiente configuración de red para interactuar con servicios externos.

Configuración de red

Dirección	Descripción
activation- v2.kaspersky.com/activation-service/activation-service.svc Protocolo: HTTPS Puerto: 443	Activación de la aplicación
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	Actualización de las bases de datos y los módulos de la aplicación

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

downloads.upd.kaspersky.com

Protocolo: HTTPS

Puerto: 443

- Actualización de las bases de datos y los módulos de la aplicación
- Comprobación de la accesibilidad de 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).

	<p>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, póngase en contacto con el Servicio de soporte técnico para obtener un parche privado.</p>
<p>touch.kaspersky.com Protocolo: HTTP</p>	<ul style="list-style-type: none"> <li>• Recibiendo el tiempo de confianza para revisar el periodo de validez del certificado (conexión TLS).</li> <li>• Advertencia sobre la denegación de acceso a un recurso web en el navegador (Protección frente a amenazas web y Control web).</li> </ul>
<p>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</p>	<p>Actualización de las bases de datos y los módulos de la aplicación</p>

<p>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</p> <p>Protocolo: HTTP  Puerto: 80</p>	
<p>ds.kaspersky.com</p> <p>Protocolo: HTTPS  Puerto: 443</p>	Uso de Kaspersky Security Network.
<p>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</p> <p>Protocolo: Cualquier  Puerto: 443, 1443</p>	Uso de Kaspersky Security Network.
<p>click.kaspersky.com  redirect.kaspersky.com</p> <p>Protocolo: HTTPS</p>	Haga clic en los enlaces de la interfaz
<p>cr1.kaspersky.com  ocsp.kaspersky.com</p> <p>Protocolo: HTTP  Puerto: 80</p>	Infraestructura de clave pública (PKI)

## Apéndice 6. Eventos de la aplicación en el Registro de eventos de Windows

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 almacenan en el Registro de eventos de Windows.

[Auditoría del sistema](#) 

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
201		Infracción del Contrato de licencia de usuario final.	✓
203		La licencia está a punto de caducar.	–
206		Base de datos ausente o dañada.	–
207		Las bases de datos están muy desactualizadas.	–
209		Autoejecución de la aplicación desactivada.	–
229		Error de activación.	✓
231		Amenaza activa detectada. Se debe iniciar la Desinfección avanzada.	✓
2023		Servidores de KSN no disponibles.	–
343		No hay suficiente espacio en el almacén de cuarentena.	✓
346		No se restauró el objeto desde la cuarentena.	✓
348		No se eliminó el objeto de la cuarentena.	✓
212		No se puede realizar la tarea.	–
237		La aplicación falló durante una sesión anterior.	✓
204		La licencia está a punto de caducar.	–
208		Las bases de datos están desactualizadas.	–
210		Las actualizaciones automáticas están desactivadas.	–
211		Autoprotección desactivada.	–
214		Componentes de protección desactivados.	–
215		El equipo se está ejecutando en modo seguro.	–
216		Hay archivos no procesados.	–
219		Directiva de grupo aplicada.	✓
222		Tarea detenida.	–
224		Reinicie la aplicación para completar la actualización.	–
225		Es necesario reiniciar el equipo.	✓
226		La licencia permite el uso de componentes que no se han instalado.	–
232		Desinfección avanzada iniciada.	–
233		Desinfección avanzada completada.	–
230		Clave de licencia de reserva incorrecta.	–
240		La suscripción vence pronto.	✓
336		No se puede restaurar el objeto de Copias de seguridad.	–
2001		Se ha detectado actividad de red sospechosa.	–
250		Conexión cifrada terminada.	✓

2021		La participación en KSN está desactivada.	-
245		El procesamiento de algunas funciones del SO está desactivado.	✓
344		El almacén de cuarentena está casi sin espacio.	✓
235		Aplicación iniciada.	✓
236		Aplicación detenida.	✓
213		La operación con recursos de la aplicación ha sido bloqueada por Autoprotección.	-
217		Informe borrado.	✓
220		Directiva de grupo desactivada.	-
218		Configuración de la aplicación modificada.	✓
221		Tarea iniciada.	-
223		Tarea terminada.	-
227		Todos los componentes de la aplicación que define la licencia se han instalado y funcionan de modo normal.	-
238		La configuración de suscripción ha cambiado.	✓
239		Se ha renovado la suscripción.	✓
335		Objeto restaurado de Copias de seguridad.	-
2000		Introduzca un nombre de usuario y contraseña.	-
2020		La participación en KSN está activada.	-
2022		Servidores de KSN disponibles.	-
2024		La aplicación funciona y procesa datos según las leyes correspondientes, y usa la infraestructura adecuada.	✓
345		Se restauró el objeto de la Cuarentena.	✓
347		Se eliminó el objeto eliminado de la Cuarentena	✓

### [Detección de comportamiento](#)












## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	–
313		No se puede eliminar.	–
452		Proceso finalizado.	–
453		No es posible finalizar el proceso.	–
455		Operación de deshacer completada.	–
331		Bloqueado.	–
307		Objeto eliminado.	–
323		El objeto se eliminará al reiniciar.	–
311		No se puede crear una copia de seguridad.	–
303		Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.	–
457		Archivo restaurado.	–
308		Se creó una copia de seguridad del objeto.	–
458		Valor del registro restaurado.	–
459		Valor del registro eliminado.	–
329		Objeto renombrado.	–

[Prevención de exploits <sup>?</sup>](#)

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	–
331		Bloqueado.	–
455		Operación de deshacer completada.	–
307		Objeto eliminado.	–
323		El objeto se eliminará al reiniciar.	–
457		Archivo restaurado.	–
458		Valor del registro restaurado.	–
459		Valor del registro eliminado.	–
329		Objeto renombrado.	–

[Prevención de intrusiones en el host <sup>?</sup>](#)

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	✓
312		No se puede desinfectar.	–
313		No se puede eliminar.	–
317		Error de procesamiento.	–
452		Proceso finalizado.	–
453		No es posible finalizar el proceso.	–
310		No se puede crear una copia de seguridad.	–
314		Objeto no procesado.	–
320		Objeto cifrado.	–
321		Objeto dañado.	–
323		El objeto se eliminará al reiniciar.	–
324		El objeto se desinfectará al reiniciar.	–
303		Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.	–
336		No se puede restaurar el objeto de Copias de seguridad.	–
307		Objeto eliminado.	–
306		Objeto desinfectado.	–
301		Objeto procesado.	–
308		Se creó una copia de seguridad del objeto.	–
315		Objeto omitido.	–
318		Archivo comprimido detectado.	–
319		Objeto comprimido detectado.	–
327		Sobrescrito por una copia desinfectada anteriormente.	–
332		Información sobre el objeto detectado.	–
322		Archivo comprimido protegido con contraseña detectado.	–
335		Objeto restaurado de Copias de seguridad.	–
401		Aplicación puesta en el grupo de confianza.	–
402		Aplicación colocada en grupo restringido.	–
403		Se ha activado Prevención de intrusiones en el host.	–
340		El objeto está en la lista de admitidos de KSN privada.	✓

