kaspersky

# Kaspersky Endpoint Security para Windows 11.6.0

# Contenido

# 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 en forma remota?

ACTUALIZACIÓN

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

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

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

¿Puedo usar un servidor proxy para realizar una actualización?

SEGURIDAD

¿Cómo analiza Kaspersky Endpoint Security el correo electrónico?

¿Cómo evito que un archivo de confianza se analice?

¿Cómo protejo el equipo contra las unidades flash infectadas?

¿Cómo puedo 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 eliminó por error?

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

INTERNET

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

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

¿Cómo bloqueo las redes sociales?

APLICACIONES

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

¿Cómo evito que se ejecuten juegos de computadora?

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

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

DISPOSITIVOS

¿Cómo puedo impedir el uso de unidades flash?

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

¿Es posible obtener acceso a un dispositivo bloqueado?

CIFRADO

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

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

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

¿Podré 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 habilito la creación de archivos de volcado?

# Novedades

## Actualización 11.6.0

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

1. Compatibilidad con 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 ha agregado el componente Managed Detection and Response. El componente facilita la interacción con la solución Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* ofrece protección continua contra amenazas diseñadas para sortear defensas automatizadas. Estas amenazas son cada vez más comunes, y muchas organizaciones no han podido encontrar especialistas debidamente cualificados para hacerles frente o no tienen los recursos internos que se necesitan para defenderse. Para más detalles sobre el funcionamiento de la solución, *consulte la guía de ayuda de Kaspersky Managed Detection and Response*.

3. Kaspersky Endpoint Agent, aplicación incluida en el kit de distribución, se ha actualizado a la versión 3.10. Kaspersky Endpoint Agent 3.10 cuenta con nuevas funciones, mejoras de estabilidad y correcciones de errores. Para más detalles, consulte la documentación de las soluciones de Kaspersky que son compatibles con Kaspersky Endpoint Agent.

4. La aplicación ahora permite administrar la protección frente a ataques tales como escaneo de puertos y saturación de solicitudes en Configuración de Protección contra amenazas de red.

5. Se agregó un nuevo método para crear reglas de red para Firewall. Puede agregar reglas de paquetes y reglas de aplicaciones para las conexiones que se muestran en la ventana Monitor de red. Sin embargo, las opciones de conexión de las reglas de red se configurarán automáticamente.

6. La interfaz Monitor de red ya está mejorada. Se agregó la información sobre la actividad de red: Id. del proceso, que inicia la actividad de la red; el tipo de red (red local o Internet); puertos locales. De forma predeterminada, la información sobre el tipo de red está oculta.

7. A partir de ahora, la aplicación puede crear cuentas del Agente de autenticación en forma automática cuando detecta un usuario de Windows nuevo. Los usuarios emplean el Agente de autenticación para identificarse, obtener acceso a las unidades de sus equipos cuando estas han sido cifradas con la tecnología de Cifrado de disco de Kaspersky y cargar el sistema operativo. Kaspersky Endpoint Security examina las cuentas de Windows que se han creado en el equipo. Si detecta que una cuenta de Windows no tiene su correspondiente cuenta para el Agente de autenticación, crea esa cuenta para que el usuario pueda acceder a las unidades cifradas de su equipo. Esto quiere decir que ya no es necesario agregar cuentas del Agente de autenticación manualmente cuando las unidades de un equipo ya están cifradas.

8. A partir de esta versión, el proceso de cifrado de disco (con BitLocker o con Cifrado de disco de Kaspersky) puede monitorearse desde la interfaz de la aplicación en el equipo del usuario. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.

## Actualización 11.5.0

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

1. Compatibilidad con 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. Se actualizó la interfaz de la aplicación. También se actualizaron el icono de la aplicación en el área de notificación, las notificaciones de la aplicación y los cuadros de diálogo.

3. Se mejoró la interfaz del complemento web de Kaspersky Endpoint Security para los componentes Control de aplicaciones, Control de dispositivos y Control de anomalías adaptativo.

4. Se agregó una funcionalidad para importar y exportar listas de reglas y exclusiones en formato XML. El formato XML le permite editar listas después de exportarlas. Solo se puede administrar listas en la Consola de Kaspersky Security Center. Las siguientes listas están disponibles para exportar/importar:

   - Detección de comportamiento (lista de exclusiones).
   - Protección contra amenazas web (lista de direcciones web de confianza).
   - Protección contra amenazas de correo (lista de extensiones de filtro de archivos adjuntos).
   - Protección contra amenazas de 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 supervisados 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 agregó al informe de detección de amenazas. En versiones anteriores de la aplicación, Kaspersky Endpoint Security mostraba solo el SHA256 de un objeto.

6. Se agregó capacidad para asignar la prioridad para las reglas de acceso al dispositivo 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 agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de 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 para el grupo de administradores y asigne una prioridad de 1 para el 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. Se agregó una nueva funcionalidad:

   - Administrar notificaciones de audio.
   - Redes basadas en costos Kaspersky Endpoint Security limita su propio tráfico de red si la conexión a Internet es limitada (por ejemplo, a través de una conexión móvil).
   - Administre la configuración de Kaspersky Endpoint Security a través de aplicaciones de administración remota de confianza (como TeamViewer, LogMeIn Pro y Remotely Anywhere). Puede utilizar aplicaciones de administración remota para iniciar Kaspersky Endpoint Security y administrar la configuración en la interfaz de la aplicación.
   - Administre 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 habilita automáticamente el uso del almacenamiento de certificados de Windows en Firefox y Thunderbird.

8. Se agregó una capacidad para configurar el modo de análisis de tráfico seguro: siempre analice el tráfico, aunque los componentes de protección están deshabilitados, o analice el tráfico cuando lo soliciten los componentes de protección.

9. Se revisó el procedimiento para eliminar información de informes. Un usuario solo 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. Se revisó el procedimiento para importar un archivo de configuración que contiene la configuración de Kaspersky Endpoint Security y el 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, podía ver los valores de la nueva configuración antes de que se aplicaran.

11. Se simplificó el 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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

13. Se agregó capacidad para ingresar comentarios en las propiedades de aplicaciones de confianza. Los comentarios ayudan a simplificar las búsquedas y la clasificación de aplicaciones de confianza.

14. Uso de la API REST para administrar la aplicación:

    - Ahora existe la capacidad de ajustar la configuración de la extensión Protección contra amenazas de correo para Outlook.

    - Está prohibido deshabilitar 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. Se renovó el diseño del icono que la aplicación coloca en el área de notificación de la barra de tareas. El nuevo icono es  (el anterior era ). El icono cambia a  cuando se necesita que el usuario realice alguna acción (por ejemplo, reiniciar el equipo tras una actualización del software). Cuando hay componentes de protección deshabilitados o que no funcionan correctamente, el icono cambia a  o a . El usuario puede posar el puntero del mouse sobre el icono para que Kaspersky Endpoint Security le muestre una descripción del problema de protección.

2. Kaspersky Endpoint Agent, que forma parte del kit de distribución, se ha actualizado a la versión 3.9. Kaspersky Endpoint Agent 3.9 permite la integración con nuevas soluciones de Kaspersky. Para más detalles, consulte la documentación de las soluciones de Kaspersky que son compatibles con Kaspersky Endpoint Agent.

3. Los componentes de Kaspersky Endpoint Security ahora pueden tener el estado *No compatible con la licencia*. Para ver el estado de los distintos componentes, haga clic en el botón **Componentes de protección** de la ventana principal de la aplicación.

4. Los informes ahora pueden incluir nuevos eventos vinculados al componente Prevención de exploits.

5. Los controladores de la tecnología Cifrado de disco de Kaspersky ahora se agregan automáticamente al Entorno de recuperación de Windows (WinRE) cuando comienza el proceso de cifrado de una unidad. En la versión anterior, los controladores se agregaban durante la instalación de Kaspersky Endpoint Security. Agregar estos controladores al entorno de WinRE ayuda a mejorar la estabilidad de la aplicación al momento de recuperar el sistema operativo de un equipo protegido con Cifrado de disco de Kaspersky.

El componente Sensor de Endpoint ya no forma parte de Kaspersky Endpoint Security. No obstante ello, aún podrá usar una directiva para configurar los ajustes de este componente en equipos con Kaspersky Endpoint Security versiones 11.0.0 a 11.3.0.

# Kaspersky Endpoint Security para Windows

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

Para proteger su equipo, Kaspersky Endpoint Security utiliza las siguientes tecnologías de detección de amenazas:

- **Aprendizaje automático**. Kaspersky Endpoint Security utiliza un modelo basado en el aprendizaje automático. Los expertos de Kaspersky desarrollaron este modelo. Durante su uso, el modelo recibe continuamente datos actualizados de amenazas de KSN, lo que permite entrenar el modelo.

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

- **Análisis de expertos**. Kaspersky Endpoint Security utiliza datos de amenazas agregados por los analistas de virus de Kaspersky. Los analistas de virus comprueban los objetos de forma manual si la reputación de un objeto no se puede determinar automáticamente.

- **Análisis de comportamiento**. Kaspersky Endpoint Security analiza la actividad de un objeto en tiempo real.

- **Análisis automático**. Kaspersky Endpoint Security recibe datos de un sistema automático de análisis de objetos. El sistema procesa todos los objetos recibidos por Kaspersky, determina la reputación de los objetos y agrega los datos correspondientes a las bases de datos antivirus. Si el sistema no puede determinar la reputación de un objeto, envía una solicitud a los analistas de virus de Kaspersky.

- **Kaspersky Sandbox**. Kaspersky Endpoint Security analiza los objetos en una máquina virtual. Kaspersky Sandbox analiza el comportamiento de un objeto y toma una decisión sobre su reputación. Esta tecnología solo está disponible si utiliza Kaspersky Sandbox.

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

Los siguientes componentes de la aplicación son componentes de control:

- **Control de aplicaciones**. Este componente realiza un seguimiento de los intentos del usuario para iniciar aplicaciones y regula el inicio de las aplicaciones.

- **Control de dispositivos**. Este componente le permite configurar restricciones de acceso a dispositivos de almacenamiento de datos (por ejemplo: discos duros, unidades extraíbles y discos CD/DVD), a equipos de transmisión de datos (por ejemplo: módems), a equipos que convierten información (como las impresoras) o a interfaces para conectar dispositivos a equipos (como USB y Bluetooth).

- **Control Web**. Este componente le permite establecer restricciones flexibles de acceso a recursos web para diferentes grupos de usuarios.

- **Control de anomalías adaptativo**. El componente detecta y controla acciones que no son típicas para el equipo protegido y que podrían resultar dañinas.

Los siguientes componentes de la aplicación son componentes de protección:

- **Detección de comportamientos**. Este componente recibe información sobre la actividad de las aplicaciones en el equipo y remite esos datos a los demás componentes para lograr una protección más efectiva.

- **Prevención de exploits**. Este componente realiza un seguimiento de los archivos ejecutables que son ejecutados por aplicaciones vulnerables. Cuando hay un intento de ejecutar un archivo ejecutable de parte de

una aplicación vulnerable que no fue iniciado por el usuario, Kaspersky Endpoint Security bloquea la ejecución de este archivo.

- **Prevención contra intrusos** Este componente registra las acciones de las aplicaciones en el sistema operativo y regula la actividad de las aplicaciones según el grupo de confianza de una determinada aplicación. Se especifica un conjunto de reglas para cada grupo de aplicaciones. Estas reglas regulan el acceso de las aplicaciones a los datos personales del usuario y a los recursos del sistema operativo. Dichos datos incluyen archivos de usuario en la carpeta Documentos, cookies, archivos de registro de actividad del usuario y archivos, carpetas y claves de registro que contienen configuraciones e información importante para las aplicaciones de uso más frecuente.

- **Motor de reparación**. Este componente permite a Kaspersky Endpoint Security deshacer acciones que han sido realizadas por el malware en el sistema operativo.

- **Protección contra amenazas de archivos**. Este componente impide la infección del sistema de archivos del equipo. El componente se inicia inmediatamente después de que se inicie Kaspersky Endpoint Security; permanece continuamente en la memoria RAM del dispositivo y analiza todos los archivos que se abren, guardan o inician en el equipo y en todos los dispositivos de almacenamiento conectados. Este componente intercepta todos los intentos de acceso a un archivo y analiza el archivo en busca de virus y otras amenazas.

- **Protección contra amenazas web**. Este componente analiza el tráfico que llega al equipo del usuario a través de los protocolos HTTP y FTP, y verifica si las direcciones web son malintencionadas o phishing.

- **Protección contra amenazas de correo**. Este componente analiza los mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas.

- **Protección contra amenazas de red** Este componente revisa el tráfico de red entrante en busca de actividades que sean típicas de los ataques de red. Al detectar un intento de ataque de red dirigido a su equipo, Kaspersky Endpoint Security bloquea la actividad de red del equipo atacante.

- **Firewall**. Este componente protege los datos personales que se almacenan en el equipo y bloquea la mayoría de las amenazas al sistema operativo mientras el equipo está conectado a Internet o a una red de área local.

- **Prevención de ataques BadUSB**. Este componente impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo.

- **Protección vía AMSI**. El componente analiza objetos cuando lo solicita una aplicación de terceros, a la cual le remite luego el resultado del análisis.

Aunque los componentes de la aplicación protegen el equipo en tiempo real, se recomienda *realizar análisis* periódicamente para detectar virus y otras amenazas. Esto ayuda a descartar la posibilidad de propagar malware que no fue detectado por los componentes de protección, por ejemplo, debido a un nivel bajo de seguridad.

Para evitar que la protección del equipo quede obsoleta, es necesario *actualizar las bases de datos y los módulos* de la aplicación. La aplicación se actualiza automáticamente de forma predeterminada, pero, si es necesario, puede actualizar manualmente las bases de datos y los módulos de la aplicación.

Las siguientes tareas se proporcionan en Kaspersky Endpoint Security:

- **Comprobación de integridad**. Kaspersky Endpoint Security verifica los módulos de la aplicación presentes en la carpeta de instalación de la aplicación en busca de fallas o modificaciones. Si un módulo de la aplicación tiene una firma digital incorrecta, el módulo se considera dañado.

- **Análisis completo**. Kaspersky Endpoint Security analiza el sistema operativo, e incluye la memoria del kernel, los objetos que se cargan al sistema operativo durante el inicio, los sectores de arranque del disco, el almacenamiento de las copias de seguridad del sistema operativo y todos los discos duros y unidades extraíbles.

- **Análisis personalizado**. Kaspersky Endpoint Security analiza los objetos que selecciona el usuario.

- **Análisis de áreas críticas**. Kaspersky Endpoint Security analiza la memoria del kernel, los objetos que se cargan en el inicio del sistema operativo y los sectores de arranque del disco.

- **Actualización**. Kaspersky Endpoint Security descarga bases de datos y módulos de la aplicación actualizados. El proceso de actualización mantiene al equipo protegido contra los últimos virus y otras amenazas.

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

## Funciones de servicio de la aplicación

Kaspersky Endpoint Security incluye una gran cantidad de funciones de servicio. Se proporcionan funciones de servicio para mantener la aplicación actualizada, ampliar su funcionalidad y ayudar al usuario con la operación 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 eventos que ocurrieron durante la operación de Kaspersky Endpoint Security y de todas las operaciones que realiza la aplicación. En caso de que se produzca un incidente, puede enviar los informes a Kaspersky, donde los especialistas del Servicio de soporte técnico podrán examinar su problema en profundidad.

- **Almacenamiento de datos**. Si la aplicación detecta archivos infectados mientras realiza un análisis del equipo en busca de virus y otras amenazas, bloquea estos archivos. Kaspersky Endpoint Security almacena las copias de los archivos desinfectados y eliminados en *Copias de seguridad*. Kaspersky Endpoint Security mueve a la *lista de amenazas activas* los archivos que no se procesaron por algún motivo. Puede analizar archivos, restaurar archivos para que regresen a sus carpetas originales y vaciar el almacenamiento de datos.

- **Servicio de notificación**. El servicio de notificación ayuda al usuario a rastrear los eventos que influyen en el estado de protección del equipo y la operación de Kaspersky Endpoint Security. Las notificaciones se pueden ver 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 mediante el uso en tiempo real de la información sobre la reputación de los archivos, los recursos web y el software recibido de los usuarios de todo el mundo.

- **Licencia**. La compra de una licencia habilita todas las funcionalidades de la aplicación, proporciona acceso a las actualizaciones de los módulos y las bases de datos de la aplicación y ofrece soporte técnico por teléfono o correo electrónico para temas relacionados con la instalación, la configuración y el uso de la aplicación.

- **Soporte**. Todos los usuarios registrados de Kaspersky Endpoint Security pueden comunicarse con los especialistas del Servicio de soporte técnico para recibir ayuda. Puede enviar una solicitud al soporte técnico de Kaspersky a través del portal Kaspersky CompanyAccount y o llamar al Servicio de soporte técnico por teléfono.

Si la aplicación devuelve errores o se cuelga durante la operación, se puede reiniciar en forma automática.

Si la aplicación encuentra errores recurrentes que causan que la aplicación se cierre, la aplicación realiza las siguientes operaciones:

1. Deshabilita las funciones de control y protección (la función de cifrado permanece activa).

2. Notifica al usuario que las funciones se han deshabilitado.

3. Intenta restaurar la aplicación a un estado funcional tras actualizar las bases de datos antivirus o aplicar actualizaciones a los módulos de la aplicación.

## Kit de distribución

El kit de distribución incluye los siguientes paquetes de distribución:

- **Cifrado fuerte (AES256)**

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

- **Cifrado ligero (AES56)**

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

Cada paquete de distribución contiene los siguientes archivos:

| | |
|---|---|
| `kes_win.msi` | Paquete de instalación de Kaspersky Endpoint Security. |
| `setup_kes.exe` | Los archivos necesarios para instalar la aplicación utilizando cualquiera de los métodos disponibles. |
| `kes_win.kud` | Archivo para crear paquetes de instalación para Kaspersky Endpoint Security. |
| `klcfginst.msi` | Paquete de instalación 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 incompatible. |
| `incompatible.txt` | Archivo que contiene una lista de software incompatible. |
| `ksn_<language_ID>.txt` | Archivo donde puede leer los términos de participación en Kaspersky Security Network. |
| `license.txt` | Archivo donde puede leer el Contrato de licencia de usuario final y la Política de privacidad. |
| `installer.ini` | Archivo installer.ini que contiene las configuraciones internas del kit de distribución. |
| `endpointagent.msi` | Paquete de instalación de Kaspersky Endpoint Agent 3.10, software que permite 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 que contiene los archivos necesarios para instalar el complemento web de Kaspersky Endpoint Security. |

No se recomienda cambiar los valores de esta configuración. Si quiere cambiar opciones de instalación, use el archivo setup.ini.

## Requisitos de hardware y software

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

Requisitos mínimos generales:

- 2 GB de espacio libre en disco en la unidad de disco duro
- CPU:
  - Estación de trabajo: 1 GHz
  - Servidor: 1.4 GHz
  - Compatibilidad con el conjunto de instrucciones SSE2
- RAM:
  - Estación de trabajo (x86): 1 GB
  - Estación de trabajo (x64): 2 GB
  - Servidor: 2 GB
- Microsoft .NET Framework 4.0 o superior

Sistemas operativos admitidos en 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.

Microsoft ha dejado de utilizar el algoritmo de firma del módulo SHA-1. Se requiere la actualización KB4474419 para la instalación correcta de Kaspersky Endpoint Security en un equipo con el sistema operativo Microsoft Windows 7. Para obtener más detalles sobre 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.

Sistemas operativos admitidos en servidores:

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

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

- Windows MultiPoint Server 2011 (64 bits)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 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

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

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

Tipos de servidores de terminales compatibles:

- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services basado en Windows Server 2012;
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2012 R2;
- Microsoft Remote Desktop Services basado en Windows Server 2016;
- Servicios de Escritorio remoto de Microsoft basados en Windows Server 2019.

Plataformas virtuales admitidas:

- VMware Workstation 16 Pro
- VMware ESXi 7.0 Update 1a
- Microsoft Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Kaspersky Endpoint Security es compatible con el funcionamiento de las siguientes versiones de Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Parche A
- Kaspersky Security Center 12 Parche B
- Kaspersky Security Center 13
- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2

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

El conjunto de características disponibles en Kaspersky Endpoint Security depende de si el sistema operativo está diseñado para estaciones de trabajo o para servidores (consulte la siguiente tabla).

Comparación de las características de Kaspersky Endpoint Security

| Característica | Estaciones de trabajo | Servidores |
|---|---|---|
| **Protección avanzada contra amenazas** | | |
| Kaspersky Security Network | ✓ | ✓ |
| Detección de comportamientos | ✓ | ✓ |
| Prevención de exploits | ✓ | ✓ |
| Prevención contra intrusos | ✓ | – |
| Motor de reparación | ✓ | ✓ |
| **Protección básica contra amenazas** | | |
| Protección contra amenazas de archivos | ✓ | ✓ |
| Protección contra amenazas web | ✓ | – |
| Protección contra amenazas de correo | ✓ | – |
| Firewall | ✓ | ✓ |
| Protección contra amenazas de red | ✓ | ✓ |
| Prevención de ataques BadUSB | ✓ | ✓ |
| Protección vía AMSI | ✓ | ✓ |
| **Controles de seguridad** | | |
| Control de aplicaciones | ✓ | ✓ |
| Control de dispositivos | ✓ | – |

| | | |
|---|---|---|
| Control Web | ✓ | – |
| Control de anomalías adaptativo | ✓ | – |
| **Cifrado de datos** | | |
| Cifrado de Disco de Kaspersky | ✓ | – |
| Cifrado de Unidad BitLocker | ✓ | ✓ |
| Cifrado de archivos | ✓ | – |
| Cifrado de unidades extraíbles | ✓ | – |
| **Endpoint Agent** | ✓ | ✓ |
| **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 de más abajo).

Para administrar la aplicación, se pueden utilizar las siguientes consolas de Kaspersky Security Center 12:

- Consola de administración. Complemento para Microsoft Management Console (MMC) que se instala en la estación de trabajo del administrador.
- Web Console. Componente de Kaspersky Security Center que se instala en el Servidor de administración. Para trabajar con Web Console, utilice el navegador de cualquier equipo que tenga acceso al Servidor de administración.

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

Comparación de las características de Kaspersky Endpoint Security

| Característica | Kaspersky Security Center 12 | | Kaspersky Security Center |
|---|---|---|---|
| | Consola de administración | Web Console | Cloud Console |
| **Protección avanzada contra amenazas** | | | |
| Kaspersky Security Network | ✓ | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ | – |
| Detección de comportamientos | ✓ | ✓ | ✓ |
| Prevención de exploits | ✓ | ✓ | ✓ |
| Prevención contra intrusos | ✓ | ✓ | ✓ |
| Motor de reparación | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| **Protección básica contra amenazas** | | | |
| Protección contra amenazas de archivos | ✓ | ✓ | ✓ |
| Protección contra amenazas web | ✓ | ✓ | ✓ |
| Protección contra amenazas de correo | ✓ | ✓ | ✓ |
| Firewall | ✓ | ✓ | ✓ |
| Protección contra amenazas de red | ✓ | ✓ | ✓ |
| Prevención de ataques BadUSB | ✓ | ✓ | ✓ |
| Managed Detection and Response | ✓ | ✓ | ✓ |
| Protección vía AMSI | ✓ | ✓ | ✓ |
| **Controles de seguridad** | | | |
| Control de aplicaciones | ✓ | ✓ | ✓ |
| Control de dispositivos | ✓ | ✓ | ✓ |
| Control Web | ✓ | ✓ | ✓ |
| Control de anomalías adaptativo | ✓ | ✓ | ✓ |
| **Cifrado de datos** | | | |
| Cifrado de Disco de Kaspersky | ✓ | ✓ | – |
| Cifrado de Unidad BitLocker | ✓ | ✓ | ✓ |
| Cifrado de archivos | ✓ | ✓ | – |
| Cifrado de unidades extraíbles | ✓ | ✓ | – |
| **Endpoint Agent** | ✓ | ✓ | ✓ |
| **Tareas** | | | |
| Añadir clave | ✓ | ✓ | ✓ |
| Cambiar la selección de componentes de la aplicación | ✓ | ✓ | ✓ |
| Inventario | ✓ | ✓ | ✓ |
| Actualización | ✓ | ✓ | ✓ |
| Reversión de actualizaciones | ✓ | ✓ | ✓ |
| Análisis antivirus | ✓ | ✓ | ✓ |
| Comprobación de integridad | ✓ | ✓ | – |
| Eliminación de datos | ✓ | ✓ | ✓ |
| Administración de cuentas del Agente de autenticación | ✓ | ✓ | – |

## Compatibilidad con otras aplicaciones

Antes de la instalación, Kaspersky Endpoint Security comprueba el equipo para encontrar aplicaciones de Kaspersky. La aplicación también comprueba que no haya software no compatible en el equipo. La lista de software incompatible se encuentra en el archivo incompatible.txt, que forma parte del 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 (incluida la aplicación Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (incluido el componente Sensor de Endpoint).

  Si el componente Endpoint Agent se instaló en un equipo con las herramientas de despliegue de otras aplicaciones de Kaspersky, se lo eliminará automáticamente cuando instale Kaspersky Endpoint Security. Sensor de Endpoint y Kaspersky Endpoint Agent pueden instalarse como parte de Kaspersky Endpoint Security; para incluirlos en la instalación, seleccione 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 a que finalice 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 manera local, utilizando el Asistente de instalación;
- de manera local, utilizando la línea de comandos;
- de manera remota, a través de Kaspersky Security Center 12;
- de manera remota, utilizando el Editor de administración de directivas de grupo de Microsoft Windows (para más información, consulte el *sitio web de soporte técnico de Microsoft*);
- de manera remota, utilizando System Center Configuration Manager.

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

1. los valores recibidos del archivo setup.ini,
2. los valores recibidos del archivo installer.ini,
3. los valores recibidos de la línea de comandos.

Se recomienda cerrar todas las aplicaciones en ejecución antes de iniciar la instalación de Kaspersky Endpoint Security (incluida la instalación remota).

## Despliegue mediante Kaspersky Security Center 12

Kaspersky Endpoint Security puede desplegarse en equipo dentro de una red corporativa de varias maneras. Puede elegir el escenario de despliegue más adecuado para su organización o combinar varios escenarios de despliegue al mismo tiempo. Los principales métodos de despliegue que admite Kaspersky Security Center 12 son los siguientes:

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

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

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

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

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

Kaspersky Security Center 12 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 12*.

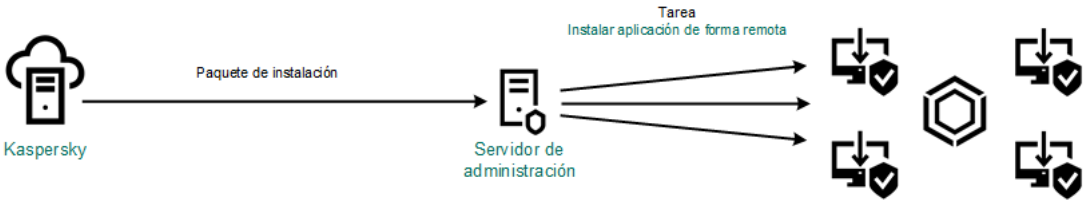
## Instalación estándar de la aplicación

Kaspersky Security Center cuenta con un Asistente de despliegue de la protección, que puede usar para instalar la aplicación en los equipos de la empresa. El Asistente de despliegue de protección incluye las siguientes acciones principales:

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

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

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




Implementación de Kaspersky Endpoint Security

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

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

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

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

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

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

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

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

### Paso 2. Seleccionar los dispositivos en los que se instalará el software

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

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

### Paso 3. Configurar la tarea de instalación remota

Configure los siguientes parámetros adicionales:

- **Fuerce la descarga del paquete de instalación**. Seleccione el método con el que se instalará la aplicación:
  - **Utilización del Agente de red**. Si el Agente de red no se ha instalado en la equipo, el primer Agente de red se instalará utilizando las herramientas del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.

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

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

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

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

- **Asignar la instalación del Agente de red en las directivas de grupo de Active Directory**. Instalar el Agente de red en forma manual, utilizando los recursos de Active Directory. Para instalar el Agente de red, la tarea de instalación remota debe ejecutarse con privilegios de administrador de dominio.

### Paso 4. Seleccionar una clave de licencia

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

### Paso 5. Seleccionar la opción de reinicio del sistema operativo

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

### Paso 6. Eliminar las aplicaciones incompatibles antes de la instalación

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

### Paso 7. Seleccionando una cuenta para acceder a los dispositivos

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

### Paso 8. Comienzo de la instalación

Salga del Asistente. De ser necesario, active la casilla **No ejecutar la tarea después de que el Asistente de instalación remota finalice**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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

En la ventana principal de Web Console, seleccione **Despliegue y descubrimiento de dispositivos → Despliegue y asignación → Asistente de despliegue de la seguridad**.

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

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

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

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

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

### Paso 2. Seleccionar una clave de licencia

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

### Paso 3. Selección del Agente de red

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

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

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

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

### Paso 5. Configuración de los parámetros avanzados

Configure los siguientes parámetros adicionales:

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

### Paso 6. Seleccionar la opción de reinicio del sistema operativo

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

### Paso 7. Eliminar las aplicaciones incompatibles antes de la instalación

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

### Paso 8. Asignación a un grupo de administración

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

### Paso 9. Seleccionando una cuenta para acceder a los dispositivos

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

### Paso 10. Iniciar la instalación

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

## Creación de un paquete de instalación

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

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

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

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

2. Haga clic en 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

Escriba el nombre que se le dará al paquete de instalación, por ejemplo `Kaspersky Endpoint Security para Windows 11.6.0`.

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

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

De ser necesario, active la casilla **Copiar actualizaciones del repositorio al paquete de instalación** para que se actualicen las bases de datos antivirus incluidas en el paquete de instalación.

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

Lea y acepte los términos del Contrato de licencia de usuario final y de la Política de privacidad.

Se creará el paquete de instalación y se lo agregará a Kaspersky Security Center. Con el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación. Puede modificar la configuración del paquete para definir qué componentes se instalarán y establecer los parámetros que se usarán durante la instalación (consulte la siguiente tabla). El paquete de instalación contendrá las bases de datos antivirus que existan en el repositorio del Servidor de administración. Si lo desea, puede actualizar las bases de datos incluidas en el paquete de instalación para que se requiera menos tráfico para actualizarlas cuando concluya la instalación de Kaspersky Endpoint Security.

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

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

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

2. Haga clic en el botón **Agregar**.

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

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

## Paso 2. Paquetes de instalación

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

Se creará el paquete de instalación y se lo agregará a Kaspersky Security Center. Con el paquete de instalación, puede instalar Kaspersky Endpoint Security en los equipos de la red corporativa o actualizar la versión de la aplicación. Puede modificar la configuración del paquete para definir qué componentes se instalarán y establecer los parámetros que se usarán durante la instalación (consulte la siguiente tabla). El paquete de instalación contendrá las bases de datos antivirus que existan en el repositorio del Servidor de administración. Si lo desea, puede actualizar las bases de datos incluidas en el paquete de instalación para que se requiera menos tráfico para actualizarlas cuando concluya la instalación de Kaspersky Endpoint Security.

Configuraciones del paquete de instalación

| Sección | Descripción |
|---|---|
| **Componentes de protección** | En esta sección, puede seleccionar los componentes de la aplicación que estarán disponibles. El conjunto de componentes puede modificarse posteriormente a través de la tarea *Cambiar componentes de la aplicación*. El componente Prevención de ataques BadUSB, el componente Endpoint Agent y los componentes de cifrado de datos no se instalan de forma predeterminada. Si desea utilizar estos componentes, puede agregarlos en la configuración del paquete de instalación. |
| **Configuración de instalación** | **Agregar la ubicación de la aplicación a la variable de entorno %PATH%**. Puede agregar la ruta de instalación a la variable %PATH% para facilitar el uso de la interfaz de línea de comandos.<br>**No proteger el proceso de instalación**. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda que desactive la protección del proceso de instalación. |

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

**Ruta de la carpeta de instalación de la aplicación**. 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 for Windows`.

**Archivo de configuración**. Puede cargar un archivo que defina la configuración de Kaspersky Endpoint Security. Puede crear un archivo de configuración en la interfaz local de la aplicación.

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

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

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

Para actualizar las bases de datos incluidas en el paquete de instalación, puede usar la Consola de administración o Kaspersky Security Center 12 Web Console. No es posible usar Kaspersky Security Center Cloud Console para este fin.

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

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

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

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

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

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

2. Haga clic en el paquete de instalación de Kaspersky Endpoint Security que contenga las bases de datos que deban actualizarse.

   Se abrirá la ventana de propiedades del paquete de instalación.

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

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

## Creación de una tarea de instalación remota

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

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

1. 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**.