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	✓
312		No se puede desinfectar.	–
313		No se puede eliminar.	–
317		Error de procesamiento.	✓
452		Proceso finalizado.	–
453		No es posible finalizar el proceso.	–
310		No se puede crear una copia de seguridad.	–
314		Objeto no procesado.	–
320		Objeto cifrado.	–
321		Objeto dañado.	–
323		El objeto se eliminará al reiniciar.	–
324		El objeto se desinfectará al reiniciar.	–
303		Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.	–
336		No se puede restaurar el objeto de Copias de seguridad.	–
307		Objeto eliminado.	–
306		Objeto desinfectado.	–
455		Operación de deshacer completada.	–
301		Objeto procesado.	–
308		Se creó una copia de seguridad del objeto.	–
315		Objeto omitido.	–
318		Archivo comprimido detectado.	–
319		Objeto comprimido detectado.	–
325		Sobrescrito por una copia desinfectada anteriormente.	–
322		Archivo comprimido protegido con contraseña detectado.	–
332		Información sobre el objeto detectado.	–
335		Objeto restaurado de Copias de seguridad.	–
340		El objeto está en la lista de admitidos de KSN privada.	✓

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	✓
362		Enlace peligroso bloqueado.	✓
363		Enlace peligroso abierto.	✓
1201		Se ha detectado un enlace peligroso abierto anteriormente.	✓
317		Error de procesamiento.	✓
303		Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.	–
331		Bloqueado	–
341		Se ha bloqueado la descarga del objeto.	–
321		Objeto dañado.	–
301		Objeto procesado.	–
301		Enlace procesado.	–
332		Información sobre el objeto detectado.	–
319		Objeto comprimido detectado.	–
318		Archivo comprimido detectado.	–
322		Archivo comprimido protegido con contraseña detectado.	–
370		El enlace está en la lista de admitidos de KSN privada.	✓
370		El objeto está en la lista de admitidos de KSN privada.	✓



[Protección frente a amenazas en el correo !\[\]\(1e1a06ebca281395f282cf61b1470f88\_img.jpg\)](#)

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	✓
312		No se puede desinfectar.	–
317		Error de procesamiento.	✓
314		Objeto no procesado.	–
303		Se ha detectado software legítimo que los delincuentes pueden usar para dañar su equipo.	–
321		Objeto dañado.	–
336		No se puede restaurar el objeto de Copias de seguridad.	–
307		Objeto eliminado.	–
342		Se eliminó el objeto eliminado según la configuración.	–
306		Objeto desinfectado.	–
301		Objeto procesado.	–
308		Se creó una copia de seguridad del objeto.	–
318		Archivo comprimido detectado.	–
319		Objeto comprimido detectado.	–
329		Objeto renombrado.	–
332		Información sobre el objeto detectado.	–
322		Archivo comprimido protegido con contraseña detectado.	–
335		Objeto restaurado de Copias de seguridad.	–
340		El objeto está en la lista de admitidos de KSN privada.	✓


**Firewall** 

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
602		Actividad de red bloqueada.	✓
601		Actividad de red permitida.	–




**Protección frente a amenazas en la red** 

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
651		Ataque de red detectado.	–
















## Prevención de ataques de BadUSB

Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2051		Teclado no autorizado.	✓
2052		Error de autorización del teclado.	✓
2050		Teclado autorizado.	–








## Protección AMSI

Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	✓
2200		Se bloqueó la solicitud de AMSI.	✓
317		Error de procesamiento.	✓
314		Objeto no procesado.	–
320		Objeto cifrado.	–
321		Objeto dañado.	–
303		Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.	–
1512		El resultado del análisis del objeto se ha enviado a una aplicación de terceros.	–
301		Objeto procesado.	–
315		Objeto omitido.	–
318		Archivo comprimido detectado.	–
319		Objeto comprimido detectado.	–
322		Archivo comprimido protegido con contraseña detectado.	–
332		Información sobre el objeto detectado.	–
340		El objeto está en la lista de admitidos de KSN privada.	✓






## Control de aplicaciones

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
702		Inicio de la aplicación prohibido.	–
710		Se ha iniciado un proceso prohibido antes del inicio de Kaspersky Endpoint Security para Windows.	–
707		Error en la configuración de tareas. No se aplicó la configuración de tareas.	–
708		Configuración de tarea aplicada correctamente.	–
701		Inicio de la aplicación permitido.	–
703		Inicio de la aplicación prohibido en modo de prueba.	–
704		Inicio de la aplicación permitido en modo de prueba.	–






[Control de dispositivos](#)

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
802		Operación con el dispositivo prohibida.	–
809		Conexión de red bloqueada.	–
803		Se activó el acceso temporal al dispositivo.	✓
801		Operación con el dispositivo permitida.	–
808		Operación de archivo realizada.	–

[Control Web](#)

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
752		Acceso denegado.	–
753		Advertencia acerca de contenido indeseado.	–
754		Se ha accedido a contenido indeseado tras una advertencia.	–
751		Acceso permitido.	–
751		Página permitida abierta.	–

[Control de anomalías adaptativo](#)

Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2200	❏	Acción del proceso bloqueada.	✓
2201	ⓘ	Acción del proceso omitida.	–

[Cifrado de datos](#) ⓘ



## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
904		Error al implementar las reglas de cifrado o descifrado de archivos.	✓
912		Error en el cifrado/descifrado de archivos.	✓
940		Acceso a los archivos bloqueado.	✓
951		Error al activar el modo portátil.	✓
953		Error al desactivar el modo portátil.	✓
931		Error al crear el paquete cifrado.	✓
1305		Error al cifrar/descifrar dispositivo.	✓
1311		Error al cargar el módulo de cifrado.	✓
1340		La tarea de administración de las cuentas del Agente de autenticación ha terminado con un error.	✓
1312		La directiva no se puede aplicar.	✓
1342		Error al actualizar FDE.	✓
1344		La reversión de la actualización de Cifrado de disco completo se ha completado con un error.	✓
903		Interrumpida la aplicación de las reglas de cifrado/descifrado de archivos.	–
914		Se ha interrumpido el cifrado/descifrado de archivos.	–
1303		Se ha interrumpido el cifrado/descifrado de dispositivos.	–
1306		El usuario ha optado por no implementar la directiva de cifrado.	–
1345		No se han podido instalar o actualizar los controladores de Cifrado de disco de Kaspersky en la imagen de WinRE.	✓
901		Iniciada la aplicación de las reglas de cifrado/descifrado de archivos.	–
902		Aplicación de las reglas de cifrado/descifrado de archivos finalizada.	–
905		Reanudada la aplicación de las reglas de cifrado/descifrado de archivos.	–
910		Cifrado o descifrado de archivos iniciado.	–
911		Se ha completado el cifrado/descifrado de archivos.	–
913		El archivo no se ha cifrado porque es una exclusión.	–
950		Modo portátil activado.	–
952		Modo portátil desactivado.	–
1301		Se ha iniciado el cifrado o descifrado del dispositivo.	–
1302		Se ha completado el cifrado o descifrado del dispositivo.	–
1304		Se ha reanudado el cifrado/descifrado de dispositivos.	–

1310		Módulo de cifrado cargado.	–
1307		El dispositivo no está cifrado.	–
1308		El proceso de cifrado/descifrado del dispositivo se ha cambiado a modo activo.	–
1309		El proceso de cifrado o descifrado de dispositivos se ha cambiado al modo pasivo.	–
1330		Nueva cuenta del Agente de autenticación creada.	–
1331		Cuenta del Agente de autenticación eliminada.	–
1332		Contraseña de la cuenta del Agente de autenticación modificada.	–
1333		Inicio de sesión correcto del Agente de autenticación.	–
1334		Error al intentar iniciar sesión el Agente de autenticación.	–
1335		Se ha accedido al disco duro por medio de la solicitud de acceso a dispositivos cifrados.	–
1336		Error al intentar acceder al disco duro por medio de la solicitud de acceso a dispositivos cifrados.	–
1337		No se añadió la cuenta. Esta cuenta ya existe.	–
1338		No se modificó la cuenta. Esta cuenta no existe.	–
1339		No se eliminó la cuenta. Esta cuenta no existe.	–
1341		Actualización del FDE correcta.	✓
1343		Deshacer actualización de FDE correcta.	✓
1346		No se han podido desinstalar los controladores de Cifrado de disco de Kaspersky de la imagen de WinRE.	✓
1370		Se cambió la clave de recuperación de BitLocker.	✓
1371		Se ha cambiado la contraseña/PIN de BitLocker.	✓
1372		La clave de recuperación de BitLocker se guardó en una unidad extraíble.	✓

## Sensor de Endpoint

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2100		Servidor de Kaspersky Anti Targeted Attack Platform no disponible.	–
2105		Se ha bloqueado el inicio de la aplicación.	✓
2106		Se ha bloqueado la apertura del documento.	✓
2112		Se han finalizado todos los procesos iniciados desde una imagen de archivo o un flujo.	✓
2113		Aplicación iniciada.	✓
2111		El archivo o la secuencia ha sido eliminado por el administrador del servidor de Kaspersky Anti Targeted Attack Platform.	✓
2110		El administrador ha restaurado el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform.	✓
2109		El administrador coloca el archivo en Cuarentena en el servidor de Kaspersky Anti Targeted Attack Platform.	✓
2107		La actividad de red de las aplicaciones de terceros se ha bloqueado.	✓
2108		Se ha desbloqueado el tráfico de red.	✓
2104		El procesamiento de tareas del servidor de Kaspersky Anti Targeted Attack Platform está activo.	–
2103		El procesamiento de tareas del servidor de Kaspersky Anti Targeted Attack Platform está inactivo.	–
2101		El componente Sensores de Endpoint se ha conectado al servidor.	–
2102		Se ha recuperado la conexión con el servidor de Kaspersky Anti Targeted Attack Platform.	–


[Análisis antivirus](#)

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
302		Objeto malicioso detectado.	✓
312		No se puede desinfectar.	–
313		No se puede eliminar.	–
317		Error de procesamiento.	–
452		Proceso finalizado.	–
453		No es posible finalizar el proceso.	–
310		No se puede crear una copia de seguridad.	–
314		Objeto no procesado.	–
320		Objeto cifrado.	–
321		Objeto dañado.	–
323		El objeto se eliminará al reiniciar.	–
324		El objeto se desinfectará al reiniciar.	–
303		Se ha detectado software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.	–
336		No se puede restaurar el objeto de Copias de seguridad.	✓
307		Objeto eliminado.	–
306		Objeto desinfectado.	–
455		Operación de deshacer completada.	–
301		Objeto procesado.	–
308		Se creó una copia de seguridad del objeto.	–
315		Objeto omitido.	–
318		Archivo comprimido detectado.	–
319		Objeto comprimido detectado.	–
327		Sobrescrito por una copia desinfectada anteriormente.	–
332		Información sobre el objeto detectado.	–
322		Archivo comprimido protegido con contraseña detectado.	–
335		Objeto restaurado de Copias de seguridad.	✓
329		Objeto renombrado.	–
340		El objeto está en la lista de admitidos de KSN privada.	✓

[Comprobación de integridad](#)

Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2002		Error al comprobar la firma del módulo de sistema.	-




[Actualización de las bases de datos](#) 

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
1011		Error al actualizar el componente.	–
1012		Error al distribuir las actualizaciones de componentes.	–
1014		Error de actualización local.	–
1015		Error de actualización de red.	–
1017		No se pueden iniciar dos tareas a la vez.	–
1018		Error al verificar las bases de datos y módulos de la aplicación.	–
1019		Error en la interacción con Kaspersky Security Center.	–
1021		No se han actualizado todos los componentes.	–
1023		Actualización completada correctamente. Error de la distribución de actualizaciones.	–
101		Ha ocurrido un error interno.	✓
2153		Error al instalar el parche.	–
2156		Error al revertir el parche.	–
1016		Operación cancelada por el usuario.	–
1001		Origen de actualizaciones seleccionado.	–
1002		Servidor proxy seleccionado.	–
1003		Descarga de archivo.	–
1004		Archivo descargado.	–
1005		Archivo instalado.	–
1006		Archivo actualizado.	–
1007		Archivo revertido debido a un error de actualización.	–
1008		Actualizando archivos.	–
1009		Distribuyendo actualizaciones.	–
1010		Restaurando archivos.	–
1013		Creando la lista de archivos para descargar.	–
1020		No hay actualizaciones disponibles.	–
1022		Distribución de actualizaciones completada correctamente.	–
2150		Descargando parches.	–
2151		Instalando parches.	–
2152		Parche instalado.	–
2154		Revertiendo parche.	–
2155		Parche revertido.	–

## Eliminación de datos

Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2252		No se puede eliminar.	–
2253		Estadísticas de la tarea de eliminación.	–
2251		Objeto eliminado.	–

## Endpoint Detection and Response

Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2551		Se bloqueó el inicio de objetos.	✓
2552		Se bloqueó el inicio de proceso.	✓
2559		Se bloqueó la ejecución de scripts.	✓
2556		Objeto no puesto en cuarentena (Endpoint Detection and Response).	✓
2651		Se ha encontrado una IOC.	✓
2553		Se permite el inicio del objeto. Registro de eventos.	✓
2554		Se permite el inicio de procesos. Registro de eventos.	✓
2560		Se permite la ejecución de scripts. Registro de eventos.	✓
2558		El objeto se borrará tras el reinicio (Endpoint Detection and Response).	✓
2700		Aislamiento de red	✓
2701		Terminación del aislamiento de la red	✓
2555		Objeto en cuarentena (Endpoint Detection and Response)	✓
2557		Objeto eliminado (Endpoint Detection and Response)	✓
2652		Se inició el análisis de IOC	✓
2653		Se completó el análisis de IOC	✓