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

### Paso 1. Selección del tipo de tarea

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

### Paso 2. Seleccionar un paquete de instalación.

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

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

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

### Paso 3. Adicional

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

### Paso 4. Configuración

Configure los siguientes parámetros adicionales:

- **Fuerce la descarga del paquete de instalación**. Seleccione el método con el que se instalará la aplicación:
  - **Utilización del Agente de red**. Si el Agente de red no se ha instalado en la equipo, el primer Agente de red se instalará utilizando las herramientas del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.
  - **Uso de recursos del sistema operativo a través de puntos de distribución**. El paquete de instalación se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si hay al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, *consulte la Ayuda de Kaspersky Security Center*.
  - **Uso de recursos del sistema operativo a través del Servidor de administración**. Los archivos se entregarán a los equipos cliente mediante el uso de los recursos del sistema operativo a través del Servidor de administración. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.

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

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

### Paso 5. Seleccionar la opción de reinicio del sistema operativo

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

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

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

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.

- Seleccione los equipos no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. El Agente de red no está instalado en dispositivos no asignados. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.

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

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

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

### Paso 8. Programación de la tarea

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

### Paso 9. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo `Instalar Kaspersky Endpoint Security para Windows 11.6.0`.

### Paso 10. Fin de la creación de la tarea

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. La aplicación se instalará en modo silencioso. Después de la instalación, el icono aparecerá en al área de notificación del equipo del usuario. Si el icono que aparece es , compruebe si la aplicación está activada.

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

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

   Se abre la lista de tareas.

2. Haga clic en el botón **Agregar**.

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

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

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Instalar aplicación remotamente**.
3. En el campo **Nombre de la tarea**, ingrese una breve descripción, por ejemplo, `Instalación de Kaspersky Endpoint Security para administradores`.
4. En la sección **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

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

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

### Paso 3. Configuración de un paquete de instalación

En este paso, ajuste la configuración del paquete de instalación**:**

1. Seleccione el paquete de instalación de Kaspersky Endpoint Security para Windows (11.6.0).
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 instala otra vez.
3. En la sección **Forzar descarga del paquete de instalación**, seleccione el método de installation de la aplicación:

   - **Utilización del Agente de red**. Si el Agente de red no se ha instalado en la equipo, el primer Agente de red se instalará utilizando las herramientas del sistema operativo. Luego, Kaspersky Endpoint Security se instala con las herramientas del Agente de red.
   - **Uso de recursos del sistema operativo a través de puntos de distribución**. El paquete de instalación se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si hay al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, *consulte la Ayuda de Kaspersky Security Center*.

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

4. En el campo **Número máximo de descargas simultáneas**, establezca un límite en el número de solicitudes de descarga de paquete de instalación enviadas al Servidor de administración. Un límite en el número de solicitudes ayudará a evitar que la red se sobrecargue.

5. En el campo **Número de intentos de instalación**, establezca un límite en el número de intentos para instalar la aplicación. Si la instalación de Kaspersky Endpoint Security finaliza con un error, la tarea iniciará automáticamente la instalación nuevamente.

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

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

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

9. Si es necesario, seleccione la casilla de verificación **Ofrecer a los usuarios que dejen de ejecutar aplicaciones**. La instalación de Kaspersky Endpoint Security utiliza los recursos informáticos. Para la comodidad del usuario, el Asistente de instalación de aplicaciones le solicita que cierre las aplicaciones en ejecución antes de iniciar la instalación. Esto ayuda a evitar interrupciones en el funcionamiento de otras aplicaciones y evita posibles fallos de funcionamiento de el equipo.

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

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

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

### Paso 5. Completar creación de la tarea

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

# Instalación local a través del Asistente

La interfaz del Asistente de instalación de la aplicación consiste en una secuencia de ventanas correspondiente a los pasos de instalación de la aplicación.

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

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

   Se inicia el Asistente de instalación.

## Preparativos para la instalación

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

- 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 los requisitos de hardware y software.
- Si el usuario tiene los derechos necesarios para instalar el producto de software.

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

Si el equipo cumple los requisitos mencionados anteriormente, el Asistente de instalación busca las aplicaciones de Kaspersky que podrían generar conflictos de ejecutarse mientras se está instalando la aplicación. Si se encuentran estas aplicaciones, se le pregunta si desea eliminarlas manualmente.

Si las aplicaciones detectadas incluyen versiones anteriores de Kaspersky Endpoint Security, todos los datos que se pueden migrar (por ejemplo, los datos de activación y la configuración de la aplicación) se conservan y se usan durante la instalación de Kaspersky Endpoint Security 11.6.0 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 1 Maintenance Release 4 para Windows (compilación 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 para Windows (versión 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 para Windows (compilación 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 para Windows (compilación 10.3.0.6294).
- 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 (versión 11.0.0.6499)
- Kaspersky Endpoint Security 11.0.1 para Windows (versión 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 (versión 11.1.0.15919)
- Kaspersky Endpoint Security 11.1.1 para Windows (versión 11.1.1.126)
- Kaspersky Endpoint Security 11.2.0 para Windows (versión 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 (versión 11.3.0.773)
- Kaspersky Endpoint Security 11.4.0 para Windows (versión 11.4.0.233)
- Kaspersky Endpoint Security 11.5.0 para Windows (versión 11.5.0.590)

## Componentes de Kaspersky Endpoint Security

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

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

- Prevención de ataques BadUSB.
- Cifrado de archivos.
- Cifrado de disco completo.
- Administración de BitLocker.
- Endpoint Agent. Si selecciona el componente *Endpoint Agent*, se instalará Kaspersky Endpoint Agent 3.10 para permitir que la aplicación interactúe con ciertas soluciones de Kaspersky diseñadas para detectar amenazas avanzadas (por ejemplo, Kaspersky Sandbox).

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

## La configuración avanzada

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

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

**Agregar la ubicación de la aplicación a la variable de entorno %PATH%**. Puede agregar la ruta de instalación a la variable %PATH% para facilitar el uso de la interfaz de línea de comandos.

# Instalación de la aplicación desde la línea de comandos

Kaspersky Endpoint Security puede instalarse a través de la línea de comandos en dos modos:

- En modo interactivo usando el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez iniciada la instalación en modo silencioso, no es necesaria su participación en el proceso de instalación. Para instalar la aplicación en modo silencioso, use los modificadores `/s` y `/qn`.

  Antes de instalar la aplicación en modo silencioso, abra y lea el Contrato de licencia de usuario final y el texto de la Política de privacidad. Encontrará ambos documentos en el kit de distribución de Kaspersky Endpoint Security. Instale la aplicación únicamente si ha leído y comprende y acepta en su totalidad las disposiciones y los términos del Contrato de licencia de usuario final; si comprende y acepta el hecho de que sus datos se procesarán y transmitirán (incluso a otros países) según lo descrito en la Política de privacidad; y si ha leído y comprende en su totalidad la Política de privacidad. Si no está de acuerdo con las disposiciones y los términos del Contrato de licencia de usuario final y de la Política de privacidad, no instale ni utilice Kaspersky Endpoint Security.

*Para instalar la aplicación o actualizar una versión anterior de la aplicación:*

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/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

   ```
   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]
   ```

| | |
|---|---|
| `EULA=1` | Aceptación de los términos del Contrato de licencia de usuario final. El texto del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security.<br><br>Es necesario aceptar los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar su versión. |
| `PRIVACYPOLICY=1` | Aceptación de la Política de privacidad. El texto de la Política de privacidad se incluye en el kit de distribución de Kaspersky Endpoint Security.<br><br>Para instalar la aplicación o actualizar la versión de la aplicación, deberá aceptar la Directiva de privacidad. |

| | |
|---|---|
| KSN | Participar o negarse a participar en Kaspersky Security Network. Si no especifica ningún valor para este parámetro, se le preguntará si desea participar en KSN cuando inicie Kaspersky Endpoint Security por primera vez. Valores disponibles:<br>• 1: participar en KSN.<br>• 0: negarse a participar en KSN (valor predeterminado).<br>El paquete de distribución de Kaspersky Endpoint Security está optimizado para ser utilizado con Kaspersky Security Network. Si opta por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que se haya completado la instalación. |
| ALLOWREBOOT=1 | Permitir que el equipo se reinicie automáticamente, de ser necesario, cuando la aplicación termine de instalarse o actualizarse. Si no especifica ningún valor para este parámetro, se bloquea el reinicio automático del equipo.<br>No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación. |
| SKIPPRODUCTCHECK=1 | Deshabilitar la búsqueda de software incompatible. La lista de software incompatible se encuentra en el archivo incompatible.txt, que forma parte del kit de distribución. Si no se fija un valor para este parámetro y se detectan aplicaciones incompatibles, la instalación de Kaspersky Endpoint Security se detendrá. |
| SKIPPRODUCTUNINSTALL=1 | Deshabilitar la eliminación automática del software incompatible que se detecte. Si no se fija un valor para este parámetro, Kaspersky Endpoint Security intentará eliminar las aplicaciones incompatibles.<br>No se puede activar la eliminación automática de software incompatible cuando se instala Kaspersky Endpoint Security con el instalador msiexec. Use setup_kes.exe para activar la eliminación automática del software incompatible. |
| KLLOGIN | Permite definir el nombre de usuario con el que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (componente de Protección con contraseña). El nombre de usuario se configura a la par de los parámetros KLPASSWD y KLPASSWDAREA. El nombre de usuario predeterminado es KLAdmin. |
| KLPASSWD | Permite definir la contraseña con la que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros KLLOGIN y KLPASSWDAREA).<br>Si especifica una contraseña, pero no un nombre de usuario con el parámetro KLLOGIN, se utilizará de forma predeterminada el nombre de usuario KLAdmin. |
| KLPASSWDAREA | Permite especificar el alcance de la contraseña de acceso a Kaspersky Endpoint Security. Cuando un usuario intente realizar una acción que esté |

| | |
|---|---|
| | dentro de este alcance, Kaspersky Endpoint Security le solicitará las credenciales (parámetros `KLLOGIN` y `KLPASSWD`). Si necesita especificar más de un valor, use el carácter "`;`". Valores disponibles:<br>• `SET`: modificar la configuración de la aplicación.<br>• `EXIT`: salir de la aplicación.<br>• `DISPROTECT`: deshabilitar los componentes de protección y detener las tareas de análisis.<br>• `DISPOLICY`: deshabilitar la directiva de Kaspersky Security Center.<br>• `UNINST`: eliminar la aplicación del equipo.<br>• `DISCTRL`: deshabilitar los componentes de control.<br>• `REMOVELIC`: eliminar la clave.<br>• `REPORTS`: acceder a los informes. |
| `ENABLETRACES` | Habilitar o deshabilitar el seguimiento del programa. Una vez que Kaspersky Endpoint Security se inicia, los archivos de seguimiento se guardan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Valores disponibles:<br>• `1`: La función de seguimiento de la aplicación está habilitada.<br>• `0`: No realizar un seguimiento (valor predeterminado). |
| `TRACESLEVEL` | Nivel de detalle de los archivos de seguimiento. Valores disponibles:<br>• `100` (crítico). Solo mensajes sobre errores graves.<br>• `200` (alto). Mensajes sobre todos los errores, incluidos los graves.<br>• `300` (diagnóstico). Mensajes sobre todos los errores, además de las advertencias.<br>• `400` (importante). Todos los mensajes de error y de advertencia, así como otra información adicional.<br>• `500` (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado).<br>• `600` (bajo). Todos los mensajes. |
| `AMPPL` | Habilitar o deshabilitar el uso de la tecnología AM-PPL (Antimalware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft.<br>La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019.<br>Valores disponibles: |

| | |
|---|---|
| | • `1`: los procesos de Kaspersky Endpoint Security se protegerán con la tecnología AM-PPL.<br>• `0`: los procesos de Kaspersky Endpoint Security no se protegerán con la tecnología AM-PPL. |
| `RESTAPI` | Administrar la aplicación a través de la API REST. Si desea administrar la aplicación mediante esta API, deberá configurar el parámetro `RESTAPI_User` para especificar el nombre de usuario.<br>Valores disponibles:<br>• `1`: la aplicación podrá administrarse a través de la API REST.<br>• `0`: la aplicación no podrá administrarse a través de la API REST (valor predeterminado).<br>Para administrar la aplicación a través de la API REST, debe permitir el uso de sistemas de administración. Para ello, defina el parámetro `AdminKitConnector=1`. Si opta por utilizar la API REST, no podrá usar los sistemas de administración de Kaspersky para controlar la aplicación. |
| `RESTAPI_User` | Nombre de usuario de la cuenta de dominio de Windows que se usará para administrar la aplicación a través de la API REST. Solo este usuario podrá administrar la aplicación con la API REST. El nombre de usuario debe especificarse en formato `<DOMINIO>\<NombreDeUsuario>` (por ejemplo, `RESTAPI_User=EMPRESA\Administrador`). El uso de la API REST está limitado a un único usuario.<br>Especificar este valor es requisito indispensable para administrar la aplicación a través de la API REST. |
| `RESTAPI_Port` | Puerto que se usará para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782. |
| `ADMINKITCONNECTOR` | Permitir que la aplicación se administre a través de un sistema de administración. Kaspersky Security Center es uno de esos sistemas. Además de los sistemas de administración de Kaspersky, es posible utilizar soluciones de terceros. La API de Kaspersky Endpoint Security se ha diseñado para ello.<br>Valores disponibles:<br>• `1`: la aplicación podrá administrarse a través de un sistema de administración (valor predeterminado).<br>• `0`: la aplicación podrá administrarse únicamente a través de su interfaz local. |

Ejemplo:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Clave
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Cuando concluya la instalación, Kaspersky Endpoint Security se activará con una licencia de prueba (a menos que haya especificado un código de activación en el archivo setup.ini). Usualmente, una licencia de prueba tiene un plazo corto. Cuando la licencia de prueba se vence, se deshabilitan todas las características de Kaspersky Endpoint Security. Para 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 su versión en modo silencioso, se admite el uso de los siguientes archivos:

- setup.ini: parámetros generales para instalar la aplicación.
- install.cfg: parámetros relativos al funcionamiento de Kaspersky Endpoint Security.
- setup.reg: claves del Registro.

  Las claves del archivo setup.reg se escriben en el registro solo si se establece el valor de `setup.reg` para el parámetro `SetupReg` en el archivo setup.ini. El archivo setup.reg es generado por los expertos de Kaspersky. No se recomienda modificar el contenido de este archivo.

Para que se apliquen los parámetros de setup.ini, install.cfg y setup.reg, los archivos deben estar ubicados en la carpeta que contenga 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=<ruta al archivo setup.reg>.`.

## Instalación remota de la aplicación con System Center Configuration Manager

Estas instrucciones corresponden a System Center Configuration Manager 2012 R2.

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

1. Abra la consola del Administrador de configuración.
2. En la parte derecha de la consola, en la sección **Administración de la aplicación**, seleccione **Paquetes**.
3. En la parte superior de la consola en el panel de control, haga clic en el botón **Crear paquete**.

   Se iniciará el *Asistente de nuevo paquete y aplicación*.
4. En el Asistente de nuevo paquete y aplicación:

   a. En la sección **Paquete**:

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

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

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

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

d. En la sección **Requisitos**:

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

  Seleccione la aplicación en la lista desplegable **Aplicación** o especifique la ruta al archivo ejecutable de esta aplicación con el botón **Examinar**.
- Seleccione la opción **Esta aplicación solo puede iniciarse en las plataformas especificadas** en la sección **Requisitos de plataforma** si quiere que la aplicación se instale solo en los sistemas operativos especificados.

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

Este paso es opcional.

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

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

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

   Se inicia el *Asistente de implementación*.

6. En el Asistente de implementación:

   a. En la sección **General**:

   - En el campo **Software**, ingrese el nombre único del paquete de instalación o seleccione el paquete de instalación desde la lista haciendo clic en el botón **Examinar**.
   - En el campo **Conjunto**, ingrese el nombre del conjunto de equipos en los cuales se instalará la aplicación, seleccione el conjunto haciendo clic en el botón **Examinar**.

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

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

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

   Una vez finalizado el Asistente de implementación, se creará una tarea para la instalación remota de Kaspersky Endpoint Security.

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

El archivo setup.ini se utiliza cuando la aplicación se instala a través de la línea de comandos o al usar el Editor de directivas de grupo de Microsoft Windows. Para que los parámetros de este archivo se apliquen, colóquelo en la misma carpeta que el paquete de distribución de Kaspersky Endpoint Security.

DESCARGAR EL ARCHIVO SETUP.INI

El archivo setup.ini consta de las siguientes secciones:

- `[Setup]`: parámetros generales para instalar la aplicación.
- `[Components]`: selección de componentes que se instalarán con la aplicación. Si no se especifica ningún componente, se instalarán todos los componentes que estén disponibles para el sistema operativo. Protección contra archivos peligrosos es un componente obligatorio y se instala en el equipo independientemente de la configuración indicada en esta sección. El componente Managed Detection and Response tampoco está incluido en esta sección. Para instalarlo, deberá 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 ninguna tarea, se incluyen todas las tareas en la lista de tareas de Kaspersky Endpoint Security.

Las alternativas al valor `1` son los valores `sí`, `activado`, `habilitar` y `habilitado`.

Las alternativas al valor `0` son los valores `no`, `apagado`, `deshabilitar` y `deshabilitado`.

Parámetros del archivo setup.ini

| Sección | Parámetro | Descripción |
|---|---|---|
| `[Setup]` | `InstallDir` | Ruta a la carpeta de instalación de la aplicación. |
| | `ActivationCode` | Código de activación de Kaspersky Endpoint Security. |
| | `EULA=1` | Aceptación de los términos del Contrato de licencia de usuario final. El texto del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security.<br>Es necesario aceptar los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar su versión. |
| | `PrivacyPolicy=1` | Aceptación de la Política de privacidad. El texto de la Política de privacidad se incluye en el kit de distribución de Kaspersky Endpoint Security.<br>Para instalar la aplicación o actualizar la versión de la aplicación, deberá aceptar la Directiva de privacidad. |

| | | |
|---|---|---|
| | `KSN` | Participar o negarse a participar en Kaspersky Security Network. Si no especifica ningún valor para este parámetro, se le preguntará si desea participar en KSN cuando inicie Kaspersky Endpoint Security por primera vez. Valores disponibles:<br>• `1`: participar en KSN.<br>• `0`: negarse a participar en KSN (valor predeterminado).<br>El paquete de distribución de Kaspersky Endpoint Security está optimizado para ser utilizado con Kaspersky Security Network. Si opta por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que se haya completado la instalación. |
| | `Login` | Permite definir el nombre de usuario con el que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (componente de Protección con contraseña). El nombre de usuario se configura a la par de los parámetros `Password` y `PasswordArea`. El nombre de usuario predeterminado es KLAdmin. |
| | `Password` | Permite definir la contraseña con la que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros `Login` y `PasswordArea`).<br>Si especificó una contraseña, pero no especificó un nombre de usuario con el parámetro `Login`, se utiliza de forma predeterminada el nombre de usuario KLAdmin. |
| | `PasswordArea` | Permite especificar el alcance de la contraseña de acceso a Kaspersky Endpoint Security. Cuando un usuario intente realizar una acción que esté dentro del alcance de la contraseña, Kaspersky Endpoint Security le solicitará las credenciales (parámetros `Nombre de usuario` y `Contraseña`). Si necesita especificar más de un valor, use el carácter "`;`". Valores disponibles:<br>• `SET`: modificar la configuración de la aplicación.<br>• `EXIT`: salir de la aplicación.<br>• `DISPROTECT`: deshabilitar los componentes de protección y detener las tareas de análisis.<br>• `DISPOLICY`: deshabilitar la directiva de Kaspersky Security Center.<br>• `UNINST`: eliminar la aplicación del equipo.<br>• `DISCTRL`: deshabilitar los componentes de control.<br>• `REMOVELIC`: eliminar la clave. |

| | | |
|---|---|---|
| | | • `REPORTS`: acceder a los informes. |
| | `SelfProtection` | Habilitar o deshabilitar el mecanismo para proteger la instalación de la aplicación. Valores disponibles:<br>• `1`: habilitar el mecanismo para proteger la instalación (valor predeterminado).<br>• `0`: deshabilitar el mecanismo para proteger la instalación.<br>El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Endpoint Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda que desactive la protección del proceso de instalación. |
| | `Reboot=1` | Permitir que el equipo se reinicie automáticamente, de ser necesario, cuando la aplicación termine de instalarse o actualizarse. Si no especifica ningún valor para este parámetro, se bloquea el reinicio automático del equipo.<br>No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación. |
| | `AddEnvironment` | Agregar a la variable del sistema %PATH% la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security. Valores disponibles:<br>• `1`: la variable del sistema %PATH% se complementará con la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security.<br>• `0`: la variable del sistema %PATH% no se complementará con la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security. |
| | `AMPPL` | Habilitar o deshabilitar el uso de la tecnología AM-PPL (Antimalware Protected Process Light) para proteger los procesos de Kaspersky Endpoint Security. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft.<br>La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019.<br>Valores disponibles: |

| | | |
|---|---|---|
| | | • `1`: los procesos de Kaspersky Endpoint Security se protegerán con la tecnología AM-PPL.<br>• `0`: los procesos de Kaspersky Endpoint Security no se protegerán con la tecnología AM-PPL. |
| | `SetupReg` | Grabar las claves del archivo setup.reg en el Registro. Para que esto ocurra, el parámetro `SetupReg` debe tener el valor setup.reg. |
| | `EnableTraces` | Habilitar o deshabilitar el seguimiento del programa. Una vez que Kaspersky Endpoint Security se inicia, los archivos de seguimiento se guardan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Valores disponibles:<br>• `1`: La función de seguimiento de la aplicación está habilitada.<br>• `0`: No realizar un seguimiento (valor predeterminado). |
| | `TracesLevel` | Nivel de detalle de los archivos de seguimiento. Valores disponibles:<br>• `100` (crítico). Solo mensajes sobre errores graves.<br>• `200` (alto). Mensajes sobre todos los errores, incluidos los graves.<br>• `300` (diagnóstico). Mensajes sobre todos los errores, además de las advertencias.<br>• `400` (importante). Todos los mensajes de error y de advertencia, así como otra información adicional.<br>• `500` (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado).<br>• `600` (bajo). Todos los mensajes. |
| | `RESTAPI` | Administrar la aplicación a través de la API REST. Si desea administrar la aplicación mediante esta API, deberá configurar el parámetro `RESTAPI_User` para especificar el nombre de usuario.<br>Valores disponibles:<br>• `1`: la aplicación podrá administrarse a través de la API REST.<br>• `0`: la aplicación no podrá administrarse a través de la API REST (valor predeterminado). |

| | | |
|---|---|---|
| | | Para administrar la aplicación a través de la API REST, debe permitir el uso de sistemas de administración. Para ello, defina el parámetro `AdminKitConnector=1`. Si opta por utilizar la API REST, no podrá usar los sistemas de administración de Kaspersky para controlar la aplicación. |
| | `RESTAPI_User` | Nombre de usuario de la cuenta de dominio de Windows que se usará para administrar la aplicación a través de la API REST. Solo este usuario podrá administrar la aplicación con la API REST. El nombre de usuario debe especificarse en formato `<DOMINIO>\<NombreDeUsuario>` (por ejemplo, `RESTAPI_User=EMPRESA\Administrador`). El uso de la API REST está limitado a un único usuario.<br>Especificar este valor es requisito indispensable para administrar la aplicación a través de la API REST. |
| | `RESTAPI_Port` | Puerto que se usará para administrar la aplicación a través de la API REST. El puerto predeterminado es el 6782. |
| `[Components]` | `ALL` | Instalar todos los componentes. Si el valor del parámetro es `1`, se instalarán todos los componentes, sin que se tenga en cuenta la configuración de instalación de cada componente individual. |
| | `MailThreatProtection` | Protección contra amenazas de correo. |
| | `WebThreatProtection` | Protección contra amenazas web. |
| | `AMSI` | Protección vía AMSI. |
| | `HostIntrusionPrevention` | Prevención contra intrusos |
| | `BehaviorDetection` | Detección de comportamientos. |
| | `ExploitPrevention` | Prevención de exploits. |
| | `RemediationEngine` | Motor de reparación. |
| | `Firewall` | Firewall. |
| | `NetworkThreatProtection` | Protección contra amenazas de red |
| | `WebControl` | Control web. |
| | `DeviceControl` | Control de dispositivos. |
| | `ApplicationControl` | Control de aplicaciones. |
| | `AdaptiveAnomaliesControl` | Control de anomalías adaptativo. |
| | `FileEncryption` | Bibliotecas de cifrado de archivos. |
| | `DiskEncryption` | Bibliotecas de cifrado de disco completo. |
| | `BadUSBAttackPrevention` | Prevención de ataques BadUSB |
| | `AntiAPT` | Endpoint Agent. Si selecciona el componente *Endpoint Agent*, se instalará Kaspersky Endpoint Agent 3.10 para permitir que la aplicación interactúe con ciertas soluciones de Kaspersky diseñadas para detectar amenazas avanzadas (por ejemplo, Kaspersky Sandbox). |
| | `AdminKitConnector` | Permitir que la aplicación se administre a través de un |

| | | |
|---|---|---|
| | | sistema de administración. Kaspersky Security Center es uno de esos sistemas. Además de los sistemas de administración de Kaspersky, es posible utilizar soluciones de terceros. La API de Kaspersky Endpoint Security se ha diseñado para ello.<br>Valores disponibles:<br>• `1`: la aplicación podrá administrarse a través de un sistema de administración (valor predeterminado).<br>• `0`: la aplicación podrá administrarse únicamente a través de su interfaz local. |
| `[Tasks]` | `ScanMyComputer` | Tarea de Análisis completo. Valores disponibles:<br>• `1`: incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.<br>• `0`: no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. |
| | `ScanCritical` | Tarea de Análisis de áreas críticas. Valores disponibles:<br>• `1`: incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.<br>• `0`: no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. |
| | `Updater` | Tarea de actualización. Valores disponibles:<br>• `1`: incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.<br>• `0`: no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. |

## Cambiar componentes de la aplicación

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

- De manera local, utilizando el Asistente de instalación.

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

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

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

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

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

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

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

**Cómo agregar o eliminar componentes de 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**.

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.6.0) → Cambiar componentes de la aplicación**.

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

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

Active la casilla **Eliminar aplicaciones incompatibles de terceros**. Puede consultar la lista de aplicaciones incompatibles en el archivo `incompatible.txt`, que forma parte del kit de distribución. Si se instalan aplicaciones incompatibles en el equipo, la instalación de Kaspersky Endpoint Security finaliza con un error.

De ser necesario, habilite la protección con contraseña para realizar la tarea:

1. Haga clic en el botón **Adicional**.
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 KLAdmin.

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

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

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

### Paso 4. Programación de la tarea

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

### Paso 5. Nombre de la tarea

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

### Paso 6. Completar creación de la tarea

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

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

[Cómo agregar o eliminar componentes de la aplicación mediante 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 **Agregar**.

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

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

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Cambiar componentes de la aplicación**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, `Agregar el componente Control de aplicaciones`).
4. En la sección **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

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

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

### Paso 3. Completar creación de la tarea

Active la casilla **Abrir la ventana de propiedades de la tarea tras crear la tarea** y cierre el asistente. En las propiedades de la tarea, abra la ficha **Configuración de la aplicación** y seleccione los componentes que estarán disponibles.

De ser necesario, habilite la protección con contraseña para realizar la tarea:

1. En la sección **Configuración avanzada**, active la casilla **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 e inicie la tarea.

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

## Actualización de una versión más antigua de la aplicación

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

- Kaspersky Endpoint Security 11.6.0 es compatible con Kaspersky Security Center 12.
- Se recomienda cerrar todas las aplicaciones activas antes de realizar la actualización.
- Si el equipo en el que va a realizar la actualización tiene sus discos duros cifrados con la tecnología de cifrado de disco completo (FDE), deberá descifrarlos para poder actualizar Kaspersky Endpoint Security de la versión 10 a las versiones 11.0.0 y posteriores.

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

Puede actualizar las siguientes versiones de Kaspersky Endpoint Security:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 para Windows (compilación 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 para Windows (versión 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 para Windows (compilación 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 para Windows (compilación 10.3.0.6294).
- 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 (versión 11.0.0.6499)
- Kaspersky Endpoint Security 11.0.1 para Windows (versión 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 (versión 11.1.0.15919)
- Kaspersky Endpoint Security 11.1.1 para Windows (versión 11.1.1.126)
- Kaspersky Endpoint Security 11.2.0 para Windows (versión 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 (versión 11.3.0.773)
- Kaspersky Endpoint Security 11.4.0 para Windows (versión 11.4.0.233)
- Kaspersky Endpoint Security 11.5.0 para Windows (versión 11.5.0.590)

Cuando Kaspersky Endpoint Security 10 Service Pack 2 para Windows se actualiza a Kaspersky Endpoint Security 11.6.0 para Windows, los archivos colocados en Copia de seguridad o en Cuarentena de la versión anterior de la aplicación se transfieren a Copia de seguridad de la versión nueva. Por el contrario, cuando la versión que se actualiza es anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, los archivos colocados en la Cuarentena o en el depósito Copias de seguridad de la versión antigua no se transfieren a la versión más reciente.

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

- de manera local, utilizando el Asistente de instalación;
- de manera local, utilizando la línea de comandos;
- de manera remota, a través de Kaspersky Security Center 12;
- de manera remota, utilizando el Editor de administración de directivas de grupo de Microsoft Windows (para más información, consulte el *sitio web de soporte técnico de Microsoft*);
- de manera remota, utilizando System Center Configuration Manager.

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

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

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

- la Consola de administración de Kaspersky Security Center,

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

## Eliminar la aplicación

La eliminación de Kaspersky Endpoint Security deja el equipo y los datos del usuario sin protección contra amenazas.

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

- de manera local, utilizando el Asistente de instalación;
- de manera local, utilizando la línea de comandos;
- de manera remota, utilizando Kaspersky Security Center (para más información, consulte la *Ayuda de Kaspersky Security Center*);
- de manera remota, utilizando el Editor de administración de directivas de grupo de Microsoft Windows (para más información, consulte 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. Cuando desinstale Kaspersky Endpoint Security, también se desinstalará Kaspersky Endpoint Agent.

## Desinstalación mediante Kaspersky Security Center

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

**Cómo desinstalar la aplicación mediante la Consola de administración (MMC)**

1. 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**.

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

### Paso 1. Selección del tipo de tarea

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

### Paso 2. Selección del programa que se desinstalará

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

### Paso 3. Configuración de la tarea para desinstalar la aplicación

Seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.

### Paso 4. Configuración de la utilidad de desinstalación

Configure los siguientes parámetros adicionales:

- **Forzar la descarga de la utilidad de desinstalación**. Indique cómo se distribuirá la utilidad:
  - **Utilización del Agente de red**. Si el Agente de red no se ha instalado en la equipo, el primer Agente de red se instalará utilizando las herramientas del sistema operativo. Kaspersky Endpoint Security se desinstalará entonces con las herramientas del Agente de red.
  - **Con los recursos de Microsoft Windows por medio del Servidor de administración**. La utilidad se enviará a los equipos cliente a través del Servidor de administración, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.
  - **Uso de recursos del sistema operativo a través de puntos de distribución**. La utilidad se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si hay al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, *consulte la Ayuda de Kaspersky Security Center*.
- **Comprobar la versión del sistema operativo antes de la descarga**. De ser necesario, desactive esta casilla. Esto evitará que la utilidad de desinstalación se descargue si el sistema operativo del equipo no cumple con los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple con los requisitos del software, puede omitir esta verificación.

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

1. Active la casilla **Utilizar contraseña de desinstalación**.
2. Haga clic en el botón **Modificar**.

3. Escriba la contraseña de la cuenta KLAdmin.

### Paso 5. Seleccionar la opción de reinicio del sistema operativo

Cuando concluya la desinstalación, el equipo deberá reiniciarse. Elija la acción que se llevará a cabo para reiniciar el equipo.

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

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

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

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

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

### Paso 8. Programación de la tarea

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

### Paso 9. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo `Eliminar Kaspersky Endpoint Security 11.6.0`.

### Paso 10. Fin de la creación de la tarea

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

La aplicación se desinstalará en modo silencioso.

[Cómo desinstalar la aplicación mediante Web Console y Cloud Console]

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

   Se abre la lista de tareas.