## Kaspersky Sandbox

## Códigos de eventos

ID del evento		Descripción	Activado de forma predeterminada
2603		Objeto no puesto en cuarentena (Kaspersky Sandbox).	✓
2607		Ha ocurrido un error interno.	✓
2611		Error al enviar la tarea de análisis a Kaspersky Sandbox.	✓
2613		Certificado del servidor de Kaspersky Sandbox no válido.	✓
2614		El nodo Kaspersky Sandbox no está disponible.	✓
2615		Se detecta una amenaza durante el procesamiento de tareas asíncronas.	✓
2617		Error al procesar un objeto en Kaspersky Sandbox.	✓
2618		Se ha superado la carga máxima de Kaspersky Sandbox.	✓
2651		Se ha encontrado una IOC.	✓
2620		Falló la verificación de licencia de Kaspersky Sandbox.	✓
2605		El objeto se eliminará después de reiniciar (Kaspersky Sandbox).	✓
2612		El tamaño total de las tareas de análisis superó el límite.	✓
308		Se creó una copia de seguridad del objeto.	–
2602		Objeto en cuarentena (Kaspersky Sandbox).	✓
2604		Objeto eliminado (Kaspersky Sandbox).	✓
2606		Se decidió enviar la tarea de análisis a Kaspersky Sandbox.	✓
2609		El caché local ha sido borrado.	✓
2610		La tarea de análisis se envía a Kaspersky Sandbox.	✓
2616		No se encuentran amenazas durante el procesamiento de la tarea asíncrona.	✓
2652		Se inició el análisis de IOC.	✓
2653		Se completó el análisis de IOC.	✓
2608		Se ha encontrado un resultado en caché durante el procesamiento síncrono de objetos	✓

## Apéndice 7. Eventos de la aplicación en el registro de eventos de Kaspersky Security Center

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la finalización de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se almacenan en el registro de eventos de Kaspersky Security Center.



Kaspersky Endpoint Security genera eventos de los siguientes tipos: eventos genéricos y eventos específicos. Los eventos específicos son creados únicamente por Kaspersky Endpoint Security for Windows. Los eventos específicos tienen una id. simple, como 000000cb. Los eventos específicos contienen los siguientes parámetros requeridos:















- GNRL\_EA\_DESCRIPTION es el contenido del evento.
- GNRL\_EA\_ID es el ID de servicio del evento.
- GNRL\_EA\_SEVERITY es el estado del evento. 1: Mensaje de información (i), 2: Advertencia (A), 3: Fallo operativo (E), 4: Crítico (E).
- 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 genéricos pueden ser creados por Kaspersky Endpoint Security for Windows así como por otras aplicaciones de Kaspersky (por ejemplo, Kaspersky Security for Windows Server). Los eventos genéricos tienen una ID. más compleja, como GNRL\_EV\_VIRUS\_FOUND. Además de la configuración requerida, los eventos genéricos contienen una configuración avanzada.





























[Lista de eventos específicos de Kaspersky Endpoint Security para Windows](#) ?





















ID del evento		Descripción	Activado de forma predeterminada
00000065		Error interno de la tarea.	–
000000cb		La licencia está a punto de caducar.	–
000000cc		La licencia está a punto de caducar.	✓
000008cd		Estadísticas de la tarea de eliminación.	✓
000000ce		Base de datos ausente o dañada.	–
000000cf		Las bases de datos están muy desactualizadas.	✓
000000d0		Las bases de datos están desactualizadas.	✓
000000d1		Autoejecución de la aplicación desactivada.	✓
000000d2		Las actualizaciones automáticas están desactivadas.	✓
000000d3		Autoprotección desactivada.	✓
000000d4		No se puede realizar la tarea.	✓
000000d5		La operación con recursos de la aplicación ha sido bloqueada por Autoprotección.	✓
000000d6		Componentes de protección desactivados.	✓
000000d7		El equipo se está ejecutando en modo seguro.	–
000000d8		Hay archivos no procesados.	✓
000000d9		Informe borrado.	✓
000000da		Configuración de la aplicación modificada.	✓
000000db		Directiva de grupo aplicada.	✓
000000dc		Directiva de grupo desactivada.	✓
000000dd		Tarea iniciada.	✓
000000de		Tarea detenida.	✓
000000df		Tarea terminada.	✓
000000e1		Es necesario reiniciar el equipo.	✓
000000e2		La licencia permite el uso de componentes que no se han instalado.	✓
000000e3		Todos los componentes de la aplicación que define la licencia se han instalado y funcionan de modo normal.	–
000000e6		Clave de licencia de reserva incorrecta.	✓
000000e7		Amenaza activa detectada. Se debe iniciar la Desinfección avanzada.	✓
000000e8		Desinfección avanzada iniciada.	✓
000000e9		Desinfección avanzada completada.	✓
000000ee		La configuración de suscripción ha cambiado.	✓
000000ef		Se ha renovado la suscripción.	✓

000000f0	⚠	La suscripción vence pronto.	✓
000000f5	⚠	El procesamiento de algunas funciones del SO está desactivado.	✓
00000134	🕒	Se creó una copia de seguridad del objeto.	✓
00000136	⚠	No se puede crear una copia de seguridad.	✓
00000139	🛑	No se puede eliminar.	✓
0000013a	⚠	Objeto no procesado.	✓
0000013d	🛑	Error de procesamiento.	✓
00000140	⚠	Objeto cifrado.	-
00000141	⚠	Objeto dañado.	-
00000143	⚠	El objeto se eliminará al reiniciar.	✓
00000144	⚠	El objeto se desinfectará al reiniciar.	✓
00000147	🕒	Sobrescrito por una copia desinfectada anteriormente.	-
00000149	🕒	Objeto renombrado.	✓
0000014c	🕒	Información sobre el objeto detectado.	✓
0000014f	🕒	Objeto restaurado de Copias de seguridad.	✓
00000150	⚠	No se puede restaurar el objeto de Copias de seguridad.	✓
00000154	🕒	El objeto está en la lista de admitidos de KSN privada.	✓
00000157	🛑	No hay suficiente espacio en el almacén de cuarentena.	✓
00000158	⚠	El almacén de cuarentena está casi sin espacio.	✓
00000159	🕒	Se restauró el objeto de la Cuarentena.	✓
0000015a	🛑	No se restauró el objeto desde la cuarentena.	✓
0000015b	🕒	Se eliminó el objeto eliminado de la Cuarentena	✓
0000015c	🛑	No se eliminó el objeto de la cuarentena.	✓
00000172	🕒	El enlace está en la lista de admitidos de KSN privada.	✓
00000191	🕒	Aplicación puesta en el grupo de confianza.	✓
00000192	🕒	Aplicación colocada en grupo restringido.	✓
00000193	🕒	Se ha activado Prevención de intrusiones en el host.	✓
000001c4	🛑	Proceso finalizado.	✓
000001c5	🛑	No es posible finalizar el proceso.	-
000001c7	⚠	Operación de deshacer completada.	✓
000001c9	🕒	Archivo restaurado.	✓
000001ca	🕒	Valor del registro restaurado.	✓
000001cb	🕒	Valor del registro eliminado.	-
000002c3	🛑	Error en la configuración de tareas. No se aplicó la configuración de tareas.	✓