2. Haga clic en el botón **Agregar**.

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

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

Configure los parámetros generales de la tarea:

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

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

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

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

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

1. Seleccione **Desinstalar aplicación administrada**.
2. Seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.
3. **Forzar la descarga de la utilidad de desinstalación**. Indique cómo se distribuirá la utilidad:

   - **Utilización del Agente de red**. Si el Agente de red no se ha instalado en la equipo, el primer Agente de red se instalará utilizando las herramientas del sistema operativo. Kaspersky Endpoint Security se desinstalará entonces con las herramientas del Agente de red.
   - **Con los recursos de Microsoft Windows por medio del Servidor de administración**. La utilidad se enviará a los equipos cliente a través del Servidor de administración, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si el Agente de red no está instalado en el equipo cliente, pero el equipo cliente está en la misma red que el Servidor de administración.
   - **Uso de recursos del sistema operativo a través de puntos de distribución**. La utilidad se enviará a los equipos cliente a través de los puntos de distribución, utilizando los recursos del sistema operativo. Puede seleccionar esta opción si hay al menos un punto de distribución en la red. Para obtener más información sobre puntos de distribución, *consulte la Ayuda de Kaspersky Security Center*.

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

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

5. En el campo **Número 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, desmarque la casilla de verificación **Comprobar la versión del sistema operativo antes de la instalación**. Esto evitará que la utilidad de desinstalación se descargue si el sistema operativo del equipo no cumple con los requisitos de software. Si está seguro de que el sistema operativo del equipo cumple con los requisitos del software, puede omitir esta verificación.

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

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

### Paso 5. Completar creación de la tarea

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

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

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

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

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

   Se abre la lista de tareas.

2. Haga clic en la tarea **Desinstalar aplicación de forma remota** de Kaspersky Security Center.

   Se abre la ventana de propiedades de la tarea.

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

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

5. Escriba la contraseña de la cuenta KLAdmin.

6. Haga clic en el botón **Guardar**.

## Uso del Asistente para desinstalar la aplicación

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

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

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

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

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

## Eliminación de la aplicación desde la línea de comandos

Kaspersky Endpoint Security puede desinstalarse a través de la línea de comandos de los siguientes modos:

- En modo interactivo usando el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que comience la desinstalación en modo silencioso, podrá desentenderse del proceso de eliminación. Para desinstalar la aplicación en modo silencioso, use los modificadores `/s` y `/qn`.

*Para desinstalar la aplicación en modo silencioso:*

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:
   - Si el proceso de eliminación no está protegido con contraseña:

     ```
     setup_kes.exe /s /x
     ```

o

```
msiexec.exe /x <GUID> /qn
```

<GUID> es el identificador único de la aplicación. Para determinar cuál es este identificador, utilice el siguiente comando:

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

- Si el proceso de eliminación está protegido con contraseña:

  ```
  setup_kes.exe /pKLLOGIN=<nombre de usuario> /pKLPASSWD=<contraseña> /s /x
  ```

  o

  ```
  msiexec.exe /x <GUID> KLLOGIN=<nombre de usuario> KLPASSWD=<contraseña> /qn
  ```

Ejemplo:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Contraseña1 /qn
```

# Licencias de la aplicación

En esta sección, se proporciona información sobre conceptos generales relacionados con las licencias de la aplicación.

## Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* es un acuerdo vinculante entre usted y AO Kaspersky Lab en el que se establecen las condiciones bajo las cuales podrá utilizar la aplicación.

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

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

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

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

## Acerca de la licencia

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

Una licencia válida le otorga el derecho a recibir los siguientes tipos de servicios:

- Uso de la aplicación de acuerdo con los términos del Contrato de licencia de usuario final
- Servicio de soporte técnico

El alcance del período de uso de los servicios y las aplicaciones depende del tipo de licencia que se usó para activar la aplicación.

Se proporcionan los siguientes tipos de licencia:

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

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

  La aplicación no puede activarse con una licencia de prueba más de una vez.

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

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

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

## Sobre el certificado de licencia

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

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

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

## Acerca de la suscripción

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

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

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

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

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

## Acerca de la clave de licencia

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

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

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

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

Existen dos tipos de claves: activa y de reserva.

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

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

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

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

## Acerca del código de activación

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

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

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

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

## Acerca del archivo de clave

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

Kaspersky le enviará un archivo de clave a la dirección de correo electrónico que indique al comprar Kaspersky Endpoint Security o al solicitar la versión de prueba de Kaspersky Endpoint Security.

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

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

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

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

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

## Activación de la aplicación

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

Puede activar la aplicación de las siguientes maneras:

- En forma local, utilizando el Asistente de activación en la interfaz de la aplicación. A través del asistente, podrá agregar tanto una clave activa como una de reserva.
- En forma remota, creando y ejecutando una tarea para agregar una clave de licencia en Kaspersky Security Center. Si utiliza este método, podrá agregar tanto una clave activa como una de reserva.
- Distribuyendo a los equipos cliente archivos de clave y códigos de activación que estén almacenados en el repositorio de claves del Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la distribución de claves, consulte la *Guía de ayuda de Kaspersky Security Center*. Si utiliza este método, podrá agregar tanto una clave activa como una de reserva.

  Se distribuye primero el código de activación adquirido bajo suscripción.

- Con la línea de comandos.

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

## Cómo activar la aplicación a través de Kaspersky Security Center

Puede activar la aplicación en forma remota, a través de Kaspersky Security Center, de las siguientes maneras:

- Usando la tarea *Agregar clave*.

  Este método puede usarse para agregar una clave tanto en un equipo específico como en una serie de equipos pertenecientes a un grupo de administración.

- Distribuyendo a los equipos una clave almacenada en el Servidor de administración de Kaspersky Security Center.

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

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

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

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 (**Supervisión e informes** → **Informes**).

- Ver el estado de los equipos en la ficha **Dispositivos** → **Dispositivos administrados**. Los equipos en los que la aplicación no se haya activado tendrán el estado ⚠ y la descripción de 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 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**.

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.6.0)** → **Agregar clave**.

### Paso 2. Selección de la clave que se agregará

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

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

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

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

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

### Paso 4. Programación de la tarea

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

### Paso 5. Nombre de la tarea

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

### Paso 6. Completar creación de la tarea

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

[Cómo activar la aplicación mediante Web Console y Cloud Console]

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

   Se abre la lista de tareas.

2. Haga clic en el botón **Agregar**.

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

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

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Agregar clave**.
3. En el campo **Nombre de la tarea**, ingrese una breve descripción, por ejemplo, `Activación de Kaspersky Endpoint Security para Windows`.
4. En la sección **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea. Haga clic en **Siguiente**.

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

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

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

### Paso 3. Selección de la licencia

Seleccione la licencia que se usará para activar la aplicación. Haga clic en **Siguiente**.

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

### Paso 4. Completar creación de la tarea

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

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

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

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

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

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

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

## Uso del Asistente de activación para activar la aplicación

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

1. Haga clic en el botón **Licencia** que se encuentra en la parte inferior de la ventana principal de la aplicación.
2. En la ventana que se abre, haga clic en el botón **Activar la aplicación con una nueva licencia**.

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

## Activación de la aplicación desde la línea de comandos

*Para activar la aplicación desde la línea de comandos,*

ingrese la siguiente cadena en la línea de comandos:

```
avp.com license /add <código de activación o archivo de clave> [/login=<nombre de usuario> /password=<contraseña>]
```

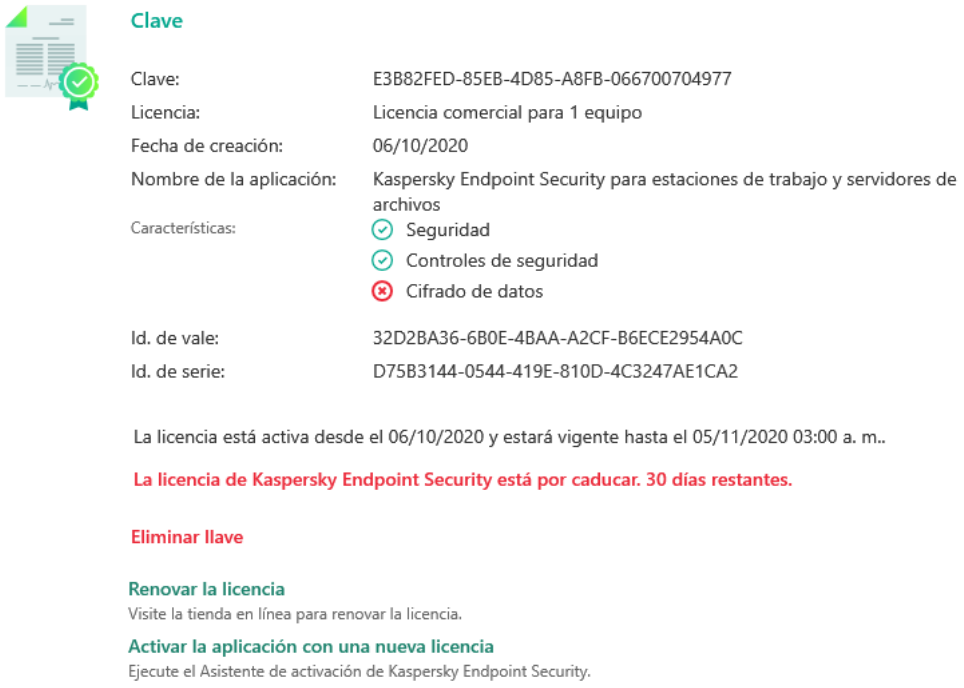
Las credenciales de la cuenta de usuario (`/login=<nombre de usuario> /password=<contraseña>`) se necesitan cuando la protección con contraseña está habilitada.

## Visualización de la información de la licencia

*Para ver información sobre la licencia:*

Haga clic en el botón **Licencia** que se encuentra en la parte inferior de la ventana principal de la aplicación.

Se abre la ventana **Licencia**. Allí encontrará la información de la licencia (vea la siguiente imagen).




Ventana Licencia

La siguiente información se proporciona en la ventana **Licencia**:

- **Estado de la clave**. Puede almacenar más de una clave en el equipo. Existen dos tipos de claves: activa y de reserva. La aplicación no puede tener más de una clave activa. Para que se active una clave de reserva, es

necesario eliminar la clave activa (con el botón ) o esperar a que caduque.

- **Clave**. Una *clave* es una secuencia alfanumérica irrepetible que se genera a partir de un código de activación o de un archivo de clave.
- **Licencias**. Los siguientes tipos de licencias están disponibles: de prueba y comercial.
- **Nombre de la aplicación**. Nombre completo de la aplicación de Kaspersky que se ha adquirido.
- **Características**. Funciones de la aplicación que la licencia permite utilizar. Entre las funciones se encuentran Protección, Controles de seguridad y Cifrado de datos. La lista de funciones también está disponible en el certificado de licencia.
- **Información adicional sobre la licencia**. Tipo de licencia, número de equipos que cubre esta licencia, fecha de inicio de la licencia y fecha y hora de caducidad (solo para la clave activa).

  El tiempo de caducidad de la licencia se muestra según la zona horaria configurada en el sistema operativo.

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

- **Comprar licencia** / **Renovar 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 agregar una clave con un código de activación o un archivo de clave. A través del Asistente de activación de la aplicación, podrá agregar una clave activa y una única clave de reserva.

## Adquisición de una licencia

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

*Para adquirir una licencia:*

1. En la ventana principal de la aplicación, haga clic en el botón **Licencia**.
2. En la ventana **Licencia**, realice una de las siguientes acciones:
   - Si no se agregó ninguna clave o si se agregó una clave para una licencia de prueba, haga clic en el botón **Comprar licencia**.
   - Si se agregó una clave para una licencia comercial, haga clic en el botón **Renovar licencia**.

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

## Renovación de una suscripción

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

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

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

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

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

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

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

2. En la ventana **Licencia**, haga clic en **Contacte al proveedor de suscripción**.

## Suministro de datos estipulado en el Contrato de licencia de usuario final

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

- tipo, versión y localización de Kaspersky Endpoint Security;
- versión de las actualizaciones instaladas en Kaspersky Endpoint Security;
- id. del equipo e id. asignado a la copia de Kaspersky Endpoint Security instalada en el equipo;
- número de serie e identificador de la clave activa;
- tipo, versión y número de bits del sistema operativo, junto con el nombre del entorno virtual (si Kaspersky Endpoint Security está instalado en un entorno virtual);
- Id. de los componentes de Kaspersky Endpoint Security que están activos cuando se transmite la información.

Kaspersky también puede usar esta información para generar estadísticas sobre la diseminación y el uso del software Kaspersky.

Al utilizar un código de activación, acepta transmitir automáticamente los datos enumerados anteriormente. Si no está de acuerdo en compartir esta información con Kaspersky, debe utilizar un archivo de clave para activar Kaspersky Endpoint Security.

Al aceptar los términos del Contrato de licencia de usuario final, acepta transmitir automáticamente la siguiente información:

- Al actualizar Kaspersky Endpoint Security:
  - versión de Kaspersky Endpoint Security,
  - id. de Kaspersky Endpoint Security,
  - clave activa,
  - id. único de la ejecución de la tarea de actualización,
  - id. único de la instalación de Kaspersky Endpoint Security.
- Al utilizar vínculos desde la interfaz de Kaspersky Endpoint Security:
  - versión de Kaspersky Endpoint Security,
  - versión del sistema operativo,
  - fecha de activación de Kaspersky Endpoint Security,
  - fecha de caducidad de la licencia,

- fecha de creación de la clave,
- fecha de instalación de Kaspersky Endpoint Security,
- id. de Kaspersky Endpoint Security,
- id. de la vulnerabilidad detectada en el sistema operativo,
- id. de la última actualización instalada en Kaspersky Endpoint Security,
- hash del archivo en el que se haya detectado una amenaza, además del nombre con el que Kaspersky clasifica dicha amenaza,
- categoría del error de activación de Kaspersky Endpoint Security,
- código del error de activación de Kaspersky Endpoint Security,
- días por delante hasta que caduque la clave,
- días transcurridos desde que se agregó la clave,
- días transcurridos desde que caducó la licencia,
- cantidad de equipos en los que se ha aplicado la licencia activa,
- clave activa,
- plazo de licencia de Kaspersky Endpoint Security,
- estado de la licencia,
- tipo de licencia activa,
- tipo de aplicación,
- id. único de la ejecución de la tarea de actualización,
- id. único asignado a la instalación de Kaspersky Endpoint Security en el equipo,
- idioma de la interfaz de Kaspersky Endpoint Security.

La información recibida es protegida por Kaspersky de acuerdo con la ley y con los requisitos y las reglamentaciones aplicables de Kaspersky. La información se transmite a través de canales de comunicación cifrados.

Puede leer el Contrato de licencia de usuario final y visitar el sitio web de Kaspersky para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn_<identificador del idioma>.txt contienen el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network y están incluidos en el kit de distribución.

## Provisión de datos al utilizar Kaspersky Security Network

El conjunto de datos que Kaspersky Endpoint Security envía a Kaspersky depende del tipo de licencia y de la configuración de uso de Kaspersky Security Network.

## Uso de KSN bajo licencia en no más de 4 equipos

Al aceptar la Declaración de Kaspersky Security Network , acepta transmitir automáticamente la siguiente información:

- información sobre las actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida, código de error de la actualización de la configuración;
- información sobre los archivos y las direcciones URL que deben analizarse: las sumas de comprobación del archivo analizado (MD5, SHA2-256, SHA1) y el patrón del archivo (MD5), el tamaño del patrón, el tipo de amenaza detectada y su nombre de acuerdo con la clasificación del Titular de los derechos; el identificador de las bases de datos antivirus, la dirección URL en la que se solicita la reputación, así como la dirección URL de referencia, el identificador del protocolo de conexión y el número del puerto utilizado;
- Id. de la tarea de análisis que detectó la amenaza;
- información sobre los certificados digitales que se usaron y que se necesitaba para verificar su autenticidad: las sumas de comprobación (SHA256) del certificado que se usó para firmar el objeto analizado y la clave pública del certificado;
- identificador del componente de software que realiza el análisis;
- ID de las bases de datos antivirus y de los registros de estas bases de datos antivirus;
- Información sobre la activación del software en el equipo: encabezado firmado del ticket del servicio de activación (identificador del centro de activación regional, suma de comprobación del código de activación, suma de comprobación del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket), estado de la licencia, fecha y hora de inicio/finalización de la validez del ticket, identificador único de la licencia, versión de la licencia, identificador del certificado utilizado para firmar el encabezado del ticket, suma de comprobación (MD5) del archivo de clave;
- Información sobre el software del titular de los derechos: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

## Uso de KSN bajo licencia en 5 o más equipos

Al aceptar la Declaración de Kaspersky Security Network , acepta transmitir automáticamente la siguiente información:

Cuando la casilla **Kaspersky Security Network** está activada y la casilla **Modo KSN extendido** está desactivada, la aplicación transmite la siguiente información:

- información sobre las actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida, código de error de la actualización de la configuración;
- información sobre los archivos y las direcciones URL que deben analizarse: las sumas de comprobación del archivo analizado (MD5, SHA2-256, SHA1) y el patrón del archivo (MD5), el tamaño del patrón, el tipo de amenaza detectada y su nombre de acuerdo con la clasificación del Titular de los derechos; el identificador de las bases de datos antivirus, la dirección URL en la que se solicita la reputación, así como la dirección URL de referencia, el identificador del protocolo de conexión y el número del puerto utilizado;
- Id. de la tarea de análisis que detectó la amenaza;
- información sobre los certificados digitales que se usaron y que se necesitaba para verificar su autenticidad: las sumas de comprobación (SHA256) del certificado que se usó para firmar el objeto analizado y la clave pública del certificado;

- identificador del componente de software que realiza el análisis;
- ID de las bases de datos antivirus y de los registros de estas bases de datos antivirus;
- Información sobre la activación del software en el equipo: encabezado firmado del ticket del servicio de activación (identificador del centro de activación regional, suma de comprobación del código de activación, suma de comprobación del ticket, fecha de creación del ticket, identificador único del ticket, versión del ticket), estado de la licencia, fecha y hora de inicio/finalización de la validez del ticket, identificador único de la licencia, versión de la licencia, identificador del certificado utilizado para firmar el encabezado del ticket, suma de comprobación (MD5) del archivo de clave;
- Información sobre el software del titular de los derechos: versión completa, tipo, versión del protocolo utilizado para conectarse a los servicios de Kaspersky.

Cuando tanto la casilla **Modo KSN extendido** como la casilla **Kaspersky Security Network** están activadas, la aplicación transmite la información que se indica más arriba y, además, lo siguiente:

- información sobre los resultados de la categorización de los recursos web solicitados, lo que contiene la URL procesada y la dirección IP del host, la versión del componente del Software que realizó la categorización, el método de categorización y el conjunto de categorías que definió el recurso web;
- información sobre el software instalado en el equipo: nombres de las aplicaciones de software y de los proveedores de software, claves de registro y sus valores, información sobre los archivos de los componentes de software instalados (sumas de comprobación [MD5, SHA2-256, SHA1], nombre, ruta al archivo en el equipo, tamaño, versión y firma digital);
- información sobre el estado de la protección antivirus del equipo: las versiones y las marcas de tiempo de lanzamiento de las bases de datos antivirus que se utilizan, el id. de la tarea y el id. del software que realiza el análisis;
- información sobre los archivos descargados por el usuario final: la URL y las direcciones IP de descarga y de las páginas de descarga, el identificador del protocolo de descarga y el número de puerto de conexión, el estado de las URL como malintencionado o no, los atributos, el tamaño y las sumas de comprobación del archivo (MD5, SHA2-256, SHA1), información sobre el proceso que descargó el archivo (sumas de comprobación (MD5, SHA2-256, SHA1), fecha y hora de creación/compilación, estado de reproducción automática, atributos, nombres de los empacadores, información sobre firmas, marca de archivo ejecutable, el identificador de formato y la entropía), el nombre del archivo y su ruta en el equipo, la firma digital y la marca de tiempo de su generación, la dirección URL donde ocurrió la detección, el número del script en la página que parece ser sospechosa o dañina, información sobre solicitudes HTTP generadas y la respuesta a ellas;
- información sobre las aplicaciones en ejecución y sus módulos: datos sobre los procesos que se están ejecutando en el sistema (identificador del proceso [PID], nombre del proceso, información sobre la cuenta con la que se inició el proceso, aplicación y comando con que se inició el proceso, el signo de programa o proceso de confianza, ruta de acceso completa a los archivos del proceso y sus sumas de comprobación [MD5, SHA2-256, SHA1], línea de comandos de inicio, nivel de integridad del proceso y descripción del producto al cual pertenece el proceso [nombre del producto e información sobre el editor], así como los certificados digitales utilizados y la información necesaria para verificar su autenticidad o información sobre la ausencia de la firma digital de un archivo), información sobre los módulos cargados en los procesos (sus nombres, tamaños, tipos, fechas de creación, atributos y sumas de comprobación [MD5, SHA2-256, SHA1], además de las rutas de acceso a estos en el equipo), información del encabezado de archivo PE y nombres de los empaquetadores (para archivos empaquetados);
- información sobre todos los objetos y actividades potencialmente malintencionados: nombre del objeto detectado y ruta completa al objeto en el equipo; sumas de comprobación de los archivos procesados (MD5, SHA2-256, SHA1); fecha y hora de detección; nombre, tamaño y ruta de los archivos infectados; código de la plantilla de la ruta; marca de archivo ejecutable; indicador que señala si el objeto es un contenedor; nombres del empaquetador (para archivos empaquetados); código del tipo de archivo; id. del formato de archivo; lista de acciones realizadas por el malware y decisión tomada por el software y por el usuario en respuesta a ellas: id. de

las bases de datos antivirus y de los registros de las bases de datos antivirus que se hayan usado para tomar la decisión; indicador de un objeto potencialmente malintencionado; nombre de la amenaza detectada según la clasificación del Titular de los derechos; nivel de peligro; estado de detección y método de detección; motivo de inclusión en el contexto analizado y número de secuencia del archivo en el contexto; sumas de comprobación (MD5, SHA2-256, SHA1); nombre y atributos del archivo ejecutable de la aplicación a través de la cual se transmitieron el mensaje o el vínculo infectados; direcciones IP despersonalizadas (IPv4 e IPv6) del host del objeto bloqueado; entropía del archivo; indicador de ejecución automática del archivo; hora a la que se detectó por primera vez el archivo en el sistema; número de ocasiones en las que se ejecutó el archivo desde el envío de las últimas estadísticas; información sobre el nombre; sumas de comprobación (MD5, SHA256, SHA1) y tamaño del cliente de correo a través del cual se recibió el objeto malintencionado; id. de la tarea del software que realizó el análisis; indicador que señala si la firma o la reputación del archivo se comprobaron; resultado del procesamiento del archivo; suma de comprobación (MD5) del patrón obtenido para el objeto; tamaño del patrón en bytes; y las especificaciones técnicas de las tecnologías de detección aplicadas;

- información sobre los objetos analizados: el grupo de confianza asignado en el que se ubicó el archivo o desde el que se ubicó; el motivo por el que el archivo se ubicó en esa categoría; el identificador de la categoría; la información sobre el origen de las categorías y la versión de la base de datos de la categoría; la marca de certificado de confianza del archivo; el nombre del proveedor del archivo; la versión del archivo; el nombre y la versión de la aplicación de software que contiene el archivo;

- información sobre las vulnerabilidades detectadas: el identificador de la vulnerabilidad en la base de datos de vulnerabilidades, la clase de riesgo de la vulnerabilidad;

- información acerca de la emulación del archivo ejecutable: el tamaño del archivo y sus sumas de comprobación (MD5, SHA2-256, SHA1); la versión del componente de la emulación, la profundidad de la emulación, el conjunto de propiedades de los bloques lógicos y las funciones situadas dentro de estos bloques que se obtuvieron durante la emulación; los datos provenientes de los encabezados de PE del archivo ejecutable;

- las direcciones IP del equipo atacante (IPv4 e IPv6), el número del puerto del equipo al que se dirige el ataque de red, el identificador del protocolo del paquete IP que contiene el ataque, el objetivo del ataque (nombre de la organización, sitio web), la marca de la reacción ante el ataque, la ponderación del ataque y el nivel de confianza;

- información sobre ataques asociados a recursos de red falsificados, y las direcciones IP (IPv4 e IPv6) y DNS de los sitios web visitados;

- direcciones IP (IPv4 o IPv6) y DNS del recurso web solicitado; la información sobre el archivo y el cliente web que accede al recurso web; información sobre el archivo y el cliente web que accede al recurso web; el nombre, el tamaño y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo, ruta completa al archivo y código de plantilla de la ruta, el resultado de la comprobación de la firma digital y su estado de conformidad con KSN;

- información sobre reversión de acciones de malware: los datos del archivo cuya actividad se ha revertido (el nombre del archivo, ruta entera al archivo, su tamaño y sumas de comprobación (MD5, SHA2-256, SHA1)), datos de acciones correctas y fallidas a eliminar, renombra y copia archivos y restaura los valores en el registro (los nombres de las claves de registro y sus valores), e información sobre los archivos del sistema modificados por el malware, antes y después de la reversión.

- información sobre las exclusiones establecidas para el componente Control de anomalías adaptativo: el identificador y el estado de la regla que se ejecutó, la acción llevada a cabo por el Software cuando se ejecutó la regla, el tipo de cuenta de usuario con la cual el proceso o el hilo lleva a cabo una actividad sospechosa, así como sobre el proceso sujeto a la actividad sospechosa (identificador de la secuencia o nombre del archivo del proceso, ruta de acceso completa al archivo del proceso, código del patrón de la ruta, sumas de comprobación [MD5, SHA2-256, SHA1] del archivo del proceso); información sobre el objeto que llevó a cabo las actividades sospechosas, así como sobre el objeto que quedó sujeto a acciones sospechosas (nombre de la clave del registro o nombre del archivo, ruta completa al archivo, código del patrón de la ruta, y sumas de comprobación [MD5, SHA2-256, SHA1] del archivo).

- Información sobre los módulos de software cargados: nombre, tamaño y sumas de comprobación (MD5, SHA2-256, SHA1) del archivo del módulo, la ruta completa hacia el archivo y código de la plantilla de la ruta, configuración de la firma digital del archivo del módulo, fecha y hora de la creación de la firma, nombre del

asunto y organización que firmó el archivo del módulo, ID del proceso en el cual se cargó el módulo, nombre del proveedor del módulo y número de secuencia del módulo en la cola que carga.

- información sobre la calidad de la interacción del Software con los servicios KSN: fecha y hora de comienzo y finalización del periodo en el que se generaron las estadísticas, información sobre la calidad de las solicitudes y conexión con cada uno de los servicios KSN utilizados (identificador del servicio KSN, cantidad de solicitudes exitosas, cantidad de solicitudes con respuestas del caché, cantidad de solicitudes no exitosas (problemas de red, KSN desactivado en la configuración del Software, ruta incorrecta), intervalo de tiempo de las solicitudes exitosas, intervalo de tiempo de las solicitudes canceladas, intervalo de tiempo de las solicitudes con límite de tiempo excedido, cantidad de conexiones a KSN tomadas del caché, cantidad de conexiones exitosas a KSN, cantidad de conexiones no exitosas a KSN, cantidad de transacciones exitosas, cantidad de transacciones no exitosas, intervalo de tiempo de las conexiones exitosas a KSN, intervalo de tiempo de las conexiones no exitosas a KSN, intervalo de tiempo de las transacciones exitosas, intervalo de tiempo de las transacciones no exitosas);

- si se detecta un objeto posiblemente malicioso, se debe proporcionar información sobre los datos en la memoria de los procesos: los elementos de la jerarquía de los objetos del sistema (ObjectManager), los datos de la memoria UEFI BIOS, los nombres de las claves del registro y sus valores;

- información sobre los eventos en los registros de los sistemas: la marca de tiempo del evento, el nombre del registro en el que se encontró el evento, el tipo y la categoría del evento, el nombre de la fuente del evento y su descripción;

- información sobre las conexiones de red: la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo desde el que se inició el proceso de apertura del puerto, la ruta de acceso al archivo del proceso y su firma digital, las direcciones IP locales y remotas, la cantidad de puertos de conexión local y remota, el estado de conexión, y la marca de tiempo de apertura del puerto;

- información sobre la fecha de instalación y activación del software en el equipo: el id. del socio que vendió la licencia, el número de serie de la licencia, el encabezado firmado del ticket del servicio de activación (el id. de un centro de activación regional, la suma de comprobación del código de activación, la suma de comprobación del ticket, la fecha de creación del ticket, el id. único del ticket, la versión del ticket, el estado de la licencia, la fecha y hora de inicio/finalización del ticket, el id. único de la licencia, la versión de la licencia), el id. del certificado utilizado para firmar el encabezado del ticket, la suma de comprobación (MD5) del archivo de clave, el id. único de la instalación del software en el equipo, el tipo y el id. de la aplicación que se actualiza, el id. de la tarea de actualización;

- información sobre el conjunto de todas las actualizaciones instaladas y el conjunto de las últimas actualizaciones instaladas o eliminadas, el tipo de evento que ocasionó que se enviara la información de actualización, el tiempo transcurrido desde la instalación de la última actualización, y la información sobre las bases de datos antivirus instaladas;

- información sobre el funcionamiento del software en el equipo: datos de uso de la CPU, datos de uso de memoria (Bytes Privados, grupo no paginado, grupo paginado), número de amenazas activas en el proceso de software y amenazas pendientes y el tiempo de funcionamiento del software antes del error.

- cantidad de volcados de software y volcados del sistema (BSOD) desde que se instaló el Software y a partir del momento de la última actualización, además del identificador y la versión del módulo del Software en la que se produjo el error, la pila de memoria del proceso del Software e información sobre las bases de datos antivirus en el momento en que se generó el error;

- datos acerca del volcado del sistema (BSOD): la marca que refleja su aparición en el equipo, el nombre del controlador que provocó el BSOD, la dirección y la pila de memoria del controlador, la marca que refleja la duración de la sesión del SO antes de que ocurriera el BSOD, la pila de memoria de los controladores que se bloquearon, el tipo de volcado de la memoria almacenada, la marca de la sesión del SO antes de que el BSOD se prolongara por más de 10 minutos, el identificador único del volcado y la marca de tiempo del BSOD;

- información sobre los errores o problemas de rendimiento que tuvieron lugar durante la operación de los componentes del Software: identificación del estado del Software, tipo de error, código y causa, así como el horario en el que ocurrió el error, identificador del componente, módulo y proceso del producto en el que tuvo lugar el error, identificador de la tarea o categoría de actualización en el que tuvo lugar el error, registros de las unidades que utiliza el Software (código de error, nombre del módulo, nombre del archivo de origen y línea en la que ocurrió el error);

- información sobre las actualizaciones de bases de datos de antivirus y componentes del Software: nombre, fecha y horario de los archivos de índice descargados durante la última actualización y en descarga en la actualización vigente;

- información sobre la terminación anormal de la operación del Software: marca de tiempo de la creación del volcado, su tipo, tipo de evento que provocó la terminación anormal del funcionamiento del Software (cierre inesperado, error en la aplicación de terceros), fecha y horario del cierre inesperado;

- información sobre la compatibilidad de los controladores del Software con el hardware y el Software: información sobre las propiedades del sistema operativo que limitan la funcionalidad de los componentes del Software (arranque seguro, KPTI, WHQL Enforce, BitLocker, distinción entre mayúsculas y minúsculas), tipo de Software de descarga instalado (UEFI, BIOS), identificador de módulo de plataforma segura (TPM), versión de especificación de TPM, información sobre el CPU instalado en el equipo, modo operativo y parámetros de la Integridad del Código y la Protección de Dispositivos, modo de funcionamiento de los controladores y motivo para utilizar el modo actual, versión de los controladores del Software, estado de soporte de virtualización del software y del hardware del equipo;

- información acerca de las aplicaciones externas que generaron el error: su nombre, la versión y la ubicación; el código de error y la información sobre este, proveniente del registro de aplicaciones del sistema; la dirección de la aparición del error y la pila de la memoria de la aplicación externa; la marca que representa la aparición del error en el componente del Software; el período durante el cual funcionó la aplicación externa antes de que se produjera el error; las sumas de comprobación (MD5, SHA2-256, SHA1) de la imagen del proceso de la aplicación en el cual ocurrió el error; la ruta de acceso a la imagen del proceso de la aplicación y el código del patrón de la ruta de acceso; la información del registro del sistema, con una descripción del error asociado a la aplicación; la información sobre el módulo de la aplicación en la que se produjo el error (el identificador de la excepción, la ubicación del error en la memoria como un desplazamiento del módulo de la aplicación, el nombre y la versión del módulo, el identificador del error de la aplicación en el complemento del Titular de los derechos y la pila de memoria del error, y la duración de la sesión de aplicación antes de que se produjera el error);

- versión del componente de actualización del Software y la cantidad de errores que ocurrieron en este componente durante la ejecución de tareas de actualización durante su ciclo de vida, el identificador de los tipos de tareas de actualización, la cantidad de intentos fallidos que realizó el componente de actualización a fin de completar las tareas correspondientes;

- información sobre el funcionamiento de los componentes de supervisión del sistema del Software: versiones completas de los componentes, fecha y hora en que se iniciaron los componentes, código del evento que desbordó la cola de eventos y la cantidad de dichos eventos, cantidad total de eventos de desborde de la cola, información sobre el archivo del proceso del iniciador del evento (nombre de archivo y su ruta en el equipo, código de plantilla de la ruta del archivo, sumas de comprobación (MD5, SHA2-256, SHA1) del proceso asociado con el archivo, versión del archivo), identificador de la intercepción del evento que tuvo lugar, versión completa del filtro de intercepción, identificador del tipo de evento interceptado, tamaño de la cola del evento y la cantidad de eventos entre el primer evento de la cola y el evento actual, cantidad de eventos vencidos en la cola, información sobre el archivo del proceso del iniciador del evento actual (nombre del archivo y su ruta en el equipo, código de patrón de la ruta del archivo, sumas de comprobación (MD5, SHA2-256, SHA1) del proceso asociado con el archivo), duración del procesamiento del evento, duración máxima del procesamiento del evento, probabilidad del envío de estadísticas, información sobre los eventos del sistema operativo respecto de los cuales se excedió el límite de tiempo de procesamiento (fecha y hora del evento, cantidad de inicializaciones reiteradas de las base de datos de antivirus, fecha y hora de la inicialización repetida por última vez de las base de datos de antivirus luego de su actualización, tiempo de demora de procesamiento del evento para cada uno de los componentes de supervisión del sistema, cantidad de eventos en cola, cantidad de eventos procesados, cantidad de eventos demorados del tipo actual, tiempo de demora total para los eventos del tipo actual, tiempo de demora total para todos los eventos);

- información de la herramienta de seguimiento de eventos de Windows (Event Tracing for Windows, ETW) en caso de que se presenten problemas de rendimiento con el Software, proveedores de eventos SysConfig/SysConfigEx/WinSATAssessment de Microsoft: información sobre el equipo (modelo, fabricante, factor de forma del alojamiento, versión), información sobre las métricas de rendimiento de Windows (evaluaciones WinSAT, índice de rendimiento de Windows), nombre de dominio, información sobre los procesadores físicos y lógicos (cantidad de procesadores físicos y lógicos, fabricante, modelo, nivel de revisión, cantidad de núcleos, frecuencia del reloj, CPUID, características del caché, indicadores de modos e instrucciones compatibles), información sobre los módulos RAM (tipo, factor de forma, fabricante, modelo, capacidad, granularidad de la distribución de la memoria), información sobre las interfaces de red (direcciones IP y MAC, nombre; descripción; configuración de las interfaces de red, desglose de la cantidad y del tamaño de los paquetes de red por tipo, velocidad del intercambio de la red, desglose de la cantidad de errores de red por tipo), configuración del controlador IDE, direcciones IP de los servidores DNS, información sobre la tarjeta de video (modelo, descripción, fabricante, compatibilidad, capacidad de memoria de video, permiso de la pantalla, cantidad de bits por píxel, versión BIOS), información sobre los dispositivos "enchufar y reproducir" (nombre, descripción, identificador del dispositivo [PnP, ACPI], información sobre los discos y dispositivos de almacenamiento (cantidad de discos o unidades flash, fabricante, modelo, capacidad de disco, cantidad de cilindros, cantidad de pistas por cilindro, cantidad de sectores por pista, capacidad del sector, características del caché, número secuencial, cantidad de particiones, configuración del controlador SCSI), información sobre los discos lógicos (número secuencial, capacidad de partición, capacidad de volumen, letra del volumen, tipo de partición, tipo del sistema de archivos, cantidad de clústeres, tamaño del clúster, cantidad de sectores por clúster, cantidad de clústeres vacíos y ocupados, carta de volumen reiniciable, dirección de desplazamiento de la partición en relación con el inicio del disco), información sobre la placa madre BIOS (fabricante, fecha de lanzamiento, versión), información sobre la placa madre (fabricante, modelo, tipo), información sobre la memoria física (capacidad compartida y libre), información sobre los servicios del sistema operativo (nombre, descripción, estado, etiqueta, información sobre los procesos [nombre y PID]), parámetros de consumo de energía para el equipo, configuración del controlador de interrupción, ruta a las carpetas del sistema de Windows (Windows y System32), información sobre el sistema operativo (versión, edición, fecha de lanzamiento, nombre, tipo, fecha de instalación), tamaño del archivo de página, información sobre monitores (cantidad, fabricante, permiso de pantalla, capacidad de resolución, tipo), información sobre el controlador de la tarjeta de video (fabricante, fecha de lanzamiento, versión);

- información sobre ETW, proveedores de eventos EventTrace/EventMetadata de Microsoft: información sobre la secuencia de eventos del sistema (tipo, horario, fecha, zona horaria), metadatos sobre el archivo con resultados de pista (nombre, estructura, parámetros de la pista, desglose de la cantidad de operaciones de pista por tipo), información sobre el sistema operativo (nombre, tipo, versión, edición, fecha de lanzamiento, horario de inicio);

- información de ETW, proveedores de eventos Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power de Microsoft: información sobre los procesos iniciados y completos (nombre, PID, parámetros de inicio, línea de comando, código de retorno, parámetros de administración de la energía, horario de inicio y finalización, tipo de token de acceso, SID, Id. de sesión, cantidad de descriptores instalados), información sobre los cambios en las prioridades del hilo (TID, prioridad, horario), información sobre las operaciones de disco del proceso (tipo, horario, capacidad, cantidad), historial de cambios en la estructura y capacidad de procesos de memoria utilizable;

- información de ETW, proveedores de eventos StackWalk/Perfinfo de Microsoft; información sobre los contadores de rendimiento (rendimiento de secciones de código individual, secuencia de llamadas de función, PID, TID, direcciones y atributos de ISR y DPC);

- información de ETW, proveedor de eventos KernelTraceControl-ImageID de Microsoft: información sobre los archivos ejecutables y las bibliotecas dinámicas (nombre, tamaño de la imagen, ruta completa), información sobre archivos PDB (nombre, identificador), datos de recursos VERSIONINFO para los archivos ejecutables (nombre, descripción, creador, localización, versión e identificador de la aplicación, versión del archivo e identificador);

- información de ETW; proveedores de eventos FileIo/DiskIo/Image/Windows Kernel Disk de Microsoft: información sobre el archivo y las operaciones del disco (tipo, capacidad, horario de inicio, horario de finalización, duración, estado de finalización, PID, TID, direcciones de llamada de la función del controlador, Paquete de Solicitud de E/S (IRP), atributos de objeto de archivo de Windows), información sobre los archivos

que forman parte de operaciones de archivo y disco (nombre, versión, tamaño, ruta completa, atributos, desplazamiento, suma de comprobación de la imagen, acciones abiertas y de acceso);

- información de ETW, proveedor de eventos PageFault de Microsoft: información sobre los errores de acceso de la página de memoria (dirección, horario, capacidad, PID, TID, atributos del objeto de archivo de Windows, parámetros de distribución de la memoria);

- información de ETW, proveedor de eventos de hilo de Microsoft: información sobre la creación/finalización del hilo, información sobre hilos iniciados (PID, TID, tamaño de la pila, prioridades y asignación de recursos del CPU, recursos de E/S, páginas de memoria entre hilos, dirección de la pila, dirección de la función init, dirección del Thread Environment Block [TEB], etiqueta de servicios de Windows);

- información de ETW, proveedor de eventos Microsoft Windows Kernel Memory de Microsoft: información sobre las operaciones de administración de la memoria (estado de finalización, hora, cantidad, PID), estructura de asignación de la memoria (tipo, capacidad, id. de sesión, PID);

- información sobre el funcionamiento del Software en caso de problemas de rendimiento: identificador de la instalación del Software, tipo y valor de caída en el rendimiento, información sobre la secuencia de eventos en el Software (hora, zona horaria, tipo, estado de finalización, identificador del componente de Software, identificador del escenario operativo del Software, TID, PID, direcciones de llamada de funciones), información sobre las conexiones de red a verificarse (URL, dirección de la conexión, tamaño del paquete de red), información sobre los archivos PDB (nombre, identificador, tamaño de imagen del archivo ejecutable), información sobre los archivos a verificarse (nombre, ruta completa; suma de comprobación), parámetros de supervisión del rendimiento del Software;

- información sobre el último reinicio fallido del SO: la cantidad de reinicios fallidos desde la instalación del SO, datos sobre el volcado del sistema (el código y los parámetros del error; el nombre, la versión y la suma de comprobación [CRC32] del módulo que generó el error en el funcionamiento del SO; la ubicación del error como un desplazamiento en el módulo; las sumas de comprobación [MD5, SHA2-256, SHA1] del volcado del sistema);

- información para verificar la autenticidad de los certificados digitales que se utilizan para firmar archivos: la huella digital del certificado, el algoritmo de la suma de comprobación, la clave pública y el número de serie del certificado, el nombre del emisor del certificado, el resultado de la validación del certificado y el identificador de la base de datos del certificado;

- información sobre el proceso que ejecuta el ataque en la autodefensa del Software: el nombre y el tamaño del archivo de proceso, sus sumas de comprobación (MD5, SHA2-256, SHA1), la ruta completa al archivo de proceso y el código de plantilla de la ruta de archivo, las marcas de tiempo de creación/compilación, marca de archivo ejecutable, atributos del archivo de proceso, información sobre el certificado utilizado para firmar el archivo de proceso, código de la cuenta utilizada para iniciar el proceso, Id. de las operaciones realizadas para acceder al proceso, tipo de recurso con el que se realiza la operación (proceso, archivo, objeto de registro, función de búsqueda FindWindow), nombre del recurso con el que se realiza la operación, indicador que muestra que la operación se completó correctamente, el estado del archivo del proceso y su firma según la KSN;

- información sobre el software del titular de los derechos: versión completa, tipo, localización y estado de funcionamiento del software utilizado, versiones de los componentes del software instalados y su estado de funcionamiento, información sobre las actualizaciones de software instaladas, el valor del filtro TARGET, la versión del protocolo utilizado para conectarse a los servicios del titular de los derechos;

- información sobre el hardware que se instaló en el equipo: el tipo, el nombre, el nombre del modelo, la versión del firmware, los parámetros de los dispositivos integrados y conectados, el identificador único del equipo con el Software instalado;

- información sobre las versiones del sistema operativo y de las actualizaciones instaladas, tamaño de palabra, edición y parámetros del modo de ejecución del SO, versión y sumas de comprobación (MD5, SHA2-256, SHA1) del archivo del núcleo del SO, fecha y hora de inicio del SO;

- archivos ejecutables y no ejecutables, total o parcialmente;
- secciones de la RAM del equipo;
- sectores involucrados en el proceso de arranque del SO;
- paquetes de datos tomados del tráfico de red;
- páginas web y mensajes de correo electrónico con objetos sospechosos o malintencionados;
- descripción de las clases e instancias de las clases del repositorio de WMI;
- informes de actividad de aplicaciones:
    - el nombre, tamaño y versión del archivo que se envía, su descripción y sumas de comprobación (MD5, SHA2-256, SHA1), identificador de formato de archivo, el nombre del proveedor del archivo, el nombre del producto al que pertenece el archivo, ruta completa al archivo en el equipo, código de plantilla de la ruta, las marcas de hora de creación y modificación del archivo;
    - fecha/hora de inicio y finalización del período de validez del certificado (si el archivo tiene una firma digital), la fecha y la hora de la firma, el nombre del emisor del certificado, información sobre el titular del certificado, la huella dactilar, la clave pública del certificado y los algoritmos apropiados, y el número de serie del certificado;
    - el nombre de la cuenta desde la que se ejecuta el proceso;
    - sumas de comprobación (MD5, SHA2-256, SHA1) del nombre del equipo en el que se ejecuta el proceso;
    - títulos de las ventanas de proceso;
    - identificador de las bases de datos antivirus, nombre de la amenaza detectada según la clasificación del titular de los derechos;
    - datos sobre la licencia del software instalado, su identificador, tipo y fecha de caducidad;
    - hora local del equipo en el momento de la provisión de información;
    - nombres y rutas de los archivos a los que accedió el proceso;
    - nombres de claves de registro y sus valores a los que accedió el proceso;
    - Direcciones URL e IP a las que accedió el proceso;
    - Direcciones URL e IP desde las que se descargó el archivo en ejecución.

## Cumplimiento de la legislación de la Unión Europea (RGPD)

Kaspersky Endpoint Security puede transmitir datos a Kaspersky en las siguientes situaciones:

- Uso de Kaspersky Security Network
- Activar la aplicación con un código de activación nuevo
- Actualizar módulos de aplicaciones y bases de datos antivirus

- Seguir vínculos en la interfaz de la aplicación
- Creación de archivos de volcado