000002c4		Configuración de tarea aplicada correctamente.	✓
000002c6		Se ha iniciado un proceso prohibido antes del inicio de Kaspersky Endpoint Security para Windows.	✓
000002f2		Se ha accedido a contenido indeseado tras una advertencia.	–
000002f4		Página permitida abierta.	–
00000321		Operación con el dispositivo permitida.	–
00000323		Se activó el acceso temporal al dispositivo.	✓
00000329		Conexión de red bloqueada.	✓
00000385		Iniciada la aplicación de las reglas de cifrado/descifrado de archivos.	✓
00000386		Aplicación de las reglas de cifrado/descifrado de archivos finalizada.	✓
00000388		Error al implementar las reglas de cifrado o descifrado de archivos.	✓
000003a3		Error al crear el paquete cifrado.	✓
000003b7		Error al activar el modo portátil.	✓
000003b9		Error al desactivar el modo portátil.	✓
000003f3		Error al actualizar el componente.	✓
000003f4		Error al distribuir las actualizaciones de componentes.	–
000003f7		Error de actualización de red.	–
000003f8		Operación cancelada por el usuario.	✓
000003f9		No se pueden iniciar dos tareas a la vez.	✓
000003fa		Error al verificar las bases de datos y módulos de la aplicación.	✓
000003fb		Error en la interacción con Kaspersky Security Center.	✓
000003fc		No hay actualizaciones disponibles.	–
000003fd		No se han actualizado todos los componentes.	✓
000003fe		Distribución de actualizaciones completada correctamente.	–
000003ff		Actualización completada correctamente. Error de la distribución de actualizaciones.	–
00000519		Error al cifrar/descifrar dispositivo.	✓
0000051a		El usuario ha optado por no implementar la directiva de cifrado.	✓
0000051e		Módulo de cifrado cargado.	–
0000051f		Error al cargar el módulo de cifrado.	✓
00000520		La directiva no se puede aplicar.	✓
00000532		Nueva cuenta del Agente de autenticación creada.	–
00000533		Cuenta del Agente de autenticación eliminada.	–
00000534		Contraseña de la cuenta del Agente de autenticación modificada.	–

00000535		Inicio de sesión correcto del Agente de autenticación.	–
00000536		Error al intentar iniciar sesión el Agente de autenticación.	–
00000539		No se añadió la cuenta. Esta cuenta ya existe.	–
0000053a		No se modificó la cuenta. Esta cuenta no existe.	–
0000053b		No se eliminó la cuenta. Esta cuenta no existe.	–
0000053c		La tarea de administración de las cuentas del Agente de autenticación ha terminado con un error.	✓
0000053d		Actualización del FDE correcta.	✓
0000053e		Error al actualizar FDE.	✓
0000053f		Deshacer actualización de FDE correcta.	✓
00000540		La reversión de la actualización del cifrado se ha completado con un error (para más detalles, consulte la Ayuda en línea de Kaspersky Endpoint Security for Windows).	✓
00000541		No se han podido instalar o actualizar los controladores de Cifrado de disco de Kaspersky en la imagen de WinRE.	✓
00000542		No se han podido desinstalar los controladores de Cifrado de disco de Kaspersky de la imagen de WinRE.	✓
0000055a		Se cambió la clave de recuperación de BitLocker.	✓
0000055b		Se ha cambiado la contraseña/PIN de BitLocker.	✓
0000055c		La clave de recuperación de BitLocker se guardó en una unidad extraíble.	✓
00000579		Error al cambiar componentes de la aplicación.	✓
0000057a		Se cambiaron con éxito los componentes de la aplicación.	✓
0000057b		Es necesario reiniciar para completar la tarea.	✓
000007d0		Introduzca un nombre de usuario y contraseña.	✓
000007d1		Se ha detectado actividad de red sospechosa.	✓
000007d2		Error al comprobar la firma del módulo de sistema.	✓
000007d3		Conexión cifrada terminada.	–
000007e4		La participación en KSN está activada.	✓
000007e5		La participación en KSN está desactivada.	✓
000007e6		Servidores de KSN disponibles.	✓
000007e7		Servidores de KSN no disponibles.	✓
000007e8		La aplicación funciona y procesa datos según las leyes correspondientes, y usa la infraestructura adecuada.	✓
00000802		Teclado autorizado.	✓
00000803		Teclado no autorizado.	✓
00000804		Error de autorización del teclado.	✓
00000834		Servidor de Kaspersky Anti Targeted Attack Platform no disponible.	✓




00000835		El componente Sensores de Endpoint se ha conectado al servidor.	
00000836		Se ha recuperado la conexión con el servidor de Kaspersky Anti Targeted Attack Platform.	
00000837		El procesamiento de tareas del servidor de Kaspersky Anti Targeted Attack Platform está inactivo.	
00000838		El procesamiento de tareas del servidor de Kaspersky Anti Targeted Attack Platform está activo.	
00000839		Se ha bloqueado el inicio de la aplicación.	
0000083a		Se ha bloqueado la apertura del documento.	
0000083b		La actividad de red de las aplicaciones de terceros se ha bloqueado.	
0000083c		Se ha desbloqueado el tráfico de red.	
0000083d		El administrador coloca el archivo en Cuarentena en el servidor de Kaspersky Anti Targeted Attack Platform.	
0000083e		El administrador ha restaurado el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform.	
0000083f		El archivo o la secuencia ha sido eliminado por el administrador del servidor de Kaspersky Anti Targeted Attack Platform.	
0000083e		El administrador ha restaurado el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform.	
00000840		Se han finalizado todos los procesos iniciados desde una imagen de archivo o un flujo.	
00000841		Aplicación iniciada.	
00000869		Error al instalar el parche.	
0000086c		Error al revertir el parche.	
00000898		Se bloqueó la solicitud de AMSI.	
000008cc		Error al eliminar un objeto.	
000009f8		Se permite la ejecución del proceso, se registró el evento.	
000009f9		Se bloqueó el inicio de objetos.	
000009fa		Se permite la ejecución del objeto, se registró el evento.	
000009fb		Objeto en cuarentena (Endpoint Detection and Response).	
000009fc		Objeto no puesto en cuarentena (Endpoint Detection and Response).	
000009fd		Objeto eliminado (Endpoint Detection and Response).	
000009fe		El objeto se borrará tras el reinicio (Endpoint Detection and Response).	
00000a2a		Objeto en cuarentena (Kaspersky Sandbox).	
00000a2b		Objeto no puesto en cuarentena (Kaspersky Sandbox).	
00000a2d		El objeto se eliminará después de reiniciar (Kaspersky Sandbox).	
00000a2f		Ha ocurrido un error interno.	

00000a34		El tamaño total de las tareas de análisis superó el límite.	
00000a35		Certificado del servidor de Kaspersky Sandbox no válido.	
00000a36		El nodo Kaspersky Sandbox no está disponible.	
00000a39		Error al procesar un objeto en Kaspersky Sandbox.	
00000a3c		Falló la verificación de licencia de Kaspersky Sandbox.	
00000a5b		Se ha encontrado una IOC.	
00000a5c		Se inició el análisis de IOC.	
00000a5d		Se completó el análisis de IOC.	
00000a8c		Aislamiento de red.	
00000a8d		Terminación del aislamiento de la red.	

[Lista de eventos genéricos](#) 




ID del evento		Descripción	Configuración
GNRL_EV_VIRUS_FOUND	❗	Objeto malicioso detectado.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es el hash SHA256 del objeto.</li> <li>• GNRL_EA_PARAM_2 es el nombre del objeto.</li> <li>• GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, File.</li> <li>• GNRL_EA_PARAM_7 es el nombre del usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es el nombre de la amenaza, por ejemplo, Trojan.</li> <li>• GNRL_EA_PARAM_9 es información adicional sobre el objeto. Componente de la aplicación: Tecnología de detección de amenazas (method). Amenaza detectada por (denylist): verdadero. Versión de EDR. Identificador de amenaza. Hash MD5 del objeto.</li> </ul>
GNRL_EV_VIRUS_FOUND_BY_KSN	❗	Se detectó un objeto malicioso (KSN).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es el hash SHA256 del objeto.</li> <li>• GNRL_EA_PARAM_2 es el nombre del objeto.</li> <li>• GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, File.</li> <li>• GNRL_EA_PARAM_7 es el nombre del usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es el nombre de la amenaza, por ejemplo, Trojan.</li> <li>• GNRL_EA_PARAM_9 es información adicional sobre el objeto. Componente de la aplicación: Tecnología de detección de amenazas (method). Amenaza detectada por (denylist): verdadero.</li> </ul>






			<p>Versión de EDR. Identificador de amenaza Hash MD5 del objeto.</p>
GNRL_EV_VIRUS_FOUND_AND_BLOCKED		<p>Enlace peligroso bloqueado (Protección frente a amenazas web).</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es la</li> <li>• GNRL_EA_PARAM_5 es el objeto según la clasificación Kaspersky.</li> <li>• GNRL_EA_PARAM_7 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es el objeto de amenaza, por ejemplo, T</li> <li>• GNRL_EA_PARAM_9 es información adicional sobre el objeto. Componente de la aplicación Tecnología de detección (<a href="#">mehtod</a>). Amenaza detectada por (denylist): verdadero</li> </ul>
GNRL_EV_VIRUS_FOUND_AND_REPORTED		<p>Enlace peligroso abierto (Protección frente a amenazas web).</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es la</li> <li>• GNRL_EA_PARAM_5 es el objeto según la clasificación Kaspersky.</li> <li>• GNRL_EA_PARAM_7 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es el objeto de amenaza, por ejemplo, T</li> <li>• GNRL_EA_PARAM_9 es información adicional sobre el objeto. Componente de la aplicación Tecnología de detección (<a href="#">mehtod</a>). Amenaza detectada por (denylist): verdadero</li> </ul>
GNRL_EV_VIRUS_FOUND_AND_PASSED		<p>Se ha detectado un enlace peligroso abierto con anterioridad (Web Threat Protection).</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es la</li> <li>• GNRL_EA_PARAM_5 es el objeto según la clasificación Kaspersky.</li> <li>• GNRL_EA_PARAM_7 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es el objeto de amenaza, por ejemplo, T</li> </ul>

			<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_9 es adicional sobre el objeto Componente de la aplicación Tecnología de detección (<a href="#">method</a>). Amenaza detectada por (denylist): verdadero</li> </ul>
GNRL_EV_SUSPICIOUS_OBJECT_FOUND	⚠	Se ha detectado software legítimo que los delincuentes pueden usar para dañar su equipo o averiguar sus datos personales	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es e (SHA256).</li> <li>GNRL_EA_PARAM_2 es e objeto.</li> <li>GNRL_EA_PARAM_5 es e amenaza según la clasificación Kaspersky, por ejemplo, File.</li> <li>GNRL_EA_PARAM_7 es e usuario de la sesión.</li> <li>GNRL_EA_PARAM_8 es e amenaza, por ejemplo, T</li> </ul>
GNRL_EV_OBJECT_CURED	⚠	Objeto desinfectado.	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es e (SHA256).</li> <li>GNRL_EA_PARAM_2 es e objeto.</li> <li>GNRL_EA_PARAM_3 es la creación del objeto (opc</li> <li>GNRL_EA_PARAM_5 es e amenaza según la clasificación Kaspersky, por ejemplo, File.</li> <li>GNRL_EA_PARAM_7 es e usuario de la sesión.</li> <li>GNRL_EA_PARAM_8 es e amenaza, por ejemplo, T</li> <li>GNRL_EA_PARAM_9 es ir adicional sobre el objeto Componente de la aplicación Tecnología de detección (<a href="#">method</a>). Amenaza detectada por (denylist): verdadero Versión de EDR. Identificador de amenaza Hash MD5 del objeto.</li> </ul>
GNRL_EV_OBJECT_DELETED	⚠	Objeto eliminado.	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es e</li> </ul>







			<p>(SHA256).</p> <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es el objeto.</li> <li>• GNRL_EA_PARAM_3 es la creación del objeto (opcional).</li> <li>• GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, File.</li> <li>• GNRL_EA_PARAM_7 es el nombre del usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es el nombre de la amenaza, por ejemplo, Trojan.</li> <li>• GNRL_EA_PARAM_9 es información adicional sobre el objeto: Componente de la aplicación, Tecnología de detección (<a href="#">mehtod</a>).</li> </ul> <p>Amenaza detectada por denylist): verdadero  Versión de EDR.  Identificador de amenaza  Hash MD5 del objeto.</p>
GNRL_EV_OBJECT_NOTCURED		No se puede desinfectar.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es el nombre de la amenaza (SHA256).</li> <li>• GNRL_EA_PARAM_2 es el nombre del objeto.</li> <li>• GNRL_EA_PARAM_3 es la creación del objeto (opcional).</li> <li>• GNRL_EA_PARAM_5 es el nombre de la amenaza según la clasificación de Kaspersky, por ejemplo, File.</li> <li>• GNRL_EA_PARAM_7 es el nombre del usuario de la sesión.</li> <li>• GNRL_EA_PARAM_9 es información adicional sobre el objeto: Componente de la aplicación, Tecnología de detección (<a href="#">mehtod</a>).</li> </ul> <p>Amenaza detectada por denylist): verdadero  Versión de EDR.  Identificador de amenaza  Hash MD5 del objeto.</p>