Independientemente de la clasificación de datos y el territorio desde el que se reciben los datos, Kaspersky respeta altos estándares de seguridad de datos y emplea diversas medidas legales, organizativas y técnicas para proteger los datos de los usuarios, garantizar la seguridad y confidencialidad de los datos, y también garantizar el cumplimiento de los derechos de los usuarios garantizados por la legislación vigente. El texto de la Política de privacidad se incluye en el kit de distribución de la aplicación y está disponible en el sitio web de Kaspersky.

Antes de utilizar Kaspersky Endpoint Security, lea atentamente la descripción de los datos transmitidos en el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network. Si los datos específicos transmitidos desde Kaspersky Endpoint Security en cualquiera de las situaciones descritas pueden clasificarse como datos personales de acuerdo con su legislación o norma local, debe asegurarse de que dichos datos se procesen legalmente y de obtener el consentimiento de los usuarios finales para la recopilación y la transmisión de tales datos.

Puede leer el Contrato de licencia de usuario final y visitar el sitio web de Kaspersky para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn_<identificador del idioma>.txt contienen el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network y están incluidos en el kit de distribución.

Si no desea transmitir datos a Kaspersky, puede deshabilitar el suministro de datos.

## Uso de Kaspersky Security Network

Al utilizar Kaspersky Security Network, acepta proporcionar automáticamente los datos indicados en la Declaración de Kaspersky Security Network. Si no acepta proporcionar estos datos a Kaspersky, utilice KSN Privada o deshabilite 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 nuevo

Al utilizar un código de activación, acepta proporcionar automáticamente los datos enumerados en el Contrato de licencia de usuario final. Si no está de acuerdo en suministrar estos datos con Kaspersky, utilice un archivo de clave para activar Kaspersky Endpoint Security.

## Actualizar módulos de aplicaciones y bases de datos antivirus

Al utilizar los servidores de Kaspersky, acepta proporcionar automáticamente los datos indicados en el Contrato de licencia de usuario final. Kaspersky requiere esta información para verificar que Kaspersky Endpoint Security se esté utilizando legítimamente. Si no acepta proporcionar esta información a Kaspersky, utilice Kaspersky Security Center para actualizaciones de la base de datos o Kaspersky Update Utility.

## Seguir vínculos en la interfaz de la aplicación

Al utilizar los vínculos en la interfaz de la aplicación, acepta proporcionar automáticamente los datos indicados en el Contrato de licencia de usuario final. La lista precisa de datos transmitidos en cada vínculo específico depende de dónde se encuentra el vínculo en la interfaz de la aplicación y del problema que pretende resolver. Si no acepta proporcionar estos datos a Kaspersky, utilice la interfaz de la aplicación simplificada u oculte la interfaz de la aplicación.

## Creación de archivos de volcado

Si ha habilitado la escritura de volcado, Kaspersky Endpoint Security creará un archivo de volcado que incluirá todos los datos de la memoria de los procesos de la aplicación en el momento en que se creó este archivo de volcado.

# Primeros pasos

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

- la interfaz local de la aplicación,
- la Consola de administración de Kaspersky Security Center,
- Kaspersky Security Center 12 Web Console,
- Kaspersky Security Center Cloud Console.

## Consola de administración de Kaspersky Security Center

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

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

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

## Kaspersky Security Center 12 Web Console y Kaspersky Security Center Cloud Console

Kaspersky Security Center 12 Web Console (en lo sucesivo también denominada *Web Console*) es una aplicación web que permite realizar, de manera centralizada, las principales tareas que se requieren para administrar y mantener el sistema de seguridad de la red de una organización. Web Console es un componente de Kaspersky Security Center que proporciona una interfaz de usuario. Para obtener información detallada sobre Kaspersky Security Center 12 Web Console, consulte la *Ayuda de Kaspersky Security Center*.

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

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

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

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

# Acerca del Complemento de administración para Kaspersky Endpoint Security para Windows

El Complemento de administración para Kaspersky Endpoint Security para Windows es el software que posibilita la interacción entre Kaspersky Endpoint Security y Kaspersky Security Center. Con el complemento, podrá administrar Kaspersky Endpoint Security a través de directivas, tareas y la configuración local de la aplicación. La interacción con Kaspersky Security Center 12 Web Console depende del complemento web.

La versión del complemento de administración puede diferir de la versión de Kaspersky Endpoint Security instalada en el equipo cliente. Si la versión instalada del complemento de administración tiene menos funcionalidad que la versión instalada de Kaspersky Endpoint Security, la configuración de las funciones faltantes no será controlada por el complemento de administración. Estos parámetros pueden ser modificados por el usuario en la interfaz local de Kaspersky Endpoint Security.

De manera predeterminada, el complemento web no forma parte de la instalación de Kaspersky Security Center 12 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 12 Web Console. Las funciones del complemento web quedan entonces disponibles para cualquier administrador que pueda acceder a Web Console con un navegador. Puede usar la interfaz de Web Console para ver la lista de complementos web instalados: **Configuración de Console** → **Complementos**. Para más información sobre la compatibilidad de Web Console con las distintas versiones de los complementos 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 utilizando el Asistente de configuración inicial de Kaspersky Security Center 12 Web Console.

  Web Console le pedirá que ejecute el Asistente de configuración inicial cuando se conecte Web Console al Servidor de administración por primera vez. También podrá abrir el Asistente de configuración inicial desde la interfaz de Web Console (**Distribución y detección de dispositivos** → **Distribución y asignación** → **Asistente de configuración inicial**). El Asistente de configuración inicial 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 configuración inicial de Kaspersky Security Center 12 Web Console, consulte la *Ayuda de Kaspersky Security Center*.

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

  Para instalar el complemento web, en la interfaz de Web Console, seleccione el paquete de distribución del complemento web de Kaspersky Endpoint Security: **Configuración de Console** → **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, agregue el archivo ZIP del paquete de distribución para el complemento web de Kaspersky Endpoint Security en la interfaz de Web Console: **Configuración de Console** → **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 para Kaspersky Endpoint Security para Windows, descargue la última versión del complemento (viene incluida en el kit de distribución) y ejecute el asistente de instalación del mismo.

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

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

Puede actualizar el complemento web de las siguientes maneras:

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

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

- Actualice el complemento de web desde un archivo.

  Para actualizar el complemento web, debe seleccionar el archivo ZIP del paquete de distribución para el complemento web de Kaspersky Endpoint Security en la interfaz de Web Console: **Configuración de Console** → **Complementos**. El paquete de distribución del complemento web puede descargarse, por ejemplo, del sitio web de Kaspersky. Solo puede actualizar el complemento web de Kaspersky Endpoint Security a una versión más reciente. El complemento web no puede actualizarse a una versión anterior.

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

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

Puede administrar Kaspersky Endpoint Security mediante Kaspersky Security Center solo si tiene un complemento de administración de la misma versión (o posterior) que la especificada en la información en cuanto a la compatibilidad de Kaspersky Endpoint Security con el complemento de administración. Puede ver la versión mínima requerida del complemento de administración en el archivo installer.ini que se incluye en el kit de distribución.

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

## Actualización del Complemento de administración para Kaspersky Endpoint Security 10 para Windows

Si el Complemento de administración para Kaspersky Endpoint Security 10 para Windows está instalado en la Consola de administración, tenga en cuenta lo siguiente al instalar el Complemento de administración para Kaspersky Endpoint Security 11 para Windows:

- El Complemento de administración para Kaspersky Endpoint Security 10 para Windows no se eliminará y estará disponible para ser usado. Por lo tanto, tendrá acceso a dos complementos de administración para trabajar con las versiones 10 y 11 de la aplicación.
- El Complemento de administración para 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 para Kaspersky Endpoint Security 11 para Windows no es compatible con los elementos (directivas, tareas, etc.) creados con el Complemento de administración para Kaspersky Endpoint Security 10 para Windows.

  Puede usar el Asistente de conversión por lotes de directivas y tareas para convertir las directivas y tareas de la versión 10 a la versión 11. Para más detalles sobre cómo convertir directivas y tareas, consulte la *Guía de ayuda de Kaspersky Security Center*.

## Actualización del Complemento de administración para Kaspersky Endpoint Security 11 para Windows

Si el Complemento de administración para Kaspersky Endpoint Security 11 para Windows está instalado en la Consola de administración, tenga en cuenta lo siguiente al instalar una nueva versión del Complemento de administración para Kaspersky Endpoint Security 11 para Windows:

- Se eliminará la versión anterior del Complemento de administración para Kaspersky Endpoint Security 11 para Windows.
- La nueva versión del Complemento de administración para Kaspersky Endpoint Security 11 para Windows admite la administración de la versión anterior del Kaspersky Endpoint Security 11 para Windows en los equipos de los usuarios.
- Podrá usar la versión nueva para cambiar la configuración de las directivas, tareas y demás elementos que haya creado con la versión anterior.
- Para los parámetros nuevos, la nueva versión del Complemento de administración asigna los valores predeterminados cuando se guarda una directiva, un perfil de directiva o una tarea por primera vez.

  Después de que se actualiza el Complemento de administración, se recomienda revisar y guardar los valores de las nuevas configuraciones de las directivas y los perfiles de las directivas. Si no hace esto, los nuevos grupos de configuraciones de Kaspersky Endpoint Security en el equipo del usuario tomarán los valores predeterminados y se pueden modificar (el atributo). Se recomienda revisar las configuraciones comenzando con las directivas y los perfiles de directivas del nivel jerárquico superior. También se recomienda usar la cuenta de usuario que tenga derechos de acceso a todas las áreas funcionales de Kaspersky Security Center.

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

- Si se ha añadido un nuevo parámetro a un grupo de configuraciones en la nueva versión del Complemento de administración, el estado definido previamente del atributo / para este grupo de configuraciones no cambia.
- 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 pedirá su confirmación para participar en KSN. Si ya actualizó 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 bases de datos y módulos de software de la aplicación;
- Activación de la aplicación con un código de activación (activación 2.0);
- Al usar Kaspersky Security Network.

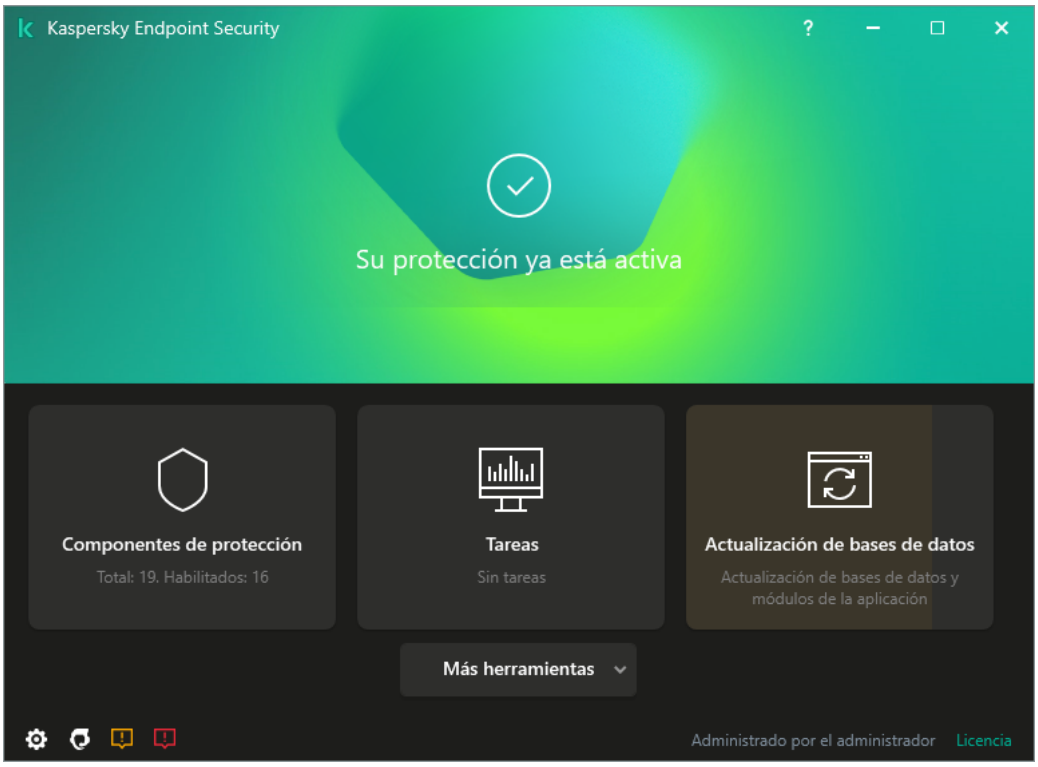
El uso de TLS protege a la aplicación al proporcionar las siguientes características:

- Cifrado. Los contenidos de los mensajes son confidenciales y no se divulgan a terceros.
- Integridad. El destinatario del mensaje está seguro de que el contenido del mensaje no se ha modificado desde que el remitente lo reenvió.
- Autenticación. El destinatario está seguro de que la comunicación se establece solo con un servidor 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 forma parte de una PKI. Kaspersky utiliza su propia autoridad de certificación, ya que los servicios de Kaspersky son altamente técnicos y no tienen carácter público. En este caso, cuando se revocan los certificados raíz de Thawte, VeriSign, GlobalTrust y otros, la PKI de Kaspersky permanece en funcionamiento sin interrupciones.

Kaspersky Endpoint Security considera que los entornos que tienen MITM (herramientas de software y hardware que admiten el análisis del protocolo HTTPS) no son seguros. Es posible que se produzcan errores al trabajar con servicios de Kaspersky. Por ejemplo, puede haber errores relacionados con el uso de certificados autofirmados. Estos errores pueden producirse debido a que una herramienta de inspección HTTPS de su entorno no reconoce la PKI de Kaspersky. Para solucionar estos problemas, debe configurar exclusiones para interactuar con servicios externos.

## Interfaz de aplicación




Ventana principal de la aplicación

| | |
|---|---|
| **Componentes de protección** | Estado operativo de los componentes instalados. También puede proceder a configurar cualquiera de los componentes instalados, excepto los componentes de cifrado. |
| **Tareas** | Administre las tareas de análisis de Kaspersky Endpoint Security. Puede ejecutar un análisis antivirus y una comprobación de integridad de la aplicación. Un administrador puede ocultar tareas a un usuario o restringir la administración de tareas. |
| **Actualización de bases de datos** | Administre las tareas de actualización de Kaspersky Endpoint Security. Puede actualizar las bases de datos antivirus y los módulos de la aplicación, además de revertir la última actualización. Un administrador puede ocultar tareas a un usuario o restringir la administración de tareas. |
| **Más herramientas** | Continúe con otras características de la aplicación.<br>• **Informes**. Visualice eventos que ocurrieron durante el funcionamiento de la aplicación, componentes individuales y tareas.<br>• **Copia de seguridad**. Visualice una lista de copias guardadas de archivos infectados que la aplicación ha eliminado.<br>• **Tecnologías de detección de amenazas**. Visualice información sobre tecnologías de detección de amenazas y la cantidad de amenazas detectadas por estas tecnologías.<br>• **Kaspersky Security Network**. Estado de la conexión entre Kaspersky Endpoint Security y Kaspersky Security Network, y estadísticas de KSN Global. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, 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. |

| | |
|---|---|
| | • **System Watcher**. Visualice información sobre el funcionamiento de las aplicaciones instaladas. System Watcher lleva un registro de los eventos de archivos, del registro y del sistema operativo relacionados con la aplicación.<br>• **Monitor de red**. Visualice información sobre la actividad de red del equipo en tiempo real.<br>• **Monitoreo de Cifrado**. Permite monitorear en tiempo real el cifrado o descifrado de una unidad. El componente Monitoreo de Cifrado estará disponible solamente si también se han instalado los componentes Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker. |
| | Ajuste la configuración de la aplicación. Un administrador puede prohibir cambios en la configuración de Kaspersky Security Center. |
| | Información sobre la aplicación: versión actual de Kaspersky Endpoint Security, fecha de lanzamiento de la base de datos, clave y otra información. También puede proceder a los recursos de información de Kaspersky, que brindan información útil, recomendaciones y respuestas a las preguntas frecuentes sobre cómo comprar, instalar y usar la aplicación. |
| / | Mensajes que contienen información sobre actualizaciones disponibles y solicitudes de acceso a archivos y dispositivos cifrados. |
| **Licencia** | Licencias de la aplicación. Puede adquirir una licencia, activar la aplicación o renovar una suscripción. También puede ver información sobre la licencia actual. |

## Icono de la aplicación en el área de notificación de la barra de tareas

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

El icono tiene las siguientes finalidades:

- Indica la actividad de la aplicación.
- Funciona como acceso directo al menú contextual y a la ventana principal de la aplicación.

El funcionamiento de la aplicación se representa a través de los siguientes iconos de estado:

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

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

- **Kaspersky Endpoint Security para Windows**. Se abre la ventana principal de la aplicación. En esta ventana, puede ajustar el funcionamiento de las tareas y los componentes de la aplicación, además de mostrar las estadísticas de los archivos procesados y las amenazas detectadas.

- **Pausar la protección/Reanudar protección**. Permite poner en pausa todos los componentes de protección y control que no estén marcados con un candado () en la directiva. Recomendamos deshabilitar la directiva de Kaspersky Security Center antes de realizar esta operación.

  Antes de pausar los componentes de protección y control, la aplicación le pedirá la contraseña de acceso a Kaspersky Endpoint Security (contraseña de cuenta o contraseña temporal). A continuación, podrá seleccionar la duración de la pausa. Los componentes pueden quedar en pausa por un tiempo específico, hasta que ocurra un reinicio o hasta que el usuario decida reanudarlos.

  Este elemento del menú contextual está disponible si la protección con contraseña está habilitada. Para que los componentes de protección y control comiencen a funcionar nuevamente, seleccione **Reanudar 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.

- **Deshabilitar directiva** / **Habilitar directiva**. Deshabilitar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado () en la directiva, quedarán desbloqueados y podrán configurarse. Si deshabilita la directiva, la aplicación le solicitará la contraseña de acceso a Kaspersky Endpoint Security (contraseña de cuenta o contraseña temporal). Este elemento del menú contextual está disponible si la protección con contraseña está habilitada. Para habilitar la directiva, seleccione **Habilitar directiva** en el menú contextual de la aplicación.

- Configuración. Permite abrir la ventana de configuración de la aplicación.

- **Soporte**. Esto abre la ventana **Soporte** 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 los detalles de la aplicación.

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


Menú contextual del icono de la aplicación

## Interfaz de la aplicación simplificada

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

- **Deshabilitar directiva** / **Habilitar directiva**. Deshabilitar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado () en la directiva, quedarán desbloqueados y podrán configurarse. Si deshabilita la directiva, la aplicación le solicitará la contraseña de acceso a Kaspersky Endpoint Security (contraseña de cuenta o contraseña temporal). Este elemento del menú contextual está disponible si la protección con contraseña está habilitada. Para habilitar la directiva, seleccione **Habilitar directiva** en el menú contextual de la aplicación.

- **Tareas**. La lista desplegable contiene los siguientes elementos:
  - **Comprobación de integridad**.
  - **Revertir la última actualización**.
  - **Análisis completo**.
  - **Análisis personalizado**.
  - **Análisis de áreas críticas**.
  - **Actualización**.
- **Soporte**. Esto abre la ventana **Soporte** 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 elemento del menú contextual, la aplicación se descarga de la memoria RAM del equipo.


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

## Configuración de la visualización de la interfaz de la aplicación

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

- **Con 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 interfaz completa**. La ventana principal de Kaspersky Endpoint Security y el icono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
- **Ninguna 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 presentación de la interfaz a través de la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Configuración general → Interfaz**.
6. En la sección **Interacción con el usuario**, realice una de las siguientes acciones:
   - Seleccione la casilla **Mostrar interfaz de la aplicación** si desea que se muestren los siguientes elementos de la interfaz en el equipo cliente:
     - Carpeta que contiene el nombre de la aplicación en el menú **Inicio**
     - Icono de Kaspersky Endpoint Security en el área de notificación de la barra de tareas de Microsoft Windows
     - Notificaciones emergentes

     Si se ha seleccionado esta casilla, el usuario podrá ver y, dependiendo de los derechos disponibles, cambiar la configuración de la aplicación desde la interfaz de la aplicación.
   - Desactive la casilla **Mostrar interfaz de la aplicación** si desea ocultar todos los símbolos de Kaspersky Endpoint Security en el equipo del cliente.
7. En la sección **Interacción con el usuario**, seleccione la casilla **Interfaz de la aplicación simplificada** si quiere que se muestre la interfaz simplificada de la aplicación en un equipo del cliente con Kaspersky Endpoint Security instalado.

**Cómo configurar el modo de presentación de la interfaz a través de Web Console y Cloud Console**

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desee permitir el uso del modo portátil.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Configuración general** → **Interfaz**.
5. En la sección **Interacción con el usuario**, elija uno de los siguientes modos de presentación:

   - **Con 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 interfaz completa**. La ventana principal de Kaspersky Endpoint Security y el icono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono.
   - **Ninguna 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. Haga clic en **Aceptar**.

## Primeros pasos

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

- Crear y configurar una directiva.

  Puede utilizar directivas para aplicar configuraciones idénticas de Kaspersky Endpoint Security en todos los equipos cliente dentro de un grupo de administración. El Asistente de configuración inicial de Kaspersky Security Center Web Console 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 configuración inicial 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**.

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.6.0) → Análisis antivirus**.

### Paso 2. Alcance del análisis

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

### Paso 3. Acción de Kaspersky Endpoint Security

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

- **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
- **Desinfectar; informar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.
- **Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.
- **Ejecutar la desinfección avanzada inmediatamente**. Si activa esta casilla, Kaspersky Endpoint Security usará la tecnología de desinfección avanzada para procesar las amenazas activas que se detecten durante el análisis.

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

Utilice la casilla **Ejecutar solo cuando el equipo esté inactivo** para configurar el modo de ejecución de la tarea. Si activa la casilla, la tarea *Análisis antivirus* se suspenderá cuando los recursos del equipo sean limitados. Kaspersky Endpoint Security pondrá la tarea *Análisis antivirus* en pausa si el protector de pantalla está desactivado 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 ejecutará la tarea. Están disponibles los siguientes opciones:

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

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

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

### Paso 6. Programación de la tarea

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

### Paso 7. Nombre de la tarea

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

### Paso 8. Completar creación de la tarea

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. Como resultado, la tarea de análisis de virus se ejecutará en los equipos de los usuarios de acuerdo con la programación 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.

   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 **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

6. Para configurar la programación de la tarea, abra las propiedades de la tarea.

   Recomendamos definir una programación para que la tarea 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 los usuarios de acuerdo con la programación especificada.

## Administración de directivas

Una *directiva* es un grupo de valores de configuración que se han definido para una aplicación y un grupo de administración específicos. Es posible configurar más de una directiva, cada una con valores distintos, para una misma aplicación. La aplicación puede funcionar con configuraciones distintas asociadas a grupos de administración distintos. Cada grupo de administración puede tener su propia directiva para la aplicación.

La configuración de una directiva se envía a los equipos cliente a través del Agente de red durante la *sincronización*. De manera predeterminada, el Servidor de administración ejecuta el proceso de sincronización en cuanto se modifica una directiva. El puerto UDP 15000 en el equipo cliente se usa para la sincronización. El Servidor de administración realiza la sincronización cada 15 minutos por defecto. Si la sincronización falla después de cambiar la configuración de la política, el siguiente intento de sincronización se realizará de acuerdo con el programa configurado.

### 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 con unidades flash, puede activarse una directiva que impida el uso de unidades flash. En tal caso, la directiva activa cambia de estado a inactiva automáticamente.

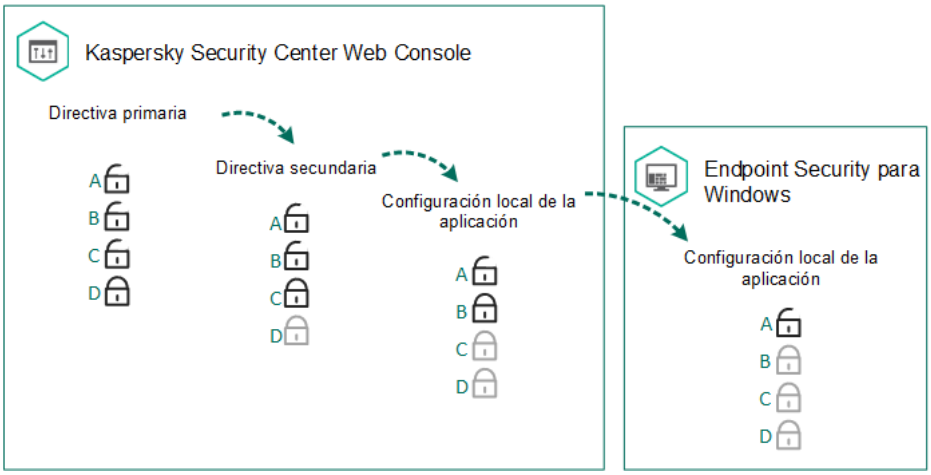
## Directiva fuera de la oficina

Una directiva fuera de la oficina se activa cuando un equipo sale del perímetro de la red de la organización.

## Herencia de configuración

Al igual que los grupos de administración, las directivas se organizan en una jerarquía. De manera predeterminada, las directivas secundarias heredan la configuración de las directivas primarias. Una *directiva secundaria* es una directiva creada para un nivel anidado de una jerarquía; en otras palabras, es una directiva para grupos de administración anidados y Servidores de administración secundarios. Si desea que una directiva secundaria no herede la configuración de su directiva primaria, puede indicarlo.

En las directivas, cada parámetro tiene el atributo que indica si el valor del parámetro se puede modificar en las directivas secundarias o en la configuración local de una aplicación. 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 para la configuración de la directiva de acceso (lectura, escritura y ejecución) se especifican para cada usuario que tiene acceso al Servidor de administración de Kaspersky Security Center y en forma separada para cada alcance funcional de Kaspersky Endpoint Security. Para configurar los derechos para la configuración de la directiva de acceso, diríjase a la sección **Seguridad** de la ventana 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Haga clic en el botón **Nueva directiva**.

   Se inicia el Asistente para directivas.
5. Siga las instrucciones del Asistente para 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 **Agregar**.
   Se inicia el Asistente para directivas.
3. Seleccione Kaspersky Endpoint Security y haga clic en **Siguiente**.
4. Lea y acepte los términos de la Declaración de Kaspersky Security Network (KSN) y haga clic en **Siguiente**.
5. En la ficha **General**, puede realizar las siguientes acciones:
   - Cambiar el nombre de la directiva.
   - Seleccionar el estado de la directiva:
     - **Activa**. Después de la próxima sincronización, la directiva se usará como directiva activa en el equipo.
     - **Inactiva**. Directiva de reserva. Puede convertirse en la directiva activa cuando resulta necesario.
     - **Fuera de la oficina**. La directiva se activa cuando un equipo sale del perímetro de la red de la organización.
   - Configurar la herencia de configuración:
     - **Heredar la configuración de la directiva primaria**. Si activa este interruptor, los valores de configuración de la directiva se tomarán de la directiva de mayor nivel jerárquico. La configuración de la directiva no se puede editar si está establecida para la directiva principal.
     - **Forzar la herencia de configuración en las directivas secundarias**. Si el botón de alternar está activado, los valores de la configuración de la directiva se propagan a las directivas secundarias. En las propiedades de la directiva secundaria, el interruptor **Heredar configuración desde la directiva primaria** se activará automáticamente y no podrá desactivarse. La configuración de la directiva secundaria se hereda de la directiva principal, excepto la configuración marcada con . La configuración de la directiva secundaria no se puede editar si está establecida para la directiva principal.
6. En la ficha **Configuración de la aplicación**, puede modificar la configuración de la directiva de Kaspersky Endpoint Security.
7. Haga clic en el botón **Guardar**.

La configuración de Kaspersky Endpoint Security se aplicará en los equipos cliente cuando se realice la siguiente sincronización. Si desea ver información sobre la directiva aplicada al equipo (por ejemplo, el nombre de la directiva), haga clic en el botón **Soporte** en la ventana principal de la interfaz de Kaspersky Endpoint Security. Tenga en cuenta que, para que ver esta información, la opción para que se pueda obtener información adicional sobre la directiva debe estar habilitada en la directiva del Agente de red. Para más detalles sobre la directiva del Agente de red, consulte la *Guía de ayuda de Kaspersky Security Center*.

## Indicador del nivel de seguridad

El indicador del nivel de seguridad se muestra en la parte superior de la ventana **Propiedades: <Nombre de la directiva>**. El indicador puede tener uno de los valores siguientes:

- **Nivel de protección alto**. El indicador indica este valor y se muestra en verde si están habilitados todos los componentes de las siguientes categorías:
  - **Crítico**. Esta categoría incluye los siguientes componentes:
    - Protección contra archivos peligrosos,
    - Detección de comportamientos.
    - Prevención de exploits.
    - Motor de reparación.
  - **Importantes**. Esta categoría incluye los siguientes componentes:
    - Kaspersky Security Network.
    - Protección contra amenazas web.
    - Protección contra amenazas de correo.
    - Prevención contra intrusos
- **Nivel de protección medio**. El indicador muestra este valor y en color amarillo si se ha deshabilitado uno de los componentes importantes.
- **Nivel de protección bajo**. El indicador muestra este valor y aparece en color rojo en uno de los siguientes casos:
  - Se han deshabilitado uno o varios componentes críticos.
  - Se han deshabilitado dos o más componentes importantes.

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

## Administración de tareas

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

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

Puede crear cuantas tareas locales, de grupo y para selecciones de equipos necesite. Para 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 especifican en la configuración de la tarea en busca de virus y otras amenazas. La tarea *Análisis antivirus*, necesaria para usar Kaspersky Endpoint Security, se crea al utilizar el Asistente de configuración inicial. Recomendamos definir una programación para que la tarea se ejecute al menos una vez por semana.

- **Añadir clave**. Kaspersky Endpoint Security agrega una clave que le permite activarse, así como una clave adicional. Antes de ejecutar la tarea, asegúrese de que el número de equipos en los que la tarea vaya a ejecutarse no supere el número de equipos permitido por la licencia.

- **Cambiar componentes de la aplicación**. Kaspersky Endpoint Security instala o elimina componentes en equipos cliente conforme a la lista de componentes especificada en la configuración de la tarea. El componente Protección contra archivos peligrosos no puede eliminarse. El conjunto óptimo de componentes de Kaspersky Endpoint Security ayuda a hacer un buen uso de los recursos del equipo.

- **Inventario**. Kaspersky Endpoint Security recibe información sobre todos los archivos ejecutables de aplicaciones almacenados en los equipos. La tarea *Inventario* se ejecuta usando el componente Control de aplicaciones. Si Control de aplicaciones no está instalado, la tarea finaliza con un error.

- **Actualización**. 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 configuración inicial. Recomendamos definir una programación para que la tarea se ejecute al menos una vez al día.

- **Eliminación de datos**. Kaspersky Endpoint Security elimina archivos y carpetas de los equipos de los usuarios en forma inmediata o cuando no ha habido conexión con Kaspersky Security Center en mucho tiempo.

- **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 parámetros de las cuentas del Agente de autenticación. Estas cuentas se necesitan para utilizar unidades cifradas. El usuario debe autenticarse con el Agente antes de que se cargue el sistema operativo.

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

## Agregar una nueva tarea

**Cómo crear una tarea con la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. Seleccione la carpeta **Tareas** en el árbol de la Consola de administración.
3. Haga clic en el botón **Nueva tarea**.
   Se inicia el Asistente de tareas.
4. Siga las instrucciones del Asistente de tareas.

**Cómo crear una tarea con Web Console y Cloud Console**

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

   Se abre la lista de tareas.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.

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

   c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, `Actualizar la aplicación para contabilidad`).

   d. En la sección **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en el botón **Siguiente**.

5. Finalice el asistente haciendo clic en el botón **Finalizar**.

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, podrá pausar y reanudar la tarea cuando lo desee.

Puede utilizar la lista de tareas para llevar un control de sus resultados, ver el estado en que se encuentran, acceder a estadísticas sobre las tareas que se han ejecutado en los equipos y más. Para el mismo fin puede crear una selección de eventos (**Supervisión e informes** → **Selecciones de eventos**). Para obtener más información sobre la selección de eventos, *consulte la Guía de 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.

## Controlar el acceso a las tareas

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

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

**Cómo configurar el modo de administración de tareas de la interfaz de Kaspersky Endpoint Security a través de la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Tareas locales** → **Administración de tareas**.
6. Configure el modo de administración de tareas (vea la tabla de más abajo).
7. Guarde los cambios.

**Cómo configurar el modo de administración de tareas de la interfaz de Kaspersky Endpoint Security a través de Web Console**

1. En la ventana principal de Web Console, seleccione la ficha **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desee permitir el uso del modo portátil.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Tareas locales** → **Administración de tareas**.
5. Configure el modo de administración de tareas (vea la tabla de más abajo).
6. Haga clic en **Aceptar**.
7. Confirme sus cambios haciendo clic en **Guardar**.

Configuración de Administración de tareas

| Parámetro | Descripción |
|---|---|
| **Permitir el uso de tareas locales** | Si se selecciona la casilla, las tareas locales se muestran en la interfaz local de Kaspersky Endpoint Security. Cuando no haya restricciones adicionales de la directiva, el usuario puede configurar y ejecutar tareas. Sin embargo, la configuración del programa de ejecución de tareas no está disponible para el usuario. El usuario puede ejecutar tareas solo manualmente.<br>Si la casilla de verificación se desactiva, el uso de tareas locales se detiene. En este modo, las tareas locales no se ejecutan según la programación. Las tareas no pueden iniciarse o configurarse en la interfaz local de Kaspersky Endpoint Security, o al funcionar con la línea de comandos.<br>Un usuario puede iniciar un análisis antivirus de un archivo o carpeta al seleccionar la opción **Buscar virus** en el menú contextual del archivo o carpeta. La tarea de análisis se inicia con los valores predeterminados de configuración para la tarea de análisis personalizado. |
| | |

| | |
|---|---|
| **Permitir que se muestren las tareas de grupo** | Si se selecciona la casilla, las tareas de grupo se muestran en la interfaz local de Kaspersky Endpoint Security. El usuario podrá ver la lista de tareas completa a través de la interfaz de la aplicación.<br><br>Si se desactiva esta casilla, Kaspersky Endpoint Security mostrará una lista de tareas vacía. |
| **Permitir la administración de tareas de grupo** | Si se selecciona esta casilla, los usuarios podrán iniciar y detener las tareas de grupo que se creen en Kaspersky Security Center. Podrán para ello usar cualquiera de las dos interfaces de la aplicación (completa o simplificada).<br><br>Si se desactiva esta casilla, Kaspersky Endpoint Security iniciará las tareas programadas automáticamente. El administrador también podrá iniciar estas tareas manualmente a través de Kaspersky Security Center. |

## Configuración local de la aplicación

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

**Cómo modificar la configuración local de la aplicación a través de la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenece el equipo cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Seleccione el equipo en el cual desea configurar los parámetros de Kaspersky Endpoint Security.
5. En el menú contextual del equipo cliente, seleccione **Propiedades**.

   Se abre la ventana de las propiedades del equipo cliente.
6. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.

   En la parte derecha de la ventana de propiedades del equipo cliente, aparece una lista de aplicaciones de Kaspersky instaladas en el equipo cliente.
7. Seleccione Kaspersky Endpoint Security.
8. Haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.

   Se abre la ventana **Configuración de la aplicación Kaspersky Endpoint Security para Windows**.
9. En la sección **Configuración general**, configure los parámetros correspondientes a Kaspersky Endpoint Security, además de la configuración de los informes y el almacenamiento.

   Las demás secciones de la ventana **Configuración de Kaspersky Endpoint Security para Windows** son idénticas a 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. Para guardar los cambios, en la ventana **Configuración de la aplicación Kaspersky Endpoint Security para Windows**, haga clic en **Aceptar**.

Cómo modificar la configuración local de la aplicación a través de Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **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. Haga los cambios que necesite en la configuración local de la aplicación.
7. La configuración de la aplicación local es igual que la configuración de la directiva, excepto la configuración de cifrado.

## Iniciar y detener Kaspersky Endpoint Security

Cuando termina de instalarse en el equipo de un usuario, Kaspersky Endpoint Security se abre automáticamente. De forma predeterminada, Kaspersky Endpoint Security se inicia después del inicio del sistema operativo. No es posible configurar la autoejecución de la aplicación en el sistema operativo.

Dependiendo de las prestaciones del equipo, las bases de datos antivirus de Kaspersky Endpoint Security pueden tardar hasta dos minutos en descargarse tras el inicio del sistema operativo. Durante este tiempo, el nivel de protección del equipo se reduce. Cuando Kaspersky Endpoint Security se inicia en un sistema operativo que ya está en funcionamiento, descargar las bases de datos no afecta el nivel de protección.

**Cómo definir si Kaspersky Endpoint Security se ejecutará automáticamente a través de la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, vaya a **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 definir si Kaspersky Endpoint Security se ejecutará automáticamente 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 correspondiente a los equipos para los que desea configurar las opciones de inicio.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Configuración general**.
5. Haga clic en el vínculo **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. Haga clic en **Aceptar**.
8. Confirme sus cambios haciendo clic en **Guardar**.

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

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione la sección **General**.
3. Utilice la casilla **Ejecutar al iniciar el equipo** para configurar la forma en que se ejecuta la aplicación.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Los expertos de Kaspersky no recomiendan detener manualmente Kaspersky Endpoint Security ya que, de hacerlo, el equipo y sus datos personales quedan expuestos a amenazas. Si es necesario, puede suspender la protección del equipo mientras tenga que hacerlo, sin detener la aplicación.