GNRL_EV_OBJECT_BLOCKED		Se ha bloqueado la descarga del objeto.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es e (SHA256).</li> <li>• GNRL_EA_PARAM_2 es e objeto.</li> <li>• GNRL_EA_PARAM_5 es e amenaza según la clasifi Kaspersky, por ejemplo, File.</li> <li>• GNRL_EA_PARAM_7 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es e amenaza, por ejemplo, T</li> <li>• GNRL_EA_PARAM_9 es ir adicional sobre el objeto Componente de la aplica Tecnología de detección (<a href="#">mehtod</a>). Amenaza detectada por (denylist): verdadero Versión de EDR. Identificador de amenaz Hash MD5 del objeto.</li> </ul>
GNRL_EV_OBJECT_REPORTED		<p>Objeto no procesado (Protección frente a amenazas en el correo).</p> <p>El resultado del análisis del objeto se ha enviado a una aplicación de terceros (Protección AMSI).</p>	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es e (SHA256).</li> <li>• GNRL_EA_PARAM_2 es e objeto.</li> <li>• GNRL_EA_PARAM_5 es e amenaza según la clasifi Kaspersky, por ejemplo, File.</li> <li>• GNRL_EA_PARAM_7 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_8 es e amenaza, por ejemplo, T</li> <li>• GNRL_EA_PARAM_9 es ir adicional sobre el objeto Componente de la aplica Tecnología de detección (<a href="#">mehtod</a>). Amenaza detectada por (denylist): verdadero Versión de EDR. Identificador de amenaz Hash MD5 del objeto.</li> </ul>
GNRL_EV_PASSWD_ARCHIVE_FOUND		Archivo comprimido	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es e</li> </ul>

		protegido con contraseña detectado.	<p>objeto.</p> <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_3 es la creación del objeto (opc</li> <li>• GNRL_EA_PARAM_7 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_9 es ir adicional sobre el objeto Componente de la aplica Tecnología de detección (<a href="#">mehtod</a>?). Amenaza detectada por (denylist): verdadero o fa</li> </ul>
GNRL_EV_ATTACK_DETECTED		Ataque de red detectado (protección frente a amenazas en la red).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es e ataque.</li> <li>• GNRL_EA_PARAM_2 es e</li> <li>• GNRL_EA_PARAM_3 es la equipo que actúa como de red. La dirección IP se orden de bytes del host. 2886729929 para 172.</li> <li>• GNRL_EA_PARAM_4 es e puerto.</li> <li>• GNRL_EA_PARAM_5 es u por ejemplo, 12B012B012B012B012E</li> <li>• GNRL_EA_PARAM_6 es la equipo al que está dirigido red. La dirección IP se in de bytes del host. Por ej 2886729929 para 172.</li> </ul>
GNRL_EV_LICENSE_EXPIRATION		Infracción del Contrato de licencia de usuario final.	–
GNRL_EV_APPLICATION_LAUNCHED		Inicio de la aplicación permitido (Control de aplicaciones).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es la vez que se inició la aplica formato especial para Ka Center.</li> <li>• GNRL_EA_PARAM_3 es e veces que se inició la ap</li> <li>• GNRL_EA_PARAM_4 es e seguridad de la cuenta (</li> <li>• GNRL_EA_PARAM_5 es la categoría de la aplicació</li> </ul>

GNRL_EV_APPLICATION_LAUNCH_DENIED	❗	Inicio de la aplicación prohibido (Control de aplicaciones).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_6 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_2 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_3 es la categoría que se creó m</li> <li>• GNRL_EA_PARAM_4 es la categoría de la aplicació</li> <li>• GNRL_EA_PARAM_5 es la firma digital de la aplic</li> <li>• GNRL_EA_PARAM_6 es el archivo ejecutable de la ejemplo, chrome.exe).</li> <li>• GNRL_EA_PARAM_7 es el ejecutable.</li> <li>• GNRL_EA_PARAM_8 es el (SHA256).</li> <li>• GNRL_EA_PARAM_9 es la aplicación que el usuario ejecutar.</li> </ul>
GNRL_EV_APP_INCIDENT_OCCURRED	🕒	Alerta asíncrona de Kaspersky Sandbox.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es la del componente Kasper:</li> <li>• GNRL_EA_PARAM_2 es la</li> <li>• GNRL_EA_PARAM_3 es la</li> <li>• GNRL_EA_PARAM_4 es el (SHA256).</li> </ul>
GNRL_EV_APP_LAUNCH_TESTED_DENIED	🕒	Inicio de la aplicación prohibido en modo de prueba (Control de aplicaciones).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_3 es la categoría que se creó m</li> <li>• GNRL_EA_PARAM_4 es la seguridad de la cuenta (:</li> <li>• GNRL_EA_PARAM_5 es la firma digital de la aplic</li> <li>• GNRL_EA_PARAM_6 es el archivo ejecutable de la ejemplo, chrome.exe).</li> <li>• GNRL_EA_PARAM_7 es el ejecutable.</li> </ul>

			<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_8 es e (SHA256).</li> <li>• GNRL_EA_PARAM_9 es la aplicación que el usuario ejecutar.</li> </ul>
GNRL_EV_APP_LAUNCH_TESTED_ALLOW		Inicio de la aplicación permitido en modo de prueba (Control de aplicaciones).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_3 es e categoría que se creó m</li> <li>• GNRL_EA_PARAM_4 es e seguridad de la cuenta (:</li> <li>• GNRL_EA_PARAM_5 es la categoría de la aplicació</li> </ul>
GNRL_EV_AC_USER_REQUEST		Mensaje al administrador por bloqueo del inicio de la aplicación (Control de aplicaciones).	<ul style="list-style-type: none"> <li>• GNRL_EA_DESCRIPTION usuario.</li> <li>• GNRL_EA_PARAM_2 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_6 es e archivo ejecutable de la ejemplo, chrome.exe).</li> <li>• GNRL_EA_PARAM_7 es la ejecutable.</li> <li>• GNRL_EA_PARAM_8 es e (SHA256).</li> <li>• GNRL_EA_PARAM_9 es la aplicación que el usuario ejecutar.</li> </ul>
GNRL_EV_WEB_URL_BLOCKED		Acceso denegado (Control Web).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es la</li> <li>• GNRL_EA_PARAM_2 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_3 es e regla de Control Web.</li> </ul>
GNRL_EV_WEB_URL_BLOCKED_BY_KSN		Acceso denegado por KSN (Control Web).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es la</li> <li>• GNRL_EA_PARAM_2 es e usuario de la sesión.</li> <li>• GNRL_EA_PARAM_3 es e regla de Control Web.</li> </ul>
GNRL_EV_WEB_URL_WARNING		Advertencia acerca de	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es la</li> </ul>

		contenido indeseado (Control Web).	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_2 es el usuario de la sesión.</li> <li>GNRL_EA_PARAM_3 es la regla de Control Web.</li> </ul>
GNRL_EV_WC_USER_REQUEST		Mensaje al administrador por bloqueo del acceso a la página web (Control Web).	<ul style="list-style-type: none"> <li>GNRL_EA_DESCRIPTION es el usuario.</li> <li>GNRL_EA_PARAM_1 es la regla de Control Web.</li> <li>GNRL_EA_PARAM_2 es el usuario de la sesión.</li> </ul>
GNRL_EV_DC_USER_REQUEST		Mensaje al administrador por bloqueo del acceso al dispositivo (Control de dispositivos).	<ul style="list-style-type: none"> <li>c_er_descr es el mensaje.</li> <li>GNRL_EA_PARAM_1 es la HWID.</li> <li>GNRL_EA_PARAM_2 es el usuario de la sesión.</li> </ul>
GNRL_EV_DEVCTRL_DEV_PLUGGED		Dispositivo enchufado (Control de dispositivos).	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es la HWID.</li> <li>GNRL_EA_PARAM_2 es el usuario de la sesión.</li> </ul>
GNRL_EV_DEVCTRL_DEV_UNPLUGGED		Dispositivo desenchufado (Control de dispositivos).	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es la HWID.</li> <li>GNRL_EA_PARAM_2 es el usuario de la sesión.</li> </ul>
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		Dispositivo enchufado bloqueado (Control de dispositivos).	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es la HWID.</li> <li>GNRL_EA_PARAM_2 es el usuario de la sesión.</li> </ul>
GNRL_EV_ADSEC_DETECT		Acción de proceso bloqueada/Acción de proceso omitida (Control de anomalías adaptativo).	<ul style="list-style-type: none"> <li>GNRL_EA_PARAM_1 es la regla de Control de anomalías.</li> <li>GNRL_EA_PARAM_2 es la heurística.</li> <li>GNRL_EA_PARAM_3 es el usuario de la sesión.</li> <li>GNRL_EA_PARAM_4 es el origen.</li> <li>GNRL_EA_PARAM_5 es el destino.</li> <li>GNRL_EA_PARAM_6 es el destino.</li> </ul>