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

Cómo iniciar o detener Kaspersky Endpoint Security a través de la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenece el equipo cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Seleccione el equipo en el cual desea iniciar o detener la aplicación.
5. Haga clic con el botón derecho del mouse para mostrar el menú contextual del equipo cliente y seleccione **Propiedades**.
6. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.

   En la parte derecha de la ventana de propiedades del equipo cliente, aparece una lista de aplicaciones de Kaspersky instaladas en el equipo cliente.
7. Seleccione Kaspersky Endpoint Security.
8. Haga lo siguiente:
   - Para iniciar la aplicación, haga clic en el botón  , que encontrará a la derecha de la lista de aplicaciones de Kaspersky.
   - Para detener la aplicación, haga clic en el botón  , que encontrará a la derecha de la lista de aplicaciones de Kaspersky.

Cómo iniciar o detener Kaspersky Endpoint Security a través de Web Console

1. En la ventana principal de Web Console, seleccione **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 detener la aplicación desde la línea de comandos, habilite la administración externa de los servicios del sistema.

El archivo klpsm.exe, que se incluye en el kit de distribución de Kaspersky Endpoint Security, se usa para iniciar o detener la aplicación desde la línea de comandos.

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para iniciar la aplicación mediante la línea de comandos, use el comando `klpsm.exe start_avp_service`.
4. Para detener la aplicación mediante la línea de comandos, use el comando `klpsm.exe stop_avp_service`.

## Suspensión y reanudación de la protección y control del equipo

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

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

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

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

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

*Para pausar la protección y control del equipo:*

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

   Este elemento del menú contextual está disponible si la protección con contraseña está habilitada.
3. Seleccione una de las siguientes opciones:
   - **Suspender durante <periodo>**: las funciones de protección y control del equipo se reactivarán cuando haya transcurrido el tiempo que indique en la lista desplegable de abajo.
   - **Suspender hasta reiniciar la aplicación**: las funciones de protección y control del equipo se reactivarán luego de que cierre y vuelva a abrir la aplicación, o bien cuando se reinicie el sistema operativo. Para utilizar esta opción, debe habilitarse el inicio automático de la aplicación.

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

4. Haga clic en el botón **Pausar la protección**.

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


Menú contextual del icono de la aplicación

*Para reanudar la protección y control del equipo:*

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

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

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

# Análisis del equipo

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

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

## Análisis completo

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

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

Los especialistas de Kaspersky recomiendan no modificar el alcance de la tarea *Análisis completo*.

Para reducir el impacto en los recursos del equipo, recomendamos realizar un análisis en segundo plano en lugar de un análisis completo. El nivel de seguridad del equipo no se verá afectado.

## Análisis de áreas críticas

De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del kernel, los procesos en ejecución y los sectores de inicio del disco.

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

## Análisis personalizado

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

- Memoria del kernel
- Objetos cargados al iniciar el sistema operativo
- Copia de seguridad del sistema operativo

- el buzón de correo de Outlook
- los discos duros, las unidades extraíbles y las 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 inicio, la memoria del sistema y la partición del sistema.

### Comprobación de integridad

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

## Inicio o detención de una tarea de análisis

Independientemente del modo de ejecución de la tarea de análisis seleccionado, puede iniciar o detener una tarea de análisis en cualquier momento.

*Para iniciar o detener una tarea de análisis, realice lo siguiente:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. Haga clic en el botón **Iniciar análisis** si desea ejecutar la tarea de análisis.

   Kaspersky Endpoint Security comenzará a analizar el equipo. La aplicación mostrará el progreso del análisis, la cantidad de archivos analizados y el tiempo de análisis restante. Para detener la tarea en cualquier momento, haga clic en el botón **Detener**.

*Para iniciar o detener una tarea de análisis si está usando la interfaz simplificada de la aplicación:*

1. Haga clic con el botón derecho para mostrar el menú contextual del icono de la aplicación que se encuentra en el área de notificación de la barra de tareas.
2. En la lista desplegable **Tareas** en el menú contextual, realice una de las siguientes opciones:
   - seleccione una tarea de análisis que no se esté ejecutando para iniciarla
   - seleccione una tarea de análisis en ejecución para detenerla
   - seleccione una tarea de análisis suspendida de reanudarla o reiniciarla

## Modificación del nivel de seguridad

Kaspersky Endpoint Security puede usar diferentes grupos de configuraciones para ejecutar un análisis. Estos grupos de configuraciones guardadas en la aplicación se llaman *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que la configuración del nivel de seguridad **Recomendado** es óptima. Es el nivel recomendado por los expertos de Kaspersky. Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración del nivel de seguridad recomendada.

*Para cambiar un nivel de seguridad:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. En la sección **Nivel de seguridad**, realice una de las siguientes acciones:
   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
     - **Alto**. Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, Kaspersky Endpoint Security también analiza archivos en formato de correo.
     - **Recomendado**. Kaspersky Endpoint Security analiza solamente los formatos de archivo especificados en todos los discos duros, las unidades de red, los medios de almacenamiento extraíbles del equipo y los objetos OLE integrados. Kaspersky Endpoint Security no analiza los archivos de almacenamiento ni los paquetes de instalación.
     - **Bajo**. Kaspersky Endpoint Security analiza solamente los archivos nuevos o modificados con las extensiones especificadas en todos los discos duros, las unidades extraíbles y las unidades de red del equipo. Kaspersky Endpoint Security no analiza los archivos compuestos.
   - Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y configure los ajustes del componente.

     Para restablecer los valores de los niveles de seguridad prestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado** en la parte superior de la ventana.
4. Guarde los cambios.

## Modificación de la acción que se llevará a cabo en archivos infectados

Por defecto, en la detección de archivos infectados, Kaspersky Endpoint Security trata de desinfectarlos, o los elimina en caso de que no sea posible realizar la desinfección.

*Para modificar la acción que se llevará a cabo en archivos infectados:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. En el bloque **Acción al detectar una amenaza**, seleccione una de estas opciones:
   - **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.

- **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.

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

Antes de intentar desinfectar o eliminar un archivo infectado, Kaspersky Endpoint Security crea una copia de seguridad del archivo en caso de que necesite restaurarlo o si se puede desinfectar en el futuro.

Si se detectan archivos infectados que forman parte de la aplicación Windows Store, Kaspersky Endpoint Security intenta eliminarlos.

4. Guarde los cambios.

## Generar una lista de objetos para analizar

*Para generar una lista de objetos para analizar:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en el vínculo **Editar el alcance del análisis**.
4. En la ventana que se abre, seleccione los objetos que desea agregar al alcance del análisis o excluir de él.

   No puede quitar ni modificar objetos que estén incluidos en el alcance del análisis predeterminado.

5. Si quiere agregar un objeto nuevo al alcance del análisis:

   a. Haga clic en el botón **Agregar**.

   Se abre el árbol de carpetas.

   b. Seleccione el objeto y haga clic en **Seleccionar**.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en el alcance del análisis. Para hacerlo, desactive la casilla ubicada junto al objeto.

6. Guarde los cambios.

## Selección del tipo de archivos para analizar

Cuando seleccione el tipo de archivos por analizar, tenga presenta la siguiente información:

1. La probabilidad de que ciertos tipos de archivos (por ejemplo, los de formato TXT) contengan código malintencionado que pueda activarse es baja. Existen, por otro lado, formatos de archivo que sí contienen código ejecutable (.exe, .dll y otros). Junto con estos, existen ciertos tipos de archivos que pueden contener código ejecutable aunque no estén principalmente diseñados para ello (por ejemplo, los archivos de formato DOC). El riesgo de que el código malicioso ingrese en estos archivos y se active es alto.

2. Un intruso podría enviarle un archivo de extensión .txt que sea, en realidad, un ejecutable peligroso (un virus u otro tipo de aplicación malintencionada) al que se le ha cambiado el nombre. Si selecciona el análisis de archivos por extensión, la aplicación omite este archivo durante el análisis. Si se selecciona el análisis de archivos por formato, Kaspersky Endpoint Security analiza el encabezado del archivo independientemente de la extensión. Si se determina que el archivo es de un formato ejecutable (por ejemplo, EXE), se lo somete a análisis.

*Para seleccionar el tipo de archivos para analizar, realice lo siguiente:*

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

2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.

3. Haga clic en el botón **Configuración avanzada**.

4. En la sección **Tipos de archivos**, especifique el tipo de archivos que desea analizar cuando se ejecute la tarea de análisis seleccionada:

   - **Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones).

   - **Archivos analizados según su formato**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.

   - **Archivos analizados según su extensión**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión.

   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.

5. Guarde los cambios.

## Optimización del análisis de archivos

Puede optimizar el análisis de archivos: reducir la duración del análisis y aumentar la velocidad operativa de Kaspersky Endpoint Security. Esto se puede lograr analizando solamente los archivos nuevos y aquellos que se han modificado desde el análisis anterior. Este modo se aplica tanto a archivos simples como compuestos. También puede establecer un límite para el análisis de un único archivo. Cuando termina el intervalo de tiempo especificado, Kaspersky Endpoint Security excluye el archivo del análisis actual (excepto los archivos de almacenamiento y objetos que incluyen varios archivos).

También puede habilitar el uso de las tecnologías iChecker y iSwift. Estas tecnologías reducen el tiempo de análisis al asegurarse de que los archivos que no hayan cambiado desde el último análisis no se vuelvan a controlar.

*Para optimizar el análisis de archivos:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Optimización de análisis**, defina la configuración de análisis:
   - **Analizar solo archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como compuestos.
   - **Omitir archivos que se analicen por más de N segundos**. Limita la duración del análisis de un solo objeto. Luego de un período especificado de tiempo, Kaspersky Endpoint Security detiene el análisis de un archivo. Esto ayuda a reducir la duración del análisis.
5. Guarde los cambios.

## Análisis de archivos compuestos

Una técnica común para ocultar virus u otro malware es implantarlo en archivos compuestos, como archivos de almacenamiento o bases de datos. Para detectar virus u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

*Para configurar el análisis de archivos compuestos:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Análisis de archivos compuestos**, especifique qué archivos compuestos desea analizar: archivos de almacenamiento, paquetes de instalación, archivos con formato de Office, archivos con formatos de correo y archivos de almacenamiento protegidos con contraseña.
5. Si el análisis de solo archivos nuevos y modificados está desactivado, defina la configuración para analizar cada tipo de archivo compuesto: analice todos los archivos de este tipo o solo los archivos nuevos.

   Si está habilitado el análisis de archivos nuevos y modificados, Kaspersky Endpoint Security analiza solo archivos nuevos y modificados de todos los tipos de archivos compuestos.
6. En el bloque **Límite de tamaño**, realice una de las siguientes acciones:
   - Si no desea descomprimir archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos grandes** y especifique el valor deseado en el campo **Tamaño máximo de archivo**.
   - Si quiere descomprimir archivos compuestos grandes independientemente de su tamaño, desmarque la casilla **No desempaquetar archivos compuestos grandes**.

Kaspersky Endpoint Security analiza los archivos de gran tamaño que se extraen de archivos comprimidos, independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

7. Guarde los cambios.

## Uso de métodos de análisis

Kaspersky Endpoint Security usa una técnica de análisis llamada Aprendizaje automático y análisis de firmas. Durante el análisis de firmas, Kaspersky Endpoint Security compara el objeto detectado con los registros en su base de datos. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado.

Para aumentar la efectividad de la protección, puede utilizar el análisis heurístico. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

*Para utilizar métodos de análisis:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en el botón **Configuración avanzada**.
4. Si desea que la aplicación utilice el análisis heurístico al ejecutar la tarea de análisis, seleccione la casilla **Análisis heurístico** en el bloque **Métodos de análisis**. A continuación, utilice el control deslizante para definir el nivel de análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.
5. Guarde los cambios.

## Uso de tecnologías de análisis

*Para utilizar tecnologías de análisis:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Tecnologías de análisis**, seleccione las casillas junto a los nombres de las tecnologías que desea utilizar durante un análisis:

   - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

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

5. Guarde los cambios.

## Seleccionar el modo de ejecución para la tarea de análisis

Si no es posible ejecutar la tarea de análisis por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha ignorado para que se inicie automáticamente tan pronto como sea posible.

Puede posponer el inicio de la tarea de análisis luego del inicio de la aplicación si la hora de inicio de la tarea de análisis coincide con la hora de inicio de Kaspersky Endpoint Security. La tarea de análisis solo se puede ejecutar una vez transcurrido el intervalo de tiempo especificado después del inicio de Kaspersky Endpoint Security.

*Para seleccionar el modo de ejecución de la tarea de análisis:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en el botón **Programar análisis**.
4. En la ventana que se abre, configure la programación de la ejecución de la tarea de análisis.
5. Según la frecuencia seleccionada, defina configuraciones avanzadas que especifiquen la programación de ejecución de la tarea.
   a. Seleccione **Ejecutar análisis programado al día siguiente si el equipo está apagado** si desea que Kaspersky Endpoint Security ejecute las tareas de análisis no realizadas en la primera oportunidad.

      Si el elemento **Cada minuto**, **Cada hora**, **Luego del inicio de la aplicación** o **Luego de cada actualización** está seleccionado en la lista desplegable **Ejecutar el análisis**, la casilla de verificación **Ejecutar el análisis programado al día siguiente si el equipo está apagado** no está disponible.

   b. Si desea que Kaspersky Endpoint Security suspenda una tarea cuando los recursos del equipo sean limitados, seleccione la casilla **Ejecutar solo cuando el equipo está inactivo**. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado.

      Esta opción de programación permite conservar recursos del equipo.

6. Guarde los cambios.

## Inicio de una tarea de análisis con la cuenta de un usuario diferente

Por defecto, una tarea de análisis se ejecuta con los permisos de la cuenta con la que el usuario inició sesión en el sistema operativo. Sin embargo, cabe la posibilidad de que necesite ejecutar una tarea de análisis con una cuenta de usuario distinta. Puede especificar un usuario con los permisos adecuados en la configuración de la tarea de análisis y ejecutar dicha tarea con la cuenta de este usuario.

*Para configurar el inicio de una tarea de análisis con una cuenta de usuario diferente:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Haga clic en **Configuración avanzada** → **Ejecutar análisis como**.
4. En la ventana que se abre, seleccione el usuario que necesita los derechos para iniciar la tarea de análisis.
5. Guarde los cambios.

## Análisis de unidades extraíbles cuando se conectan al equipo

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

*Para configurar el análisis de los discos extraíbles cuando se conectan, haga lo siguiente:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis de la unidad extraíble y haga clic en el botón ⚙.
3. Utilice el interruptor **Análisis de unidades extraíbles** para habilitar o deshabilitar los análisis de unidades extraíbles al conectarse al equipo.
4. Seleccione el modo para analizar unidades extraíbles al conectarse:
   - **Análisis detallado**. Si se selecciona esta opción, cuando se conecte una unidad extraíble, Kaspersky Endpoint Security analiza todos los archivos ubicados en la unidad extraíble, incluidos los archivos dentro de objetos compuestos, las carpetas comprimidas, los paquetes de distribución y los archivos con formato de Office. Kaspersky Endpoint Security no analiza archivos en formatos de correo o archivos protegidos con contraseña.
   - **Análisis rápido**. Si se selecciona esta opción, cuando se conecte una unidad extraíble, Kaspersky Endpoint Security analizará solo los archivos que sean de algunos formatos específicos, por ser los más propensos a estar infectados. Los objetos compuestos no se desempaquetarán.
5. Si desea que Kaspersky Endpoint Security analice solamente las unidades extraíbles con un tamaño que no exceda un valor especificado, seleccione la casilla **Tamaño máximo de la unidad extraíble** y especifique el valor (en megabytes) en el campo adyacente.

6. Configure cómo se mostrará el progreso del análisis de un disco extraíble. Realice una de las siguientes acciones:

   - Si desea que Kaspersky Endpoint Security muestre el progreso del análisis en una ventana independiente, active la casilla **Mostrar el progreso del análisis**.

     El usuario podrá detener el análisis de una unidad extraíble a través de la ventana de análisis. Para evitar esto y asegurarse de que las unidades extraíbles siempre se analicen, active la casilla **No permitir que se detenga la tarea de análisis**.

   - Si desea que Kaspersky Endpoint Security ejecute un análisis del disco extraíble en segundo plano, desactive la ventana **Mostrar progreso de análisis**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

## 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 inicio, la memoria del sistema y la partición del sistema. La aplicación inicia un análisis en segundo plano en los siguientes casos:

- después de que se actualizan las bases de datos antivirus;
- cuando Kaspersky Endpoint Security se ha estado ejecutando por treinta minutos;
- cada seis horas;
- Cuando el equipo está inactivo durante cinco minutos o más (el equipo está bloqueado o el protector de pantalla está encendido).

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

- el equipo pasa al modo activo;

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

- el equipo (portátil) comienza a funcionar con batería.

> Cuando se realiza un análisis en segundo plano, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.

*Para que el equipo se analice en segundo plano:*

1. En la ventana principal de la aplicación, haga clic en el botón **Tareas**.
2. En la ventana que se abre, seleccione la tarea de análisis y haga clic en el botón ⚙.
3. Utilice el interruptor **Análisis en segundo plano** para habilitar o deshabilitar esta característica.

4. Guarde los cambios.

## Comprobación de la integridad de la aplicación

Kaspersky Endpoint Security verifica si los archivos almacenados en la carpeta de instalación del programa presentan daños 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.

Para crear la tarea *Comprobación de integridad*, deberá usar la Consola de administración de Kaspersky Security Center 12 o Kaspersky Security Center 12 Web Console. No es posible crear esta tarea con Kaspersky Security Center Cloud Console.

**Cómo ejecutar una comprobación de integridad de la aplicación a través de 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**.

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.6.0)** → **Comprobación de integridad**.

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

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

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

### Paso 3. Programación de la tarea

Programe la ejecución de la tarea. Puede hacer que la tarea se inicie manualmente o cuando se detecte un brote de virus, por ejemplo.

### Paso 4. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo `Comprobar la integridad de la aplicación tras una infección`.

### Paso 5. Completar creación de la tarea

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma. Como resultado, Kaspersky Endpoint Security realizará una comprobación de integridad. Si lo desea, puede modificar las propiedades de la tarea para que la integridad de la aplicación se verifique en forma programada.

[Cómo ejecutar una comprobación de integridad de la aplicación a través de 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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.

   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 **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

5. Finalice el asistente haciendo clic en el botón **Finalizar**.

   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 en forma programada.

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.

# Actualización de bases de datos y módulos de software de la aplicación

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Endpoint Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

Las actualizaciones regulares requieren una licencia en vigencia. Si no hay una licencia actual, se podrá realizar una única actualización.

La principal fuente de actualizaciones de Kaspersky Endpoint Security son los servidores de actualizaciones de Kaspersky.

Su equipo debe estar conectado a Internet para descargar correctamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. Por defecto, la configuración de la conexión a Internet se determina automáticamente. Si utiliza un servidor proxy, debe definir su configuración.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTP.

Al realizar una actualización, se descargan e instalan en el equipo los siguientes objetos:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se brinda con bases de datos que contienen firmas de virus y otras amenazas e información sobre maneras de neutralizarlas. Los componentes de protección utilizan esta información al realizar búsquedas de archivos infectados en el equipo y neutralizarlos. Las bases de datos se actualizan constantemente con registros de amenazas nuevas y métodos para contrarrestarlas. Por lo tanto, le recomendamos actualizar las bases de datos con regularidad.

  Además de las bases de datos de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de la aplicación interceptar el tráfico de la red.

- Módulos de la aplicación. Además de las bases de datos de Kaspersky Endpoint Security, también se pueden actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación repara vulnerabilidades en Kaspersky Endpoint Security y agrega funciones nuevas o mejora funciones existentes.

Durante la actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con la versión actualizada en el origen de actualizaciones. Si las bases de datos y los módulos de la aplicación actuales difieren de las respectivas versiones actualizadas, la parte faltante de las actualizaciones se instala en el equipo.

Los archivos de ayuda contextual se pueden actualizar junto con las actualizaciones de los módulos de la aplicación.

Si las bases de datos están obsoletas, es posible que el tamaño del paquete de actualización sea considerable, lo que puede ocasionar un mayor tráfico web (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en la sección **Actualización** en la ventana **Tareas**.

La información sobre los resultados de la actualización y sobre todos los eventos que ocurren durante la ejecución de la tarea de actualización se registra en el informe de Kaspersky Endpoint Security.

# Modalidades de actualización para las bases de datos y los módulos

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Endpoint Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

Los objetos que se actualizan en los equipos de los usuarios son los siguientes:

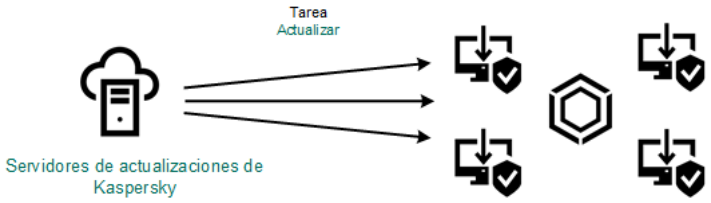
- Bases de datos antivirus. Las bases de datos antivirus contienen bases de datos con firmas de malware, descripciones de ataques de red, bases de datos de direcciones web fraudulentas y malintencionadas, bases de datos de banners, bases de datos de spam y otras clases de información.

- Módulos de la aplicación. Las actualizaciones de módulos están diseñadas para eliminar vulnerabilidades de la aplicación y mejorar los métodos con los que se protegen los equipos. Cuando se actualizan los módulos, la aplicación puede sumar nuevas funciones y modificar el comportamiento de sus componentes.

Las bases de datos y los módulos de Kaspersky Endpoint Security pueden actualizarse de las siguientes maneras:

- Actualización con los servidores de Kaspersky.

  Los servidores de actualización de Kaspersky se encuentran en varios países del mundo. Gracias a ello, el proceso de actualización es altamente fiable. Cuando Kaspersky Endpoint Security no puede descargar las actualizaciones de un servidor, cambia a uno distinto.




Actualización con los servidores de Kaspersky.

- Actualización centralizada.

  La actualización centralizada reduce el tráfico de Internet externo y facilita el control del proceso.

  La actualización centralizada consta de los siguientes pasos:

  1. Descargar el paquete de actualización a un repositorio ubicado en la red de la organización.

     Para descargar el paquete de actualización, se utiliza la tarea del Servidor de administración llamada *Descargar actualizaciones en el repositorio del Servidor de administración*.

  2. Descargar el paquete de actualización a una carpeta compartida (opcional).

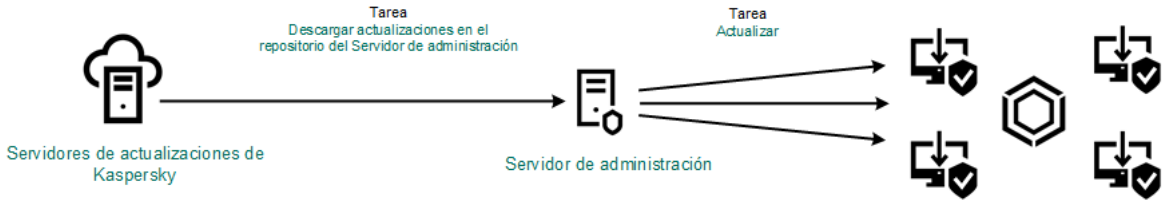
     Para descargar el paquete de actualización a una carpeta compartida, puede usar los siguientes métodos:

     - Utilizar la tarea de *actualización* de Kaspersky Endpoint Security. La tarea está diseñada para uno de los equipos en la red de la compañía local.

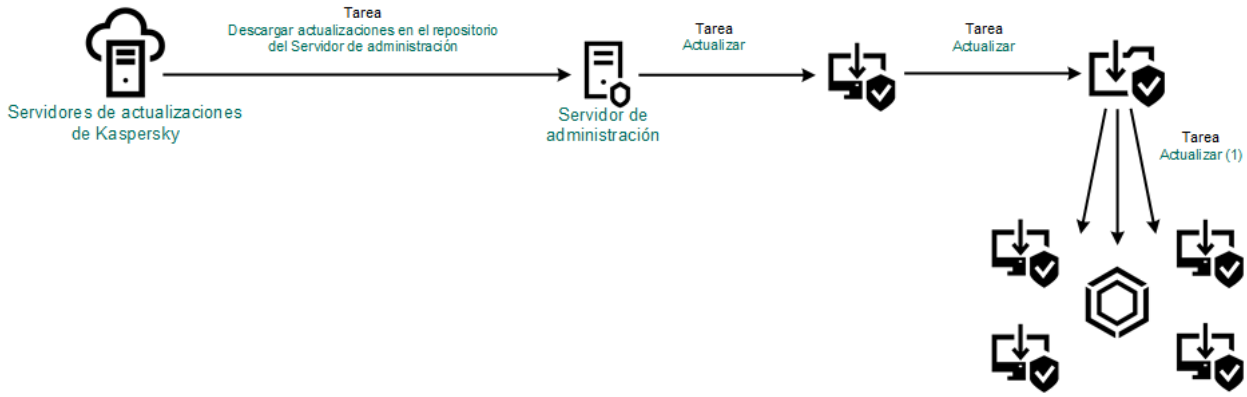
     - Usar la herramienta Kaspersky Update Utility. Para obtener información detallada sobre el uso de Kaspersky Update Utility, *consulte la Base de conocimientos de Kaspersky*.

  3. Distribuir el paquete de actualización a los equipos cliente.

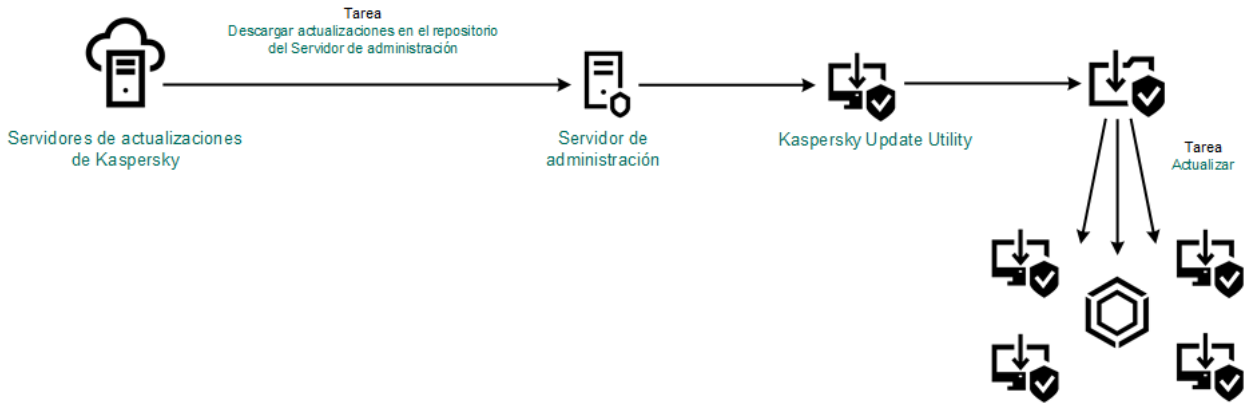
Para distribuir el paquete a los equipos cliente, utilice la tarea *Actualización* de Kaspersky Endpoint Security. Podrá crear cuantas tareas de actualización necesite para cada grupo de administración.




Actualización con un repositorio de servidor




Actualización con una carpeta compartida




Actualización con Kaspersky Update Utility

En Web Console, los orígenes de actualizaciones disponibles por defecto son el Servidor de administración de Kaspersky Security Center y los servidores de actualizaciones de Kaspersky. En Kaspersky Security Center Cloud Console, los orígenes por defecto son los puntos de distribución y los servidores de actualizaciones de Kaspersky. Para obtener más información sobre los puntos de distribución, consulte la *Ayuda de Kaspersky Security Center Cloud Console*. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las actualizaciones. Cuando Kaspersky Endpoint Security no puede descargar las actualizaciones de un origen, cambia a uno distinto.

Las actualizaciones se descargan de los servidores de actualizaciones de Kaspersky, o de otros servidores FTP o HTTP, usando protocolos de red estándar. Si la conexión al origen de actualizaciones debe establecerse a través de un servidor proxy, especifique los parámetros de conexión pertinentes en la configuración de la directiva de Kaspersky Endpoint Security.

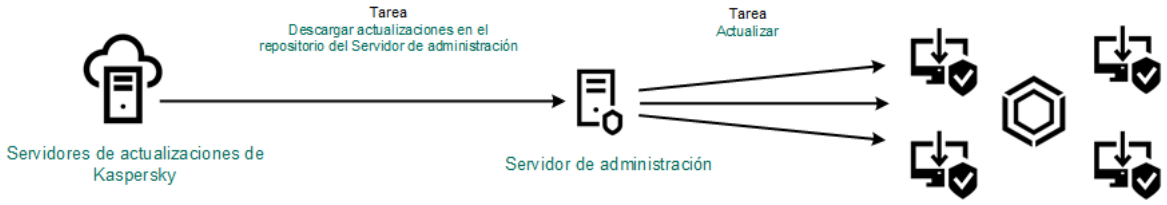
## Actualización con un repositorio de servidor

Para reducir el tráfico de Internet, los equipos conectados a la LAN de la organización pueden obtener las actualizaciones de las bases de datos y de los módulos de la aplicación de un repositorio de servidor. En esta modalidad, Kaspersky Security Center descarga un paquete de actualización de los servidores de actualizaciones de Kaspersky y lo guarda en un repositorio (un servidor FTP o HTTP, una carpeta de red o una carpeta local). Los demás equipos conectados a la LAN obtienen de allí el paquete de actualización.

Si desea utilizar un repositorio del servidor para actualizar las bases de datos y los módulos de la aplicación, debe realizar las siguientes acciones:

1. Configurar la descarga 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*).




Actualización con un repositorio de servidor

*Para configurar la descarga de un paquete de actualización a un repositorio del servidor:*

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

   Se abre la lista de tareas.

2. Seleccione la tarea del Servidor de administración **Descargar actualizaciones al repositorio**.

   Se abre la ventana de propiedades de la tarea.

   La tarea del Servidor de administración *Descargar actualizaciones en el repositorio* se crea automáticamente al usar el Asistente de configuración inicial de Kaspersky Security Center 12 Web Console. Solo puede existir una versión 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 las 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:

   - Si el origen es un servidor FTP o HTTP, escriba la dirección web o la dirección IP.

     Por ejemplo, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

     Si es necesario autenticarse para acceder al servidor FTP, especifique los datos en la dirección siguiendo este formato: `ftp://<nombre de usuario>:<contraseña>@<nodo>:<puerto>`.

   - Si el origen es una carpeta de red, escriba la ruta UNC.

     Por ejemplo, `\\ Server\Share\Update distribution`.

   - Si el origen es una carpeta local o de red, escriba la ruta completa de la carpeta.

     Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\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 de propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente al usar el Asistente de configuración inicial 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 **Agregar**.

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 las actualizaciones** cuando configuró la descarga de actualizaciones en el almacenamiento del servidor (consulte *las instrucciones anteriores*).

6. En la sección **Estado**, seleccione **Habilitado**.

7. Haga clic en **Aceptar**.

8. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.

9. Haga clic en el botón **Guardar**.

Cuando Kaspersky Endpoint Security no pueda descargar las actualizaciones del primer origen, cambiará al siguiente de manera automática.

## Actualización con una carpeta compartida

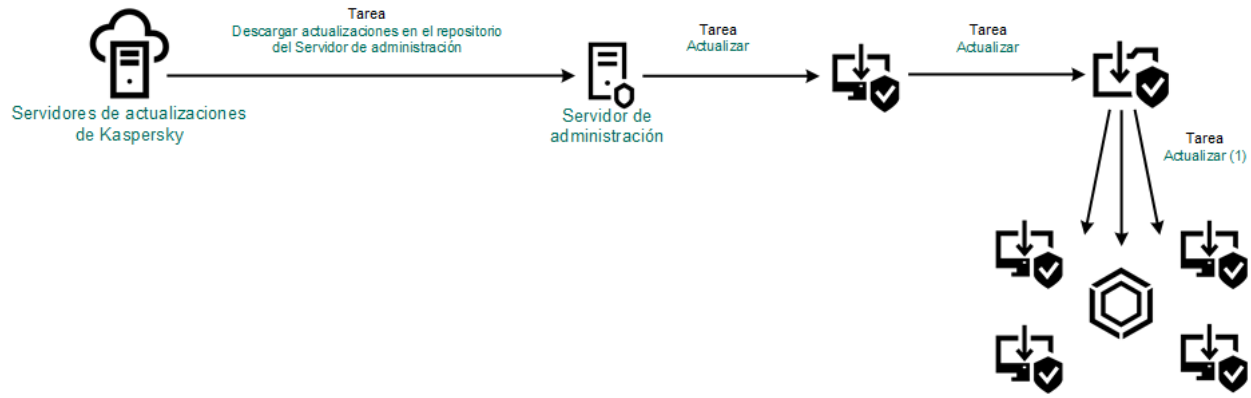
Para reducir el tráfico de Internet, los equipos conectados a la LAN de la organización pueden obtener las actualizaciones de las bases de datos y de los módulos de la aplicación de una carpeta compartida. En esta modalidad, uno de los equipos de la LAN se encarga de recibir los paquetes de actualización 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. Configurar el uso de un repositorio alojado en un servidor para actualizar las bases de datos y los módulos de la aplicación.

2. Habilite la opción para que el paquete de actualización se copie a una carpeta compartida en uno de los equipos de la LAN de la organización (vea las instrucciones a continuación).

3. Configure las actualizaciones de los módulos de la aplicación y la base de datos desde la carpeta compartida especificada hacia los equipos restantes en la LAN de la organización (vea las instrucciones a continuación).




Actualización con una carpeta compartida

*Para habilitar la copia del paquete de actualización a 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 de propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente al usar el Asistente de configuración inicial 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**, escriba la ruta UNC de 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. Haga clic en el botón **Guardar**.

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 **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.

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

   c. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, `Actualizar desde una carpeta compartida`).

   d. En la sección **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

   > La tarea *Actualización* debe asignarse a los equipos conectados a la LAN de la organización, salvo al que actúa como origen de actualizaciones.

4. Seleccione dispositivos de acuerdo con la opción de alcance de la tarea que haya elegido y haga clic en **Siguiente**.

5. Finalice el asistente haciendo clic en el botón **Crear**.

   La nueva tarea aparecerá en la tabla de tareas.

6. Haga clic en la tarea *Actualización* que acaba de crear.

   Se abre la ventana de propiedades de la tarea.

7. Vaya a la sección **Propiedades de la aplicación**.

8. Seleccione la ficha **Modo local**.

9. En la sección **Origen de actualizaciones**, haga clic en el botón **Agregar**.

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 **Subir** y **Bajar**.

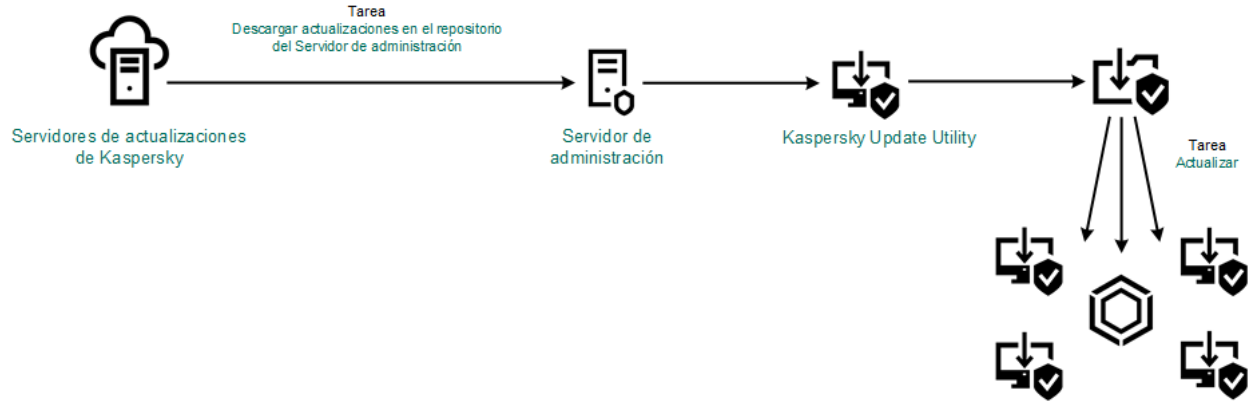
13. Haga clic en el botón **Guardar**.

## 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. Configurar el uso de un repositorio alojado en un servidor para actualizar las bases de datos y los módulos de la aplicación.
2. Instale Kaspersky Update Utility en uno de los equipos conectados a la LAN de su organización.
3. Configure Kaspersky Update Utility para que el paquete de actualización se copie a la carpeta compartida.
4. Configurar el proceso de actualización para que los demás equipos conectados a la LAN de la organización obtengan las bases de datos y los módulos más recientes de la carpeta compartida.




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 de propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente al usar el Asistente de configuración inicial 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 **Agregar**.
5. En el campo **Origen**, escriba la ruta UNC de 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 **Subir** y **Bajar**.

8. Haga clic en el botón **Guardar**.

## Actualización en modo móvil

El *modo móvil* es el modo de operación de Kaspersky Endpoint Security, cuando un equipo sale del perímetro de la red de organización (*equipo desconectado*). Para más información sobre cómo trabajar con los equipos sin conexión y los usuarios que están fuera de la oficina, *consulte la Ayuda de Kaspersky Security Center*.

Los equipos sin conexión a la red de la organización no pueden acceder al Servidor de administración para actualizar las bases de datos y los módulos de la aplicación. De forma predeterminada, solo los servidores de actualización de Kaspersky se utilizan como fuente de actualización para actualizar bases de datos y módulos de aplicaciones en el modo móvil. El uso de un servidor proxy para acceder a Internet se rige por una directiva especial, llamada directiva fuera de la oficina. Esta directiva debe crearse por separado. Cuando Kaspersky Endpoint Security cambia al modo móvil, la tarea de actualización se ejecuta cada dos horas.

*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 de propiedades de la tarea.

   La tarea *Actualización* se crea automáticamente al usar el Asistente de configuración inicial 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 ficha **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. Haga clic en el botón **Guardar**.

Una vez que complete estos pasos, los equipos del usuario estarán en condiciones de actualizar las bases de datos y los módulos de la aplicación cuando pasen al modo móvil.

## Inicio y detención de una tarea de actualización

Independientemente del modo de ejecución seleccionado para la tarea de actualización, puede iniciar o detener una tarea de actualización de Kaspersky Endpoint Security en cualquier momento.

*Para iniciar o detener una tarea de actualización:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.

2. En el bloque **Actualización de las bases de datos y módulos de aplicación**, haga clic en el botón **Actualizar** si desea iniciar la tarea de actualización.

Kaspersky Endpoint Security comenzará a actualizar las bases de datos y módulos de aplicación. La aplicación mostrará el progreso de la tarea, el tamaño de los archivos descargados y el origen de actualizaciones. Puede hacer clic en el botón  para detener esta tarea en cualquier momento.

*Iniciar o detener una tarea de actualización cuando se muestra la interfaz simplificada de la aplicación:*

1. Haga clic con el botón derecho para mostrar el menú contextual del icono de la aplicación que se encuentra en el área de notificación de la barra de tareas.
2. En la lista desplegable **Tareas** en el menú contextual, realice una de las siguientes opciones:
   - seleccione una tarea de actualización que no se esté ejecutando para iniciarla
   - seleccione una tarea de actualización en ejecución para detenerla
   - seleccione una tarea de actualización suspendida de reanudarla o reiniciarla

## Inicio de una tarea de actualización según los derechos de una cuenta de usuario distinta

Por defecto, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta ha usado para iniciar sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security puede actualizarse desde un origen de actualizaciones al cual el usuario que inició sesión no puede acceder debido a la falta de permisos exigidos (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o una fuente de actualización para la cual no se ha configurado la autenticación del servidor proxy. En la configuración de Kaspersky Endpoint Security, puede especificar un usuario que tenga dichos permisos y comenzar la tarea de actualización de Kaspersky Endpoint Security según dicha cuenta de usuario.

*Para iniciar una tarea de actualización con una cuenta de usuario distinta:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.
2. Seleccione la tarea *Actualización* y haga clic en el **Modo de ejecución: Vínculo de <modo>**.
   Se abren las propiedades de la tarea *Actualización*.
3. Haga clic en el botón **Configurar cuenta de usuario**.
4. En la ventana que se abre, seleccione la opción **Ejecutar las actualizaciones de bases de datos con derechos de usuario**.
5. Ingrese las credenciales de la cuenta de un usuario con los permisos necesarios para acceder al origen de actualizaciones.
6. Guarde los cambios.

## Selección del modo de ejecución de la tarea de actualización

Si no es posible ejecutar la tarea de actualización por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha ignorado para que se inicie automáticamente tan pronto como sea posible.

Puede posponer la ejecución de la tarea de actualización después del inicio de la aplicación si seleccionó el modo de ejecución de la tarea de actualización **Mediante programación** y si la hora de inicio de Kaspersky Endpoint Security coincide con la planificación del inicio de la tarea de actualización. La tarea de actualización sólo se puede ejecutar una vez transcurrido el intervalo de tiempo especificado después del inicio de Kaspersky Endpoint Security.

*Para seleccionar el modo de ejecución de la tarea de actualización:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.
2. Seleccione la tarea *Actualización* y haga clic en el **Modo de ejecución: Vínculo de <modo>**.

   Se abren las propiedades de la tarea *Actualización*.
3. Haga clic en el botón **Configurar el modo de actualización de bases de datos**.
4. En la ventana que se abre, seleccione el modo de ejecución de la tarea de actualización:
   - Si desea que Kaspersky Endpoint Security ejecute la tarea de actualización según si existe o no un paquete de actualizaciones disponible en el origen de las actualizaciones, seleccione **Automático**. La frecuencia de las comprobaciones de Kaspersky Endpoint Security para detectar paquetes de actualizaciones aumenta durante las epidemias de virus y disminuye en otros momentos.
   - Si desea iniciar una tarea de actualización manualmente, seleccione **Manual**.
   - Si desea configurar una programación de inicio de la tarea de actualización, seleccione <**Mediante programación**>. Defina la configuración avanzada para iniciar la tarea de actualización:
     - En el campo **Posponer la ejecución después del inicio de la aplicación durante**, especifique el intervalo de tiempo durante el cual se pospone el inicio de la tarea de actualización después del inicio de Kaspersky Endpoint Security.
     - Si desea que Kaspersky Endpoint Security ejecute las tareas de actualización omitidas lo antes posible, seleccione la casilla **Ejecutar tareas omitidas**.
5. Guarde los cambios.

## Adición de un origen de actualizaciones

Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security.

Como origen de actualizaciones, puede utilizar el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky o una carpeta local o de red dispuesta para tal fin.

La lista por defecto de orígenes de actualizaciones incluye a los servidores de actualización de Kaspersky Security Center y de Kaspersky. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las actualizaciones.

Kaspersky Endpoint Security no admite actualizaciones que provengan de servidores HTTPS, a menos que sean servidores de actualización de Kaspersky.

Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno tras otro, comenzando por el principio de la lista, y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible.

*Para agregar un origen de actualizaciones:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.
2. Seleccione la tarea *Actualización* y haga clic en el **Modo de ejecución: Vínculo de <modo>**.

   Se abren las propiedades de la tarea *Actualización*.
3. Haga clic en el botón **Seleccionar orígenes de actualizaciones**.
4. En la ventana, haga clic en el botón **Agregar**.
5. En la ventana que se abre, escriba la dirección del servidor FTP o HTTP, de la carpeta de red o de la carpeta local en la que se encuentre el paquete de actualización.

   Para el origen de actualizaciones se utiliza el siguiente formato de ruta:

   - Si el origen es un servidor FTP o HTTP, escriba la dirección web o la dirección IP.

     Por ejemplo, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

     Si es necesario autenticarse para acceder al servidor FTP, especifique los datos en la dirección siguiendo este formato: `ftp://<nombre de usuario>:<contraseña>@<nodo>:<puerto>`.

   - Si el origen es una carpeta de red, escriba la ruta UNC.

     Por ejemplo, `\\ Server\Share\Update distribution`.

   - Si el origen es una carpeta local o de red, escriba la ruta completa de la carpeta.

     Por ejemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.
6. Haga clic en el botón **Seleccionar**.
7. Configure la prioridad de los orígenes de actualizaciones con los botones **Subir** y **Bajar**.
8. Guarde los cambios.

## Configuración de actualizaciones 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. Habilitar la opción para que el paquete de actualización se copie a una carpeta compartida en uno de los equipos de la red de área local.

2. Configurar el proceso de actualización para que los demás equipos conectados a la LAN de la organización obtengan las bases de datos y los módulos más recientes de la carpeta compartida.

*Para habilitar la copia del paquete de actualización a la carpeta compartida:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.
2. Seleccione la tarea *Actualización* y haga clic en el **Modo de ejecución: Vínculo de <modo>**.

   Se abren las propiedades de la tarea *Actualización*.
3. En el bloque **Distribuyendo actualizaciones**, seleccione la casilla **Copiar las actualizaciones a la siguiente carpeta**.
4. Escriba la ruta UNC de la carpeta compartida (por ejemplo, `\\Server\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 haga clic en el botón **Actualización de bases de datos**.
2. Seleccione la tarea *Actualización* y haga clic en el **Modo de ejecución: Vínculo de <modo>**.

   Se abren las propiedades de la tarea *Actualización*.
3. Haga clic en el botón **Seleccionar orígenes de actualizaciones**.
4. En la ventana, haga clic en el botón **Agregar**.
5. En la ventana que se abre, escriba la ruta de acceso a la carpeta compartida.

   La dirección del origen debe ser la que haya especificado al configurar la copia del paquete de actualización 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 **Subir** y **Bajar**.
8. Guarde los cambios.

## Actualización de los módulos de la aplicación

Las actualizaciones del módulo de la aplicación corrigen errores, mejoran el rendimiento y agregan nuevas características. Cuando esté disponible una nueva actualización del módulo de la aplicación, debe confirmar la instalación de la actualización. Puede confirmar la instalación de una actualización del módulo de la aplicación en la interfaz de la aplicación o en Kaspersky Security Center. Cuando 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 para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final. 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 el equipo.

*Para configurar las actualizaciones de los módulos de la aplicación:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.
2. Seleccione la tarea *Actualización* y haga clic en el **Modo de ejecución: Vínculo de <modo>**.

   Se abren las propiedades de la tarea *Actualización*.
3. En el bloque **Descarga e instalación de actualizaciones de módulos de aplicación**, seleccione la casilla **Descargar actualizaciones de módulos de aplicación**.
4. Seleccione las actualizaciones del módulo de la aplicación que desea instalar.

   - **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.
   - **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. Esta opción está seleccionada por defecto.
5. Guarde los cambios.

## Actualización mediante un servidor proxy

Para que las bases de datos y los módulos de la aplicación más recientes puedan descargarse de un origen de actualizaciones, puede ser necesario especificar los parámetros de conexión de un servidor proxy. Estos parámetros se utilizan para todos los orígenes de actualizaciones. Si el servidor proxy no se necesita para un origen en particular, su uso puede deshabilitarse en las propiedades de la directiva. Kaspersky Endpoint Security también usará el servidor proxy para acceder a Kaspersky Security Network y a los servidores de activación.

*Para conectarse a los orígenes de actualizaciones a través de un servidor proxy:*

1. En la ventana principal de Web Console, haga clic en ⚙.

   Se abre la ventana de propiedades del Servidor de administración.
2. Vaya a la sección **Configuración de acceso a Internet**.
3. 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. Haga clic en el botón **Guardar**.

*Para que el servidor proxy no se utilice 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 correspondiente a los equipos en los que no se usará el servidor proxy.

   Se abre la ventana de propiedades de la directiva.

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

4. Vaya a la sección **Configuración general → Configuración de red**.

5. En la sección **Configuración del servidor proxy**, seleccione **No utilice el servidor proxy**.

6. Haga clic en **Aceptar**.

7. Confirme sus cambios haciendo clic en **Guardar**.

*Para definir la configuración del servidor proxy en la interfaz de la aplicación:*

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

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

3. En el bloque **Servidor proxy**, haga clic en el vínculo **Configuración del servidor proxy**.

4. En la ventana que se abre, seleccione una de las siguientes opciones para determinar la dirección del servidor proxy:

   - **Detección automática de la configuración del servidor proxy**.

     Esta opción está seleccionada por defecto. Kaspersky Endpoint Security utiliza la configuración del servidor proxy que está definida en la configuración del sistema operativo.

   - **Usar configuración del servidor proxy especificada**.

     Si seleccionó esta opción, defina la configuración para conectarse al servidor proxy: dirección y puerto del servidor proxy.

5. Si desea habilitar la autenticación en el servidor proxy, seleccione la casilla **Usar autenticación del servidor proxy** e ingrese las credenciales de su cuenta de usuario.

6. Para que la aplicación no utilice el servidor proxy cuando las bases de datos y los módulos de la aplicación se actualicen desde una carpeta compartida, seleccione la casilla **No usar el servidor proxy para las direcciones locales**.

7. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security utilizará el servidor proxy para descargar actualizaciones de los módulos de la aplicación y la base de datos. Kaspersky Endpoint Security también usará el servidor proxy para acceder a servidores de KSN y a servidores de activación de Kaspersky. Si se requiere autenticación en el servidor proxy, pero las credenciales de la cuenta de usuario no se proporcionaron o son incorrectas, Kaspersky Endpoint Security le solicitará el nombre de usuario y la contraseña.

## Reversión de la última actualización

Después de que se actualicen por primera vez las bases de datos y los módulos de la aplicación, queda disponible la función para volver las bases de datos y los módulos de la aplicación a sus versiones anteriores.

Cada vez que un usuario comienza el proceso de actualización, Kaspersky Endpoint Security crea una copia de seguridad de las bases de datos y los módulos de la aplicación actuales. Esto le permite volver las bases de datos y los módulos de la aplicación a sus versiones anteriores cuando sea necesario. La reversión de la última actualización es útil, por ejemplo, cuando la nueva versión de la base de datos contiene una firma no válida que hace que Kaspersky Endpoint Security bloquee una aplicación segura.

*Para revertir la última actualización:*

1. En la ventana principal de la aplicación haga clic en el botón **Actualización de bases de datos**.
2. En el bloque **Reversión de bases de datos a su versión anterior**, haga clic en el botón **Revertir**.

   Kaspersky Endpoint Security comenzará a revertir la última actualización de las bases de datos. La aplicación mostrará el progreso de la reversión, el tamaño de los archivos descargados y el origen de actualizaciones. Puede hacer clic en el botón  para detener esta tarea en cualquier momento.

*Iniciar o detener una tarea de reversión cuando se muestra la interfaz simplificada de la aplicación:*

1. Haga clic con el botón derecho para mostrar el menú contextual del icono de la aplicación que se encuentra en el área de notificación de la barra de tareas.
2. En la lista desplegable **Tareas** en el menú contextual, realice una de las siguientes opciones:
   - Seleccione una tarea de reversión que no se esté ejecutando para iniciarla.
   - Seleccione una tarea de reversión que se esté ejecutando para detenerla.
   - Seleccione una tarea de reversión que esté en pausa para reanudar o reiniciar su ejecución.

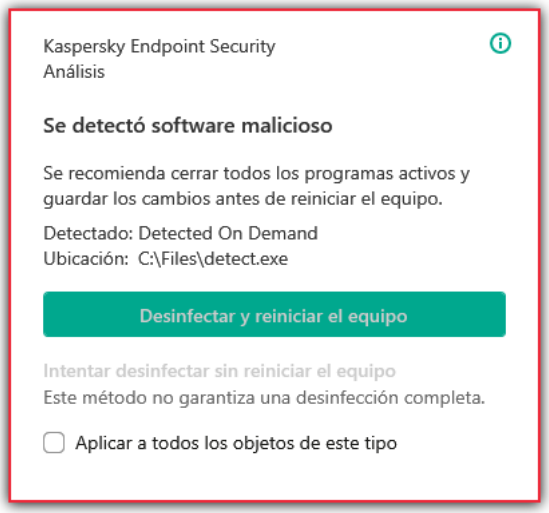
# Trabajar con amenazas activas

Kaspersky Endpoint Security registra información sobre los archivos que no procesó por algún motivo. Esta información se registra en forma de eventos en la lista de amenazas activas. 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 tecnología de Desinfección avanzada en los ajustes de la tarea *Análisis antivirus* y en la configuración de la aplicación.

## Desinfección de amenazas activas en estaciones de trabajo

Para trabajar con amenazas activas en estaciones de trabajo, habilite la tecnología de Desinfección avanzada en la configuración de la aplicación. A continuación, configure la experiencia del usuario en las propiedades de la tarea *Análisis antivirus*. En las propiedades de la tarea, encontrará la casilla **Habilitar la desinfección avanzada inmediata**. Si la casilla está marcada, Kaspersky Endpoint Security realizará la desinfección sin notificar al usuario. Cuando finalice la desinfección, se reiniciará el equipo. Si la casilla no está marcada, Kaspersky Endpoint Security mostrará una notificación acerca de las amenazas activas (consulte la imagen a continuación). No puede cerrar esta notificación sin procesar el archivo.

La Desinfección avanzada durante una tarea de análisis antivirus en un equipo solo se realiza si la función Desinfección avanzada está habilitada en las propiedades de la directiva que se aplica al equipo.




Notificación sobre amenazas activas

## Desinfección de amenazas activas en servidores

Para trabajar con amenazas activas en servidores, debe hacer lo siguiente:

- habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación;
- habilitar la Desinfección avanzada inmediata en las propiedades de la tarea *Análisis antivirus*.

Si Kaspersky Endpoint Security está instalado en un equipo con Windows for Servers, Kaspersky Endpoint Security no mostrará la notificación. Por lo tanto, el usuario no podrá seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación y habilitar la Desinfección avanzada inmediata en las propiedades de la *tarea Análisis antivirus*. A continuación, debe iniciar la tarea *Análisis antivirus*.

## Procesamiento de amenazas activas

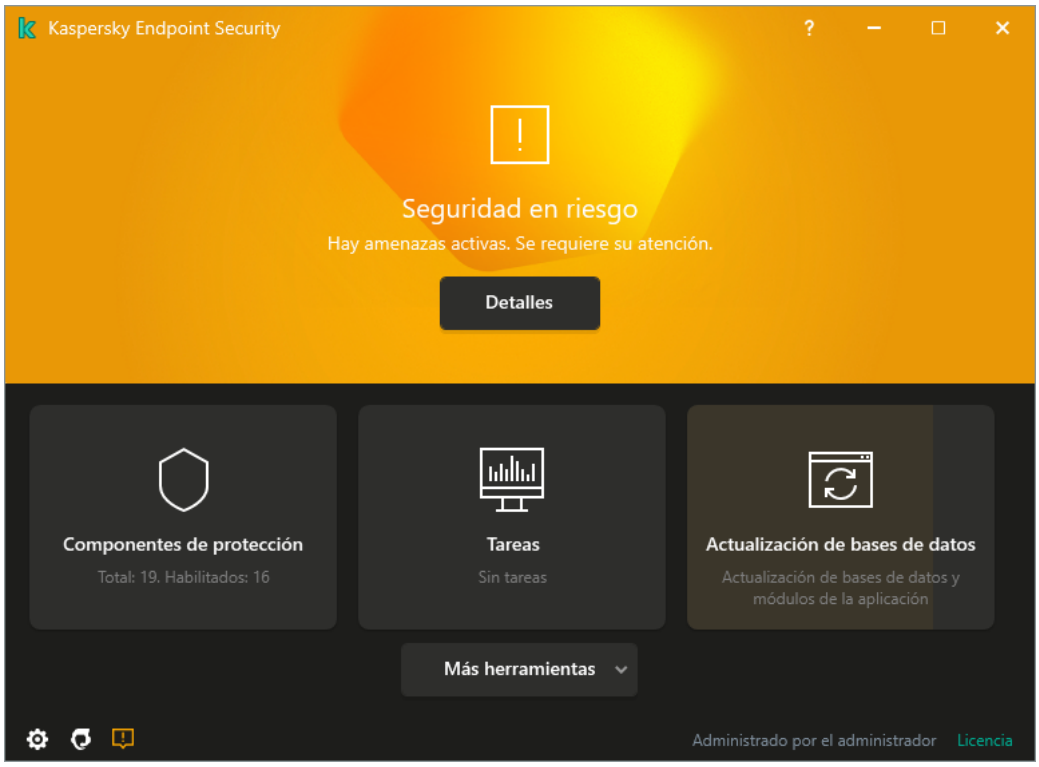
Un archivo infectado se considera *procesado* si Kaspersky Endpoint Security realiza una de las siguientes acciones sobre él, de acuerdo con la configuración de la aplicación especificada, mientras analiza el equipo en busca de virus y otras amenazas:

- Desinfectar.
- Eliminar.
- Eliminar si falla la desinfección.

Kaspersky Endpoint Security mueve el archivo a la lista de amenazas activas si, por algún motivo, Kaspersky Endpoint Security no puede realizar una acción en este archivo de conformidad con los ajustes especificados de la aplicación cuando analizar el equipo en busca de virus y otras amenazas.

Esta situación es posible en los siguientes casos:

- El archivo analizado no está disponible (por ejemplo, está ubicado en una unidad de red o en un disco extraíble sin permiso de escritura).
- La acción seleccionada en la sección **Acción al detectar una amenaza** para las tareas de análisis es **Informar**, y el usuario selecciona la acción **Omitir** cuando se muestra una notificación sobre el archivo infectado.




Ventana principal de la aplicación cuando se detecta una amenaza

*Para procesar las amenazas activas, realice lo siguiente:*

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

   Se abre la lista de amenazas activas.

2. Seleccione el objeto que desee procesar.
3. Decida cómo desea manejar la amenaza:

- **Resolver**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.

- **Ignorar**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina la entrada de la lista de amenazas activas. Si no existen amenazas activas restantes en la lista, el estado del equipo cambiará a *Sin inconvenientes*. Si se detecta el objeto nuevamente, Kaspersky Endpoint Security agregará una nueva entrada a la lista de amenazas activas.

- **Abrir carpeta contenedora**. Si se selecciona esta opción, Kaspersky Endpoint Security abre la carpeta que contiene el objeto en el Administrador de archivos. Luego, puede eliminar manualmente el objeto o moverlo a una carpeta fuera del alcance de la protección.

- **Más información**. Si se selecciona esta opción, Kaspersky Endpoint Security abre el sitio web de la Enciclopedia de virus de Kaspersky.

## Protección contra amenazas de archivos

El componente Protección contra amenazas de archivos le permite evitar la infección del sistema de archivos del equipo. De manera predeterminada, el componente se mantiene cargado en la RAM del equipo. Protección contra archivos peligrosos analiza los archivos de todas las unidades del equipo, incluidas las que se conectan al mismo. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

El componente analiza los archivos a los que acceden tanto el usuario como las aplicaciones. Cuando se detecta un archivo malintencionado, Kaspersky Endpoint Security bloquea la operación del archivo. El archivo entonces se elimina o se desinfecta, dependiendo de cómo se ha configurado el componente.

Si intenta acceder a un archivo cuyo contenido esté almacenado en la nube de OneDrive, Kaspersky Endpoint Security descargará el contenido y lo analizará.

## Habilitación y deshabilitación de la Protección contra amenazas de archivos

De manera predeterminada, el componente Protección contra amenazas de archivos está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para Protección contra archivos peligrosos, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones guardadas en la aplicación se llaman *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que el nivel de seguridad **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky (consulte la tabla a continuación). Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración del nivel de seguridad recomendada.

*Para habilitar o deshabilitar el componente Protección contra archivos peligrosos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Utilice el interruptor **Protección contra archivos peligrosos** para habilitar o deshabilitar el componente.
4. Si habilitó el componente, realice una de estas acciones en la sección **Nivel de seguridad**:
   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
     - **Alto**. Si se selecciona este nivel de seguridad de archivos, el componente Protección contra amenazas de archivos realiza el control más estricto de todos los archivos abiertos, guardados e iniciados. El componente Protección contra amenazas de archivos analiza todos los tipos de archivo en todos los discos duros, unidades extraíbles y unidades de red del equipo. También analiza archivos de almacenamiento, paquetes de instalación y objetos OLE integrados.
     - **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección contra amenazas de archivos solo analiza los formatos de archivo especificados en todos los discos duros, unidades extraíbles y unidades de red del equipo, y en los objetos de OLE

incorporados. El componente Protección contra amenazas de archivos no analiza paquetes de instalación ni archivos. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.

- **Bajo**. La configuración de este nivel de seguridad de archivos garantiza la máxima velocidad de análisis. El componente Protección contra amenazas de archivos analiza solamente los archivos con las extensiones especificadas en todos los discos duros, unidades extraíbles y unidades de red del equipo. El componente Protección contra amenazas de archivos no analiza archivos compuestos.

- Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y configure los ajustes del componente.

  Para restablecer los valores de los niveles de seguridad prestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado** en la parte superior de la ventana.

5. Guarde los cambios.

Configuración de Protección contra archivos peligrosos recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

| Parámetro | Valor | Descripción |
|---|---|---|
| **Tipos de archivos** | **Analizar archivos por formato** | Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares. |
| **Análisis heurístico** | **Análisis superficial** | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br>Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Analizar solo archivos nuevos y modificados** | **Habilitado** | Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como compuestos. |
| **Tecnología iSwift** | **Habilitado** | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS. |
| **Tecnología iChecker** | **Habilitado** | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la |

| | | |
|---|---|---|
| | | aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |
| **Analizar archivos de Microsoft Office** | **Habilitado** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **Modo de análisis** | **Modo inteligente** | En este modo, Protección contra archivos peligrosos analiza un objeto en función de las operaciones realizadas sobre ese objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo. |
| **Acción al detectar una amenaza** | **Desinfectar; si no es posible, eliminar** | Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos. |

## Suspensión automática de la Protección contra amenazas de archivos

Puede configurar la suspensión automática de la Protección contra amenazas de archivos en una hora especificada o al trabajar con aplicaciones específicas.

La Protección contra amenazas de archivos solo debe pausarse como último recurso cuando entra en conflicto con algunas aplicaciones. Si surge algún conflicto mientras se ejecuta un componente, se recomienda que se comunique con el Servicio de soporte técnico de Kaspersky. Los expertos de Soporte lo ayudarán a configurar el componente Protección contra amenazas de archivos para que se ejecute simultáneamente con otras aplicaciones en su equipo.

*Para configurar la suspensión automática de la Protección contra amenazas de archivos, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Pausar Protección contra archivos peligrosos**, haga clic en el vínculo **Pausar Protección contra archivos peligrosos**.
5. En la ventana que se abre, defina la configuración para pausar Protección contra archivos peligrosos:
   a. Configure una programación para pausar automáticamente Protección contra archivos peligrosos.
   b. Cree una lista de aplicaciones cuyo funcionamiento debería provocar que Protección contra archivos peligrosos detenga sus actividades.
6. Guarde los cambios.

## Cambio de la acción tomada respecto de archivos infectados por el componente Protección contra amenazas de archivos

Por defecto, el componente Protección contra amenazas de archivos automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección arroja un error, el componente Protección contra amenazas de archivos elimina estos archivos.

*Para cambiar la acción tomada respecto de archivos infectados por el componente Protección contra amenazas de archivos, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. En la sección **Acción al detectar una amenaza**, seleccione la opción que desee:
   - **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.
   - **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.
   - **Bloquear**. Si esta opción está seleccionada, el componente Protección contra amenazas de archivos bloquea automáticamente 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 si se puede desinfectar en el futuro.
4. Guarde los cambios.

## Formación del alcance de la protección del componente Protección contra amenazas de archivos

El alcance de la protección se refiere a los objetos que el componente analiza cuando está habilitado. Los alcances de la protección de diferentes componentes tienen diferentes propiedades. La ubicación y el tipo de archivos que se analizarán son propiedades del alcance de la protección del componente Protección contra amenazas de archivos. De forma predeterminada, el componente Protección contra amenazas de archivos analiza solo los archivos potencialmente infectables que se ejecutan desde discos duros, unidades extraíbles y unidades de red.

Cuando seleccione el tipo de archivos por analizar, tenga presenta la siguiente información:

1. La probabilidad de que ciertos tipos de archivos (por ejemplo, los de formato TXT) contengan código malintencionado que pueda activarse es baja. Existen, por otro lado, formatos de archivo que sí contienen código ejecutable (.exe, .dll y otros). Junto con estos, existen ciertos tipos de archivos que pueden contener

código ejecutable aunque no estén principalmente diseñados para ello (por ejemplo, los archivos de formato DOC). El riesgo de que el código malicioso ingrese en estos archivos y se active es alto.

2. Un intruso podría enviarle un archivo de extensión .txt que sea, en realidad, un ejecutable peligroso (un virus u otro tipo de aplicación malintencionada) al que se le ha cambiado el nombre. Si selecciona el análisis de archivos por extensión, la aplicación omite este archivo durante el análisis. Si se selecciona el análisis de archivos por formato, Kaspersky Endpoint Security analiza el encabezado del archivo independientemente de la extensión. Si se determina que el archivo es de un formato ejecutable (por ejemplo, EXE), se lo somete a análisis.

*Para crear el alcance de la protección:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Tipos de archivos**, especifique el tipo de archivos que quiera que analice el componente Protección contra amenazas de archivos:
   - **Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones).
   - **Archivos analizados según su formato**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.
   - **Archivos analizados según su extensión**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión.
5. Haga clic en el vínculo **Editar el alcance de la protección**.
6. En la ventana que se abre, seleccione los objetos que desea agregar al alcance de la protección o excluir de él.

   No puede quitar ni modificar objetos que estén incluidos en el alcance de la protección predeterminado.

7. Si quiere agregar un objeto nuevo al alcance de la protección:
   a. Haga clic en el botón **Agregar**.
      Se abre el árbol de carpetas.
   b. Seleccione el objeto y haga clic en **Seleccionar**.

   Puede excluir un objeto de los análisis sin eliminarlo de la lista de objetos en el alcance del análisis. Para hacerlo, desactive la casilla ubicada junto al objeto.
8. Guarde los cambios.

## Uso de métodos de análisis

Kaspersky Endpoint Security usa una técnica de análisis llamada Aprendizaje automático y análisis de firmas. Durante el análisis de firmas, Kaspersky Endpoint Security compara el objeto detectado con los registros en su base de datos. Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado.

Para aumentar la efectividad de la protección, puede utilizar el análisis heurístico. Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico.

*Para configurar el uso del análisis heurístico en el funcionamiento del componente Protección contra amenazas de archivos, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Haga clic en el botón **Configuración avanzada**.
4. Si desea que la aplicación utilice el análisis heurístico para la protección contra archivos peligrosos, seleccione la casilla **Análisis heurístico** en el bloque **Métodos de análisis**. A continuación, utilice el control deslizante para definir el nivel de análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.
5. Guarde los cambios.

## Utilización de tecnologías de análisis en la operación del componente Protección contra amenazas de archivos

*Para configurar el uso de tecnologías de análisis en el funcionamiento del componente Protección contra amenazas de archivos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En el bloque **Tecnologías de análisis**, seleccione las casillas junto a los nombres de las tecnologías que desea utilizar para la protección contra archivos peligrosos:
   - **Tecnología iSwift**. Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS.

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

5. Guarde los cambios.

## Optimización del análisis de archivos

Puede optimizar el análisis de archivos realizado por el componente Protección contra amenazas de archivos reduciendo la duración del análisis y aumentando la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede lograr analizando solamente los archivos nuevos y aquellos que se han modificado desde el análisis anterior. Este modo se aplica tanto a archivos simples como compuestos.

También puede habilitar el uso de las tecnologías iChecker y iSwift, que optimizan la velocidad del análisis de archivos al excluir los archivos que no se han modificado desde el análisis más reciente.

*Para optimizar el análisis de archivos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Optimización del análisis**, seleccione la casilla **Analizar solo archivos nuevos y modificados**.
5. Guarde los cambios.

## Análisis de archivos compuestos

Una técnica común para ocultar virus u otro malware es implantarlo en archivos compuestos, como archivos de almacenamiento o bases de datos. Para detectar virus u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

El método utilizado para procesar un archivo compuesto infectado (desinfección o eliminación) depende del tipo de archivo.

El componente Protección contra amenazas de archivos desinfecta archivos compuestos con formato RAR, ARJ, ZIP, CAB y LHA, y elimina archivos en todos los formatos restantes (excepto bases de datos de correo).

*Para configurar el análisis de archivos compuestos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
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, paquetes de instalación o archivos en formatos de Office.
5. Si el análisis de solo archivos nuevos y modificados está desactivado, defina la configuración para analizar cada tipo de archivo compuesto: analice todos los archivos de este tipo o solo los archivos nuevos.

   Si está habilitado el análisis de archivos nuevos y modificados, Kaspersky Endpoint Security analiza solo archivos nuevos y modificados de todos los tipos de archivos compuestos.
6. Defina la configuración avanzada para analizar archivos compuestos.

   - **No desempaquetar archivos compuestos de gran tamaño**.

     Si esta casilla está seleccionada, Kaspersky Endpoint Security no analiza los archivos compuestos si su tamaño excede el valor.

     Si esta casilla está desactivada, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.

     > Kaspersky Endpoint Security analiza los archivos de gran tamaño que se extraen de archivos comprimidos, independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

   - **Descomprimir archivos compuestos en segundo plano**.

     Si activa esta casilla, Kaspersky Endpoint Security permitirá acceder a los archivos compuestos que superen el tamaño especificado antes de que se los haya analizado. En este caso, Kaspersky Endpoint Security descomprimirá y analizará los archivos compuestos en segundo plano.

     Kaspersky Endpoint Security proporciona acceso a los archivos compuestos que son más pequeños que este valor solo después de descomprimir y analizar estos archivos.

     Si no activa esta casilla, Kaspersky Endpoint Security no permitirá acceder a ningún archivo compuesto, independientemente de su tamaño, hasta que se lo haya descomprimido y analizado.
7. Guarde los cambios.

## Modificación del modo de análisis

El *Modo de análisis* hace referencia a la condición que desencadena el análisis del archivo del componente Protección contra amenazas de archivos. Por defecto, Kaspersky Endpoint Security analiza los archivos en el modo inteligente. En este modo de análisis de archivos, el componente Protección contra amenazas de archivos decide si analiza o no los archivos después de analizar las operaciones realizadas con el archivo por el usuario, por una aplicación en nombre del usuario (en la cuenta que se usó para iniciar sesión o en otra cuenta de usuario) o por el sistema operativo. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office Word la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo.

*Para modificar el modo de análisis de archivos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra archivos peligrosos**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Modo de análisis**, seleccione el modo que desee:
   - **Modo inteligente**. En este modo, Protección contra archivos peligrosos analiza un objeto en función de las operaciones realizadas sobre ese objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo.
   - **Ante operaciones de acceso y modificación**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos siempre que haya un intento de abrirlos o modificarlos.
   - **Ante operaciones de acceso**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos solo después de un intento de abrirlos.
   - **Ante operaciones de ejecución**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos después de un intento de ejecutarlos.
5. Guarde los cambios.

## Protección contra amenazas web

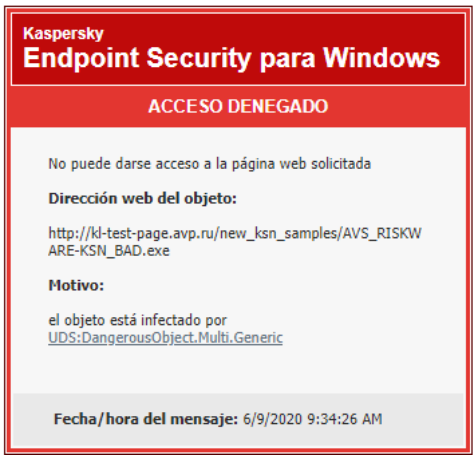
Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El componente Protección contra amenazas web está diseñado para bloquear sitios web maliciosos y fraudulentos e impedir la descarga de archivos dañinos de Internet. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Kaspersky Endpoint Security tiene la capacidad de analizar tráfico HTTP, HTTPS y FTP. La aplicación analiza tanto direcciones URL como direcciones IP. Puede permitir que Kaspersky Endpoint Security vigile todos los puertos o puede seleccionar los puertos específicos que le interese controlar.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario habilitar el análisis de conexiones cifradas.

Cuando un usuario intente abrir un sitio web malicioso o fraudulento, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia (vea la siguiente imagen).




Mensaje cuando se bloquea el acceso a un sitio web

## Habilitación y deshabilitación de la Protección contra amenazas web

De manera predeterminada, el componente Protección contra amenazas web está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para la Protección contra amenazas web, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones guardadas en la aplicación se llaman *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que el nivel de seguridad de tráfico web **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky (vea la tabla a continuación). Puede seleccionar uno de los niveles preinstalados de seguridad para el tráfico web que se recibe o se transmite mediante los protocolos HTTP y FTP, o configurar un nivel de seguridad personalizado para el tráfico web. Si modifica la configuración del nivel de seguridad del tráfico web, siempre puede volver a la configuración recomendada del nivel de seguridad del tráfico web.

*Para habilitar o deshabilitar el componente Protección contra amenazas web:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra amenazas web**.
3. Utilice el interruptor **Protección contra amenazas web** para habilitar o deshabilitar el componente.
4. Si habilitó el componente, realice una de estas acciones en la sección **Nivel de seguridad**:
   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
     - **Alto**. El nivel de seguridad con el cual el componente Protección contra amenazas web realiza el análisis máximo del tráfico web que recibe el equipo a través de los protocolos HTTP y FTP. El componente Protección contra amenazas web analiza en detalle todos los objetos de tráfico web mediante el uso de todas las bases de datos de la aplicación y realiza el análisis heurístico más avanzado posible.
     - **Recomendado**. Este es el nivel de seguridad que proporciona el equilibrio óptimo entre el rendimiento de Kaspersky Endpoint Security y la seguridad del tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de **análisis medio**. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.
     - **Bajo**. La configuración de este nivel de seguridad de tráfico web asegura la máxima velocidad de análisis de tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de **Análisis superficial**.

- Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y configure los ajustes del componente.

  Para restablecer los valores de los niveles de seguridad prestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado** en la parte superior de la ventana.

5. Guarde los cambios.

Configuración de Protección contra amenazas web recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

| Parámetro | Valor | Descripción |
|---|---|---|
| **Comprobar si los vínculos están incluidos en la base de datos de vínculos malintencionados** | **Habilitado** | Analizar los vínculos para determinar si están incluidos en la base de datos de direcciones web malintencionadas le permite rastrear sitios web que estén en la lista de bloqueo. Kaspersky realiza el mantenimiento de la base de datos de direcciones web malintencionadas, la que se incluye en el paquete de instalación de la aplicación y se actualiza durante las actualizaciones de las bases de datos de Kaspersky Endpoint Security. |
| **Comprobar si la URL está en la base de datos de direcciones URL fraudulentas** | **Habilitado** | La base de datos de direcciones web fraudulentas incluye las direcciones web de los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases de datos de Kaspersky Endpoint Security. |
| **Usar análisis heurístico** (Protección contra amenazas web) | **Análisis medio** | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br>Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Usar análisis heurístico** (Antiphishing) | **Habilitado** | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. |
| **Acción al detectar una amenaza** | **Bloquear descarga** | Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador. |

## Modificación de la acción que se llevará a cabo en objetos maliciosos del tráfico web

Por defecto, al detectar un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra una notificación sobre la acción.

*Para modificar la acción que se llevará a cabo en objetos malintencionados del tráfico web:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección básica contra amenazas → Protección contra amenazas web**.
3. En la sección **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos malintencionados del tráfico web:
   - **Bloquear descarga**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.
   - **Informar**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web permite que el objeto se descargue al equipo, pero agrega información sobre el mismo a la lista de amenazas activas.
4. Guarde los cambios.

## Análisis de URL con las bases de datos de direcciones web malintencionadas y de phishing

El análisis de vínculos para saber si están incluidos en la lista de direcciones web de phishing permite evitar *ataques de phishing*. Un ataque de phishing puede imitar, por ejemplo, un mensaje de correo electrónico supuestamente enviado por su banco, con un vínculo al sitio web oficial del banco. Cuando hace clic en el vínculo, se abre una copia exacta del sitio web del banco e, incluso, puede ver la dirección web real en el navegador, a pesar de que se trata de una imitación. A partir de ese momento, se hace un seguimiento de todas sus acciones dentro del sitio y pueden ser usadas para robar su dinero.

Teniendo en cuenta que los vínculos a los sitios web de phishing no solo pueden recibirse en mensajes de correo electrónico, sino también por otros medios, como mensajes ICQ, el componente Protección contra amenazas web supervisa los intentos de acceder a un sitio web de phishing en el nivel de análisis del tráfico web y bloquea el acceso a dichos sitios. Las listas de direcciones web de phishing se incluyen en el kit de distribución de Kaspersky Endpoint Security.

*Para configurar el componente Protección contra amenazas web para comprobar vínculos comparándolos con las bases de datos de direcciones web malintencionadas y de phishing:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección básica contra amenazas → Protección contra amenazas web**.
3. Haga clic en el botón **Configuración avanzada**.
4. Haga lo siguiente:
   - Si desea que el componente Protección contra amenazas web compruebe los vínculos comparándolos con las bases de datos de direcciones web malintencionadas, en la sección **Métodos de análisis**, seleccione la

casilla **Comprobar si la URL está en la base de datos de direcciones URL malintencionadas**. Analizar los vínculos para determinar si están incluidos en la base de datos de direcciones web malintencionadas le permite rastrear sitios web que estén en la lista de bloqueo. Kaspersky realiza el mantenimiento de la base de datos de direcciones web malintencionadas, la que se incluye en el paquete de instalación de la aplicación y se actualiza durante las actualizaciones de las bases de datos de Kaspersky Endpoint Security.

Kaspersky Endpoint analiza todos los vínculos para determinar si están incluidos en bases de datos de direcciones web malintencionadas. La configuración de análisis de conexión segura de la aplicación no afecta la funcionalidad de análisis de vínculos. En otras palabras, si los análisis de conexiones cifradas están deshabilitados, Kaspersky Endpoint Security verifica los vínculos con bases de datos de direcciones web malintencionadas, incluso si el tráfico de red se transmite a través de una conexión cifrada.

- Si desea que el componente Protección contra amenazas web compruebe los vínculos con las bases de datos de direcciones web de phishing, seleccione la casilla **Comprobar si la URL está en la base de datos de direcciones URL fraudulentas** en el bloque **Antiphishing**. La base de datos de direcciones web fraudulentas incluye las direcciones web de los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases de datos de Kaspersky Endpoint Security.

  También puede comprobar vínculos comparándolos con las bases de datos de reputación de Kaspersky Security Network.

5. Guarde los cambios.

## Utilización del análisis heurístico en la operación del componente Protección contra amenazas web

Para aumentar la efectividad de la protección, puede utilizar el análisis heurístico. Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones del sistema operativo. El análisis heurístico puede detectar amenazas sobre las cuales no existen registros en las bases de datos de Kaspersky Endpoint Security.

*Para configurar el uso del análisis heurístico:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra 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 otro malware. A continuación, utilice el control deslizante para definir el nivel de análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.
5. En el bloque **Antiphishing**, seleccione la casilla **Usar análisis heurístico** si desea que la aplicación utilice el análisis heurístico al analizar páginas web en busca de vínculos fraudulentos.

6. Guarde los cambios.