			<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_7 es el destino.</li> <li>• GNRL_EA_PARAM_8 es información adicional sobre el objeto Hashes del proceso/objeto del proceso/objeto de destino. Proceso bloqueado (verdadero o falso). ID de seguridad del usuario.</li> </ul>
GNRL_EV_ADSEC_USER_REQUEST		Mensaje de bloqueo de la actividad de la aplicación al administrador (Control de anomalías adaptativo).	<ul style="list-style-type: none"> <li>• GNRL_EA_DESCRIPTION es el usuario.</li> <li>• GNRL_EA_PARAM_1 es el nombre de la regla de Control de anomalías.</li> <li>• GNRL_EA_PARAM_2 es el tipo de heurística.</li> <li>• GNRL_EA_PARAM_3 es el ID de usuario de la sesión.</li> <li>• GNRL_EA_PARAM_4 es el IP de origen.</li> <li>• GNRL_EA_PARAM_5 es el IP de origen.</li> <li>• GNRL_EA_PARAM_6 es el IP de destino.</li> <li>• GNRL_EA_PARAM_7 es el IP de destino.</li> <li>• GNRL_EA_PARAM_8 es información adicional sobre el objeto Hashes del proceso/objeto del proceso/objeto de destino. Proceso bloqueado (verdadero o falso). ID de seguridad del usuario.</li> </ul>
GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION		Acceso a los archivos bloqueado.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es el IP de destino.</li> <li>• GNRL_EA_PARAM_2 es el ID de usuario de la sesión.</li> <li>• GNRL_EA_PARAM_3 es el nombre del archivo ejecutable (por ejemplo, chrome.exe) de la aplicación que intentó acceder al archivo.</li> </ul>
GNRL_EV_ENCRYPTION_ERROR		Error en el cifrado/descifrado de archivos.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es el nombre del archivo.</li> <li>• GNRL_EA_PARAM_2 es el ID de usuario de la sesión.</li> </ul>

			<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_3 es el dispositivo.</li> </ul>
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		Operación con el dispositivo prohibida	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es la (HWID).</li> <li>• GNRL_EA_PARAM_2 es el usuario de la sesión.</li> </ul>
GNRL_EV_USB_FILE_OPERATION		Operación de archivo realizada (Control de dispositivos).	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es el archivo (escribir o borrar)</li> <li>• GNRL_EA_PARAM_2 es la</li> <li>• GNRL_EA_PARAM_3 es el dispositivo.</li> <li>• GNRL_EA_PARAM_4 es el usuario de la sesión.</li> <li>• GNRL_EA_PARAM_5 es la (HWID).</li> </ul>
GNRL_EV_HST_CMD_RESULT		Resultados de la tarea.	<ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 es la</li> <li>• GNRL_EA_PARAM_2 es el resultado de la ejecución del comando: <ul style="list-style-type: none"> <li>1 significa que el comando ejecutado correctamente</li> <li>2 significa que el comando no se pudo ejecutar</li> <li>3 significa que el comando fue eliminado correctamente</li> <li>4 significa que el comando no se pudo eliminar</li> </ul> </li> <li>• GNRL_EA_PARAM_3 es la descripción del comando y los fallos.</li> </ul>

## Información sobre el código de terceros

La información sobre el código de terceros se incluye en el archivo legal\_notices.txt, en la carpeta de instalación de la aplicación.

## Información de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Adobe, Acrobat, Flash, Reader y Shockwave son marcas registradas o marcas comerciales de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Apple, FireWire, Safari y iTunes son marcas comerciales de Apple Inc. registradas en los Estados Unidos y en otros países.

AutoCAD es una marca comercial o marca registrada de Autodesk, Inc. y/o de sus filiales y/o empresas afiliadas en los Estados Unidos y/o en otros países.

La palabra, marca y logotipos Bluetooth son propiedad de Bluetooth SIG, Inc.

Borland es una marca comercial o una marca registrada de Borland Software Corporation.

Android y Google Chrome son marcas comerciales de Google, Inc.

Citrix, Citrix Provisioning Services y XenDesktop son marcas comerciales de Citrix Systems, Inc. y/o de una o más de sus filiales, y pueden estar registradas en la Oficina de Patentes y Marcas Registradas de los Estados Unidos y en otros países.

Dell es una marca comercial de Dell, Inc. o sus filiales.

dBase es una marca de dataBased Intelligence, Inc.

EMC es una marca registrada o marca comercial de EMC Corporation en los EE. UU. y otros países.

Radmin es una marca registrada de Famatech.

IBM es una marca comercial de International Business Machines Corporation registrada en numerosas jurisdicciones de todo el mundo.

ICQ es una marca y/o una marca de servicio de ICQ LLC.

Intel es una marca comercial de Intel Corporation en los Estados Unidos y en otros países.

IOS es una marca comercial registrada de Cisco Systems, Inc. o sus empresas afiliadas en Estados Unidos y otros países.

Lenovo y ThinkPad son marcas comerciales de Lenovo en los Estados Unidos y/o en otros países.

Linux es la marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca registrada o marca comercial de Logitech en los Estados Unidos y/o en otros países.

LogMeIn Pro y Remotely Anywhere son marcas comerciales de LogMeIn, Inc.

Mail.ru es una marca comercial registrada de Mail.Ru, LLC.

McAfee es una marca comercial o una marca comercial registrada de McAfee, Inc. en los Estados Unidos y otros países.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface e Hyper-V son marcas comerciales de Microsoft Corporation en los Estados Unidos y en otros países.

Mozilla, Firefox y Thunderbird son marcas comerciales de Mozilla Foundation.

Java y JavaScript son marcas registradas de Oracle y/o de sus filiales.

VERISIGN es una marca registrada en los Estados Unidos y en otros países o una marca comercial no registrada de VeriSign, Inc. y sus subsidiarias.

VMware y VMware ESXi son marcas registradas o marcas comerciales de VMware, Inc. en los Estados Unidos y/o en otras jurisdicciones.

Thawte es una marca comercial o una marca comercial registrada de Symantec Corporation o sus empresas afiliadas en los Estados Unidos y otros países.

SAMSUNG es una marca comercial de SAMSUNG en los Estados Unidos y otros países.