## Creación de la lista de direcciones web de confianza

Puede crear una lista de direcciones URL cuyo contenido considera confiable. El componente Protección contra amenazas web no analiza la información de direcciones web de confianza en busca de virus u otras amenazas. Esta opción es útil, por ejemplo, cuando el componente Protección contra amenazas web interfiere en la descarga de un archivo de un sitio web conocido.

Una dirección URL puede ser la dirección de una página web específica o la dirección de un sitio web.

*Para crear una lista de direcciones web de confianza:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección contra amenazas web**.
3. Haga clic en el botón **Configuración avanzada**.
4. Seleccione la casilla **No analizar el tráfico web de las direcciones web de confianza**.

   Si la casilla está seleccionada, el componente Protección contra amenazas web no analiza el contenido de las páginas o los sitios web cuyas direcciones están incluidas en la lista de direcciones web de confianza. Puede agregar a esta lista tanto direcciones específicas como máscaras de páginas o sitios web.
5. Cree una lista de direcciones URL o páginas web cuyo contenido considera confiable.
6. Guarde los cambios.

## Exportar e importar la lista de direcciones web de confianza

Puede exportar la lista de direcciones web de confianza a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de direcciones web del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de direcciones web de confianza o para migrar la lista a otro servidor.

Cómo exportar e importar una lista de direcciones web de confianza a la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección básica contra amenazas → Protección contra amenazas web**.
6. 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 vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de direcciones web de confianza exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de direcciones web de confianza completa al archivo XML.
9. Para importar la lista de direcciones web de confianza:
   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de direcciones web de confianza.

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

      Cuando ya exista una lista de direcciones web de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
10. Guarde los cambios.

[Cómo exportar e importar una lista de direcciones web de confianza a Web Console y Cloud Console]

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desee exportar o importar una lista de direcciones web de confianza.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Protección básica contra amenazas** → **Protección contra amenazas web**.
5. Para exportar la lista de exclusiones al bloque **Direcciones web de confianza**:
   a. Seleccione las direcciones web de confianza que desea exportar.
   b. Haga clic en el vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de direcciones web de confianza exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de direcciones web de confianza completa al archivo XML.
6. Para importar una lista de exclusiones al bloque **Direcciones web de confianza**:
   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de direcciones web de confianza.
   b. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de direcciones web de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
7. Guarde los cambios.

## Protección contra amenazas de correo

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El componente Protección contra amenazas de correo analiza los archivos adjuntos a los mensajes de correo entrantes y salientes para detectar virus y otras amenazas. También analiza los mensajes en busca de vínculos maliciosos o fraudulentos. De manera predeterminada, el componente se mantiene cargado en la RAM del equipo y analiza todos los mensajes enviados o recibidos mediante los protocolos POP3, SMTP, IMAP y NNTP, o a través del cliente de correo Microsoft Office Outlook (MAPI). Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Si utiliza un navegador para acceder a su cliente de correo electrónico, el componente Protección contra amenazas de correo no analizará sus mensajes.

Cuando detecta un mensaje con un archivo adjunto malicioso, Kaspersky Endpoint Security cambia el asunto del mensaje de la siguiente manera: `[Mensaje infectado] <asunto del mensaje>` o `[Se eliminó un objeto infectado] <asunto del mensaje>`.

Este componente interactúa con clientes de correo instalados en el equipo. En el caso de Microsoft Office Outlook, existe una extensión con parámetros adicionales. La extensión de la Protección contra amenazas de correo se incorpora al cliente de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

## Habilitación y deshabilitación de la Protección contra amenazas de correo

De manera predeterminada, el componente Protección contra amenazas de correo está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Para Protección contra amenazas de correo, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones guardadas en la aplicación se llaman *niveles de seguridad*: **Alto**, **Recomendado**, **Bajo**. Se considera que el nivel de seguridad de correo **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky (vea la tabla a continuación). Puede seleccionar uno de los niveles preinstalados de seguridad del correo o configurar un nivel de seguridad personalizado del correo. Si ha cambiado la configuración del nivel de seguridad del correo, siempre puede volver a la configuración recomendada del nivel de seguridad del correo.

*Para habilitar o deshabilitar el componente Protección contra amenazas de correo:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **protección básica contra amenazas** → **Protección contra amenazas de correo**.
3. Utilice el interruptor **Protección contra amenazas de correo** para habilitar o deshabilitar el componente.
4. Si habilitó el componente, realice una de estas acciones en la sección **Nivel de seguridad**:
   - Si desea aplicar uno de los niveles de seguridad predeterminados, selecciónelo con el control deslizante:
     - **Alto**. Cuando este nivel de seguridad del correo electrónico se selecciona, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico más detalladamente. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico profundo. El nivel de seguridad de correo **Alta** se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo gratuito desde una red doméstica sin protección centralizada del correo.
     - **Recomendado**. Este es el nivel de seguridad del correo electrónico que proporciona el equilibrio óptimo entre el rendimiento de Kaspersky Endpoint Security y la seguridad del correo electrónico. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad del tráfico de correo. Los valores de configuración para el nivel de seguridad recomendado se proporcionan en la siguiente tabla.
     - **Bajo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo solo analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza los archivos adjuntos a los mensajes de correo electrónico. En este nivel de

seguridad de correo electrónico, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico con una velocidad máxima y utiliza lo mínimo de los recursos del sistema operativo. Se recomienda utilizar el nivel de seguridad de correo **Bajo** en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una red LAN empresarial con protección de correo electrónico centralizada.

- Si desea definir un nivel de seguridad personalizado, haga clic en el botón **Configuración avanzada** y configure los ajustes del componente.

  Para restablecer los valores de los niveles de seguridad prestablecidos, haga clic en el botón **Restablecer el nivel de seguridad recomendado** en la parte superior de la ventana.

5. Guarde los cambios.

Configuración de Protección contra amenazas de correo recomendada por los expertos de Kaspersky (nivel de seguridad recomendado)

| Parámetro | Valor | Descripción |
|---|---|---|
| **Alcance de la protección** | **Mensajes entrantes y salientes** | El *Alcance de la protección* incluye objetos que el componente comprueba cuando se ejecuta: **Mensajes entrantes y salientes** o **Solo mensajes entrantes**.<br>Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar el envío de archivos infectados. También puede activar el análisis de mensajes salientes si desea evitar el envío de archivos en formatos particulares, como archivos de audio y video, por ejemplo. |
| **Conectar extensión de Microsoft Outlook** | **Habilitado** | 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.<br>Si planea analizar el correo con la extensión para Microsoft Outlook, recomendamos que use 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. |
| **Analizar archivos de almacenamiento adjuntos** | **Habilitado** | Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE. |
| **Analizar los formatos adjuntos de Office** | **Habilitado** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **Filtrado de documentos adjuntos** | **Cambiar el nombre de los archivos adjuntos de los tipos seleccionados** | Si selecciona esta opción, Protección contra amenazas de correo reemplazará el último carácter de extensión encontrado en los archivos adjuntos de los tipos especificados con el carácter de guion bajo (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo. |
| **Análisis heurístico** | **Análisis medio** | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido. |

| | | |
|---|---|---|
| | | Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Acción al detectar una amenaza** | **Desinfectar; si no es posible, eliminar** | Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security lo elimina. El asunto del mensaje se cambia a `[Se eliminó un objeto infectado] <asunto del mensaje>` para informarle al usuario sobre la acción realizada. |

## Modificación de la acción que se llevará a cabo en mensajes de correo electrónico infectados

Por defecto, el componente Protección contra amenazas de correo intenta desinfectar automáticamente todos los mensajes de correo infectados que se detectan. Si la desinfección produce un error, el componente Protección contra amenazas de correo elimina los mensajes de correo electrónico infectados.

*Para modificar la acción que se llevará a cabo en mensajes de correo infectados:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **protección básica contra amenazas** → **Protección contra amenazas de correo**.
3. En la sección **Acción al detectar una amenaza**, seleccione la acción que realizará Kaspersky Endpoint Security cuando se detecte un mensaje infectado:
   - **Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security lo elimina. El asunto del mensaje se cambia a `[Se eliminó un objeto infectado] <asunto del mensaje>` para informarle al usuario sobre la acción realizada.
   - **Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security agrega una advertencia al asunto del mensaje: `[Mensaje infectado] <asunto del mensaje>`. El usuario puede acceder al mensaje, con su archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.
   - **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, Kaspersky Endpoint Security agrega una advertencia al asunto del mensaje: `[Mensaje infectado] <asunto del mensaje>`. El usuario puede acceder al mensaje, con su archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, Kaspersky Endpoint Security bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.

4. Guarde los cambios.

## Formación del alcance de protección del componente Protección contra amenazas de correo

El *Alcance de la protección* hace referencia a los objetos que son analizados por el componente cuando está activo. Los alcances de la protección de diferentes componentes tienen diferentes propiedades. Las propiedades del alcance de la protección del componente Protección contra amenazas de correo incluyen la configuración para integrar el componente Protección contra amenazas de correo en clientes de correo y el tipo de mensajes de correo electrónico y los protocolos de correo electrónico cuyo tráfico es analizado por el componente Protección contra amenazas de correo. De forma predeterminada, Kaspersky Endpoint Security analiza tanto mensajes de correo electrónico como tráfico (entrantes y salientes) de los protocolos POP3, SMTP, NNTP e IMAP, y está integrado en el cliente de correo Microsoft Office Outlook.

*Para formar el alcance de protección del componente Protección contra amenazas de correo, realice lo siguiente:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **protección básica contra amenazas** → **Protección contra amenazas de correo**.

3. Haga clic en el botón **Configuración avanzada**.

4. En el bloque **Alcance de la protección**, seleccione los mensajes que desea analizar:

   - **Mensajes entrantes y salientes**.
   - **Solo mensajes entrantes**.

   Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar el envío de archivos infectados. También puede activar el análisis de mensajes salientes si desea evitar el envío de archivos en formatos particulares, como archivos de audio y video, por ejemplo.

   Si opta por analizar solo mensajes entrantes, le recomendamos que realice un análisis único de todos los mensajes salientes porque existe la posibilidad de que su equipo tenga gusanos de correo electrónico que se estén diseminando por correo electrónico. Esto ayuda a evitar problemas ocasionados por el envío masivo no controlado de mensajes infectados desde su equipo.

5. En la sección **Conectividad**, realice lo siguiente:

   - Si desea que el componente Protección contra amenazas de correo analice los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen al equipo del usuario, seleccione la casilla **Analizar tráfico POP3/SMTP/NNTP/IMAP**.

     Si no desea que el componente Protección contra amenazas de correo analice los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen al equipo del usuario, desmarque la casilla **Analizar tráfico POP3/SMTP/NNTP/IMAP**. En este caso, los mensajes son analizados por la extensión Protección contra amenazas de correo incorporada al cliente de correo de Microsoft Office Outlook después de que llegan al equipo del usuario si se selecciona la casilla **Conectar extensión de Microsoft Outlook**.

Si usa un cliente de correo que no sea Microsoft Office Outlook, el componente Protección contra amenazas de correo no analiza los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP cuando se desmarca la casilla **Analizar tráfico POP3/SMTP/NNTP/IMAP**.

- Si desea permitir el acceso a la configuración del componente Protección contra amenazas de correo desde Microsoft Office Outlook y habilitar el análisis de los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que llegan al equipo utilizando la extensión incorporada a Microsoft Office Outlook, seleccione la casilla **Conectar extensión de Microsoft Outlook**.

  Si desea bloquear el acceso a la configuración del componente Protección contra amenazas de correo desde Microsoft Office Outlook y deshabilitar el análisis de los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que llegan al equipo utilizando la extensión incorporada a Microsoft Office Outlook, desmarque la casilla **Conectar extensión de Microsoft Outlook**.

  La extensión de la Protección contra amenazas de correo se incorpora al cliente de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

6. Guarde los cambios.

## Análisis de archivos compuestos adjuntos a mensajes de correo electrónico

Puede habilitar o deshabilitar el análisis de adjuntos a mensajes, limitar el tamaño máximo de adjuntos a mensajes para analizar y limitar la duración máxima del análisis de adjuntos a mensajes.

*Para configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **protección básica contra amenazas** → **Protección contra amenazas de correo**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Análisis de archivos compuestos**, ajuste la configuración del análisis:

   - **Analizar archivos adjuntos con formatos de Microsoft Office**. Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office.

   - **Analizar archivos de almacenamiento adjuntos**. Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE.

     Si, durante el análisis, Kaspersky Endpoint Security detecta una contraseña de un archivo de almacenamiento en el texto del mensaje, esta contraseña se utilizará para analizar el contenido del archivo en busca de aplicaciones maliciosas. En este caso, la contraseña no se guarda. Durante el análisis, el archivo de almacenamiento se descomprime. Si la aplicación genera un error durante el proceso de descompresión, puede eliminar manualmente los archivos descomprimidos que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tienen el prefijo PR.

   - **No analizar archivos de almacenamiento de más de N MB**. Si esta casilla está seleccionada, el componente Protección contra amenazas de correo excluye del análisis los archivos adjuntos en los mensajes de correo si

el tamaño excede el valor especificado. Si se desactiva la casilla, el componente Protección contra amenazas de correo analiza los archivos adjuntos de correo de cualquier tamaño.

- **Limitar el tiempo de análisis del archivo a N segundos**. Si la casilla está seleccionada, el tiempo asignado al análisis de archivos adjuntos en los mensajes de correo se limita al período especificado.

5. Guarde los cambios.

## Filtrado de archivos adjuntos a mensajes de correo electrónico

La funcionalidad de filtrado de archivos adjuntos no se aplica a mensajes de correo electrónico salientes.

Las aplicaciones malintencionadas pueden propagarse por correo electrónico, en forma de archivos adjuntos. Puede configurar el filtrado según el tipo de adjuntos a mensajes de modo que los archivos de los tipos especificados se renombren o se eliminen automáticamente. Al cambiarles el nombre a los archivos adjuntos de cierta clase, Kaspersky Endpoint Security puede impedir la ejecución automática de aplicaciones malintencionadas.

*Para configurar el filtrado de archivos adjuntos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **protección básica contra amenazas** → **Protección contra amenazas de correo**.
3. Haga clic en el botón **Configuración avanzada**.
4. En la sección **Filtrado de archivos adjuntos**, realice una de las siguientes acciones:
   - Si no desea que el componente Protección contra amenazas de correo filtre los archivos adjuntos de correo, seleccione la configuración **Deshabilitar el filtrado**.
   - Si desea que el componente Protección contra amenazas de correo cambie el nombre de los archivos adjuntos de los tipos especificados, seleccione la opción **Cambiar el nombre de los archivos adjuntos de los tipos seleccionados**.
   - Si desea que el componente Protección contra amenazas de correo elimine los archivos adjuntos a mensajes de los tipos de archivos especificados, seleccione la opción **Eliminar archivos adjuntos de los tipos seleccionados**.
5. Si seleccionó la opción **Cambiar el nombre de los archivos adjuntos de los tipos seleccionados** o la opción **Eliminar archivos adjuntos de los tipos seleccionados** en el paso anterior, seleccione las casillas que se encuentran frente a los tipos de archivos relevantes.
6. Guarde los cambios.

## Exportar e importar extensiones para filtrado de datos adjuntos

Puede exportar la lista de extensiones de filtrado de archivos adjuntos a un archivo XML. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de extensiones o para migrar la lista a otro servidor.

**Cómo exportar e importar una lista de extensiones de filtrado de archivos adjuntos a la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.
6. En la sección **Nivel de seguridad**, haga clic en **Configuración**.
7. En la ventana que se abre, seleccione la pestaña **Filtrado de archivos 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 vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de extensiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.
   Kaspersky Endpoint Security exportará la lista de extensiones completa al archivo XML.
9. Para importar la lista de extensiones:
   a. Haga clic en el vínculo **Importar**.
   b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de extensiones.
   c. Haga clic en el botón **Abrir**.
   Cuando ya exista una lista de extensiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
10. Guarde los cambios.

**Cómo exportar e importar una lista de extensiones de filtrado de archivos adjuntos a 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 correspondiente a los equipos en los que desea importar o exportar una lista de exclusiones.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.
5. Para exportar la lista de extensiones al bloque **Filtrado de archivos adjuntos**:
   a. Seleccione las extensiones que desea exportar.
   b. Haga clic en el vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de extensiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de extensiones completa al archivo XML.
6. Para importar una lista de extensiones al bloque **Filtrado de archivos adjuntos**:
   a. Haga clic en el vínculo **Importar**.
   b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de extensiones.
   c. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de extensiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
7. Guarde los cambios.

## Análisis de correo electrónico en Microsoft Office Outlook

Durante la instalación de Kaspersky Endpoint Security, la extensión de la Protección contra amenazas de correo se incorpora a Microsoft Office Outlook (en adelante, Outlook). Le permite abrir la configuración del componente Protección contra amenazas de correo desde Outlook y especificar en qué momento se deben analizar los mensajes de correo electrónico en busca de virus y otras amenazas. La extensión de la Protección contra amenazas de correo para Outlook puede analizar mensajes entrantes y salientes transmitidos a través de los protocolos POP3, SMTP, NNTP, IMAP y MAPI. Kaspersky Endpoint Security también es compatible con otros clientes de correo, como Microsoft Outlook Express®, Windows Mail y Mozilla™ Thunderbird™.

La extensión de Protección contra amenazas de correo puede funcionar con Outlook 2010, 2013, 2016 y 2019.

Si se está trabajando con el cliente de correo Mozilla Thunderbird, el componente Protección contra amenazas de correo no analiza mensajes que se transmiten mediante el protocolo IMAP en busca de virus y otras amenazas si se utilizan filtros para mover mensajes desde la carpeta **Bandeja de entrada**.

En Outlook, los mensajes entrantes son analizados primero por el componente Protección contra amenazas de correo (si se selecciona la casilla Analizar el tráfico POP3, SMTP, NNTP e IMAP en la interfaz de Kaspersky Endpoint Security) y, luego, por la extensión de Protección contra amenazas de correo para Outlook. Si el componente Protección contra amenazas de correo detecta un objeto malicioso en un mensaje, lo notifica sobre este evento.

Se puede establecer la configuración del componente Protección contra amenazas de correo directamente en Outlook si la extensión de Microsoft Outlook está conectada en la interfaz de Kaspersky Endpoint Security.

Los mensajes salientes son analizados primero por la extensión de la Protección contra amenazas de correo para Outlook y luego por el componente Protección contra amenazas de correo.

Si el correo se analiza usando la extensión de la Protección contra amenazas de correo para Outlook, se recomienda usar el Modo de intercambio en caché. Para información más detallada sobre el modo caché de Exchange y recomendaciones sobre su uso, consulte la Base de conocimientos de Microsoft.

*Para configurar el modo de funcionamiento de la extensión de Protección contra amenazas de correo para Outlook usando 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Protección contra amenazas de correo**.
6. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Protección contra amenazas de correo**.
7. En la sección **Conectividad**, haga clic en el botón **Configuración**.
8. En la ventana **Protección del correo electrónico**:
   - Seleccione la casilla **Analizar al recibir** si quiere que la extensión de Protección contra amenazas de correo para Outlook analice mensajes entrantes cuando llegan al buzón de correo.
   - Seleccione la casilla **Analizar al leer** si quiere que la extensión de Protección contra amenazas de correo para Outlook analice mensajes entrantes cuando los abra el usuario.
   - Seleccione la casilla **Analizar al enviar** si quiere que la extensión de Protección contra amenazas de correo para Outlook analice mensajes salientes cuando sean enviados.
9. Guarde los cambios.

# Protección contra amenazas de red

El componente Protección contra amenazas de red analiza el tráfico de red entrante en busca de actividad típica de ataques de red. Cuando Kaspersky Endpoint Security detecta un ataque de red contra el equipo del usuario, bloquea la conexión al equipo agresor.

Las distintas clases de ataques de red sobre las que se tiene registro, así como las maneras de combatirlos, se describen en las bases de datos de Kaspersky Endpoint Security. La lista de ataques de red que detecta el componente Protección contra amenazas de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación.

# Habilitación y deshabilitación de la Protección contra amenazas de red

De forma predeterminada, la Protección contra amenazas de red está habilitada y en ejecución en modo óptimo. Si es necesario, puede deshabilitar la Protección contra amenazas de red.

*Para habilitar o deshabilitar la Protección contra amenazas de red, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección contra amenazas de red**.
3. Utilice el interruptor **Protección contra amenazas de red** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

Por lo tanto, si la Protección contra amenazas de red está habilitada, 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 ataque de red contra el equipo del usuario, bloquea la conexión al equipo agresor.

# Bloquear un equipo atacante

*Para bloquear un equipo atacante:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección contra amenazas de red**.
3. Seleccione la casilla **Agregar equipos atacantes a la lista de equipos bloqueados por N minutos**.

   Si la casilla de verificación está seleccionada, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección.

   Puede acceder a la lista de equipos bloqueados a través de la ventana del Monitor de red.

   La lista de equipos bloqueados se vacía cada vez que Kaspersky Endpoint Security se reinicia o cuando se modifica la configuración de Protección contra amenazas de red.

4. Cambie la cantidad de tiempo durante la cual un equipo atacante se bloquea en el campo que se encuentra junto con la casilla **Agregar equipos atacantes a la lista de equipos bloqueados por N minutos**.

5. Guarde los cambios.

De esta manera, cuando Kaspersky Endpoint Security detecta un ataque de red contra el equipo del usuario, bloquea todas las conexiones con el equipo atacante.

## Configuración de direcciones de exclusiones del bloqueo

Kaspersky Endpoint Security puede reconocer un ataque a la red y bloquear una conexión de red no segura que transmita una gran cantidad de paquetes (por ejemplo, desde cámaras de vigilancia). Para trabajar con dispositivos de confianza, puede agregar las direcciones IP de estos dispositivos a la lista de exclusiones.

*Para configurar direcciones de exclusiones del bloqueo:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección contra amenazas de red**.

3. Haga clic en el vínculo **Administrar exclusiones**.

4. En la ventana, haga clic en el botón **Agregar**.

5. Ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.

6. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security no rastrea la actividad de los dispositivos en la lista de exclusiones.

## Exportar e importar la lista de exclusiones de bloqueo

Puede exportar la lista de exclusiones a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de exclusiones en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección básica contra amenazas → Protección contra amenazas de red**.
6. En el bloque **Configuración de Protección contra amenazas de 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 vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.
      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.
      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
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 correspondiente a los equipos en los que desea importar o exportar una lista de exclusiones.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Protección básica contra amenazas** → **Protección contra amenazas de red**.
5. En el bloque **Configuración de Protección contra amenazas de red**, haga clic en el vínculo **Exclusiones**.

   Se abre la lista de exclusiones.
6. Para exportar la lista de reglas:
   a. Seleccione las exclusiones que desea exportar.
   b. Haga clic en el botón **Exportar**.
   c. Confirme que desea exportar solo las exclusiones seleccionadas, o bien exporte la lista completa de exclusiones.
   d. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   e. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
8. Guarde los cambios.

## Configuración de defensas contra distintos tipos de ataques de red

Puede activar o desactivar las defensas de Kaspersky Endpoint Security contra los siguientes tipos de ataques de red:

- Ataques de *saturación de solicitudes*, con los cuales se busca afectar los recursos de red (por ejemplo, los servidores web) de una organización. En esta clase de ataque, se realiza una gran cantidad de solicitudes con el fin de sobrecargar el ancho de banda disponible para los recursos de red. La sobrecarga impide el acceso a los recursos de la organización.

- Ataques de *escaneo de puertos*, en los cuales se realiza un sondeo de los puertos UDP, los puertos TCP y los servicios de red del equipo. El escaneo de puertos permite determinar qué tan vulnerable es un equipo; suele estar seguido por algún tipo de ataque más peligroso. El escaneo también revela el sistema operativo del equipo y permite, así, elegir el ataque de red más apropiado.

- Ataques de *suplantación de MAC*, que consisten en cambiar la dirección MAC de un dispositivo (tarjeta) de red. Al realizar este cambio, un atacante puede redirigir los datos destinados a un dispositivo a otro dispositivo diferente y, de ese modo, obtener acceso a la información. Kaspersky Endpoint Security le permite saber si se detecta uno de estos ataques y bloquearlo.

Si alguna de sus aplicaciones autorizadas realiza operaciones que son típicas de estas clases de ataques, puede deshabilitar las funciones de detección pertinentes. Con ello evitará las falsas alarmas.

De manera predeterminada, Kaspersky Endpoint Security no está configurado para detectar ataques de saturación de red, de escaneo de puertos o de suplantación de MAC.

*Para configurar la protección contra cada tipo de ataque de red:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección contra amenazas de red**.
3. Use el interruptor **Tratar a los análisis de puertos y las inundaciones de red como ataques** para habilitar o deshabilitar la detección de estas clases de ataque.
4. Use el interruptor **Protección contra suplantaciones de MAC**.
5. En el bloque **Al detectar un ataque de suplantación de MAC**, seleccione una de las siguientes opciones:
   - **Notificarme solamente**.
   - **Notificarme y bloquear**.
6. Guarde los cambios.

## Firewall

El componente Firewall impide que se establezcan conexiones no autorizadas cuando el equipo está conectado a una red local o a Internet. Firewall también controla la actividad de red de las aplicaciones instaladas en el equipo. Ello ayuda a proteger la LAN corporativa contra ataques de robo de identidad y otras amenazas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el servicio de nube Kaspersky Security Network y las *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. El firewall crea automáticamente las reglas de red necesarias para que la aplicación y el Agente de red funcionen. Como resultado, el firewall abre varios puertos en la computadora. Los puertos que se abren dependen de la función de la computadora (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en la computadora, consulte *la Ayuda de Kaspersky Security Center*.

### Reglas de red

Las reglas de red se pueden configurar en distintos niveles:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security incluye una serie de reglas predefinidas, con permisos configurados según las recomendaciones de los expertos de Kaspersky.

- *Reglas de red de aplicaciones*. Las reglas de red de la aplicación imponen restricciones en la actividad de la red de una aplicación específica. Tienen en cuenta no solo las características del paquete de red, sino también la aplicación específica a la cual se dirige este paquete de red o que los emitió.

Controlar el acceso de las aplicaciones a los datos personales, a los procesos y a los recursos del sistema operativo es tarea del componente Prevención de intrusiones en el host, que utiliza los *derechos* asignados a las aplicaciones para tal fin.

Cuando una aplicación se ejecuta por primera vez, Firewall realiza las siguientes acciones:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.

2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Firewall, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los *grupos de confianza*: De confianza, Restricción mínima, Restricción máxima o No confiables.

   Los grupos de confianza determinan los derechos en los que Kaspersky Endpoint Security se basa para controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea la actividad de red de la aplicación si su grupo de confianza así lo requiere. Por ejemplo, las aplicaciones del grupo Restricción máxima no tienen permitido usar ninguna conexión de red.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Si la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están definidas para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

## Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más arriba en la lista se encuentra una regla, mayor es su prioridad. Cuando un mismo tipo de actividad de red se describe en varias reglas, Firewall se basa en la regla de mayor prioridad para regular la actividad.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si las reglas de paquetes de red y las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se procesa según las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan del siguiente modo: una regla de red para aplicaciones contiene reglas de acceso basadas en un estado de red (*red pública*, *red local* o *red de confianza*). Las aplicaciones del grupo de confianza Restricción máxima, por ejemplo, no tienen permitido realizar ninguna clase de actividad de red, independientemente de que el equipo esté conectado a una red pública, local o de confianza. Cuando se crea una regla de red para una aplicación individual (aplicación principal), dicha regla afecta también a los procesos secundarios de otras aplicaciones. Cuando no existe una regla de red para una aplicación, los procesos secundarios quedan sujetos a la regla de acceso de red correspondiente al grupo de confianza de la aplicación.

Supóngase, por ejemplo, que se prohíbe el tráfico en redes de cualquier estado para todas las aplicaciones, a excepción del navegador X. El navegador X (aplicación principal) se utiliza luego para iniciar la instalación de un navegador Y (proceso secundario). En este caso, el instalador del navegador Y tendrá acceso a la red y podrá descargar los archivos que hagan falta. Tras la instalación, sin embargo, Firewall no permitirá que el navegador Y establezca conexiones de red. Para que el instalador del navegador Y no pueda acceder a la red valiéndose de su condición de proceso secundario, será necesario agregar una regla de red que cubra ese programa específico.

### Estados de las conexiones de red

Firewall puede controlar la actividad de red basándose en el estado de la conexión. Kaspersky Endpoint Security obtiene el estado de la conexión del sistema operativo. El estado informado por el sistema operativo es el que el usuario configura cuando la conexión se establece por primera vez. Si lo desea, puede cambiar el estado de la conexión de red en la configuración de Kaspersky Endpoint Security. A la hora de controlar la actividad de red, Firewall tomará como válido el estado asignado dentro de Kaspersky Endpoint Security en lugar del estado que informe el sistema operativo.

La conexión de la red puede presentar uno de los siguientes tipos de estado:

- **Red pública**. Una red que no está protegida por una aplicación antivirus, un filtro o un firewall (un ejemplo podría ser la red Wi-Fi de una cafetería). Cuando el usuario opera un equipo conectado a una red de ese tipo, el Firewall bloquea el acceso a archivos e impresoras de este equipo. Los usuarios externos tampoco tienen acceso a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella.

  De forma predeterminada, Firewall asigna el estado *Red pública* a Internet. No puede cambiar el estado de Internet.

- **Red local**. Una red en la que los usuarios tienen restricciones para acceder a los archivos y las impresoras del equipo (un ejemplo podría ser una LAN corporativa u hogareña).

- **Red confiable**. Una red segura, en la que el equipo no está expuesto a ningún ataque o a intentos no autorizados de acceder a los datos que contiene. El Firewall permite cualquier actividad de red dentro de redes con este estado.

## Habilitación o deshabilitación del Firewall

Por defecto, el Firewall está habilitado y funciona en modo óptimo.

*Para habilitar o deshabilitar el Firewall:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección básica contra amenazas → Firewall**.

3. Utilice el interruptor **Firewall** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

## Cambio del estado de la conexión de red

De forma predeterminada, Firewall asigna el estado *Red pública* a Internet. No puede cambiar el estado de Internet.

*Para cambiar el estado de la conexión de red:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección básica contra amenazas → Firewall**.

3. Haga clic en el botón **Redes disponibles**.

4. Seleccione la conexión de red cuyo estado quiera cambiar.

5. En la columna **Tipo de red**, seleccione el estado de la conexión de red:

   - **Red pública**. Una red que no está protegida por una aplicación antivirus, un filtro o un firewall (un ejemplo podría ser la red Wi-Fi de una cafetería). Cuando el usuario opera un equipo conectado a una red de ese tipo, el Firewall bloquea el acceso a archivos e impresoras de este equipo. Los usuarios externos tampoco tienen acceso a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella.

   - **Red local**. Una red en la que los usuarios tienen restricciones para acceder a los archivos y las impresoras del equipo (un ejemplo podría ser una LAN corporativa u hogareña).

   - **Red confiable**. Una red segura, en la que el equipo no está expuesto a ningún ataque o a intentos no autorizados de acceder a los datos que contiene. El Firewall permite cualquier actividad de red dentro de redes con este estado.

6. Guarde los cambios.

## Administración de reglas de paquetes de red

Puede realizar las siguientes acciones mientras administra las reglas de paquetes de red:

- Crear una nueva regla de paquetes de red.

  Puede crear una nueva regla de paquetes de red al crear un conjunto de condiciones y acciones que se aplicará a los paquetes de red y flujos de datos.

- Habilitar o deshabilitar una regla de paquetes de red.

  Todas las reglas de paquetes de red creadas por el Firewall por defecto presentan el estado *Habilitado*. Cuando se habilita una regla de paquetes de red, el Firewall aplica esta regla.

Puede deshabilitar cualquier regla de paquetes de red seleccionada en la lista de reglas de paquetes de red. Cuando se deshabilita una regla de paquetes de red, el Firewall deja temporariamente de aplicar esta regla.

Cuando se agrega una nueva regla de paquetes de red personalizada a la lista de reglas de paquetes de red, por defecto aparece con estado *Habilitado*.

- Editar la configuración de una regla de paquetes de red existente.

  Luego de crear una nueva regla de paquetes de red, siempre puede volver a editar su configuración y modificarla según sea necesario.

- Cambiar la acción del Firewall para una regla de paquetes de red.

  En la lista de reglas de paquetes de red, puede editar la acción que realizará el Firewall al detectar actividad de red que no coincide con una regla de paquetes de red específica.

- Cambiar la prioridad de una regla de paquetes de red.

  Puede elevar o disminuir la prioridad de una regla de paquetes de red seleccionada en la lista.

- Eliminar una regla de paquetes de red.

  Puede eliminar una regla de paquetes de red para que el Firewall deje de aplicar esta regla al detectar actividad de red y para evitar que aparezca esta regla en la lista de reglas de paquetes de red con estado *Deshabilitado*.

## Creación de una regla de paquetes de red

Existen distintos métodos para crear una regla de paquetes de red:

- Utilizar la herramienta Monitor de red.

  El *Monitor de red* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de red del equipo de un usuario. Si opta por utilizar esta herramienta, no necesitará configurar todos los ajustes de la regla. Algunos de los ajustes de Firewall se tomarán de los datos del Monitor de red y se insertarán automáticamente. Para usar el Monitor de red, debe tener acceso a la interfaz de la aplicación.

- Configurar los ajustes de Firewall.

  Este método permite configurar cada parámetro de Firewall en detalle. Podrá crear reglas que cubran cualquier clase de actividad de red, aunque se trate de tráfico que no se haya registrado al momento de crear la regla.

Al crear reglas de paquetes de red, recuerde que estas tienen prioridad sobre las reglas de red para aplicaciones.

**Cómo usar la herramienta Monitor de red para crear una regla de paquetes de red mediante la interfaz de la aplicación**

1. En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Monitor de red**.
2. Seleccione la pestaña **Actividad de la red**.

   En la ficha **Actividad de la red** se muestran todas las conexiones de red actuales del equipo. Se muestran las conexiones de red entrantes y salientes.
3. En el menú contextual de alguna conexión de red, seleccione **Crear regla de paquetes**.

   Se abren las propiedades de la regla de red.
4. Establezca el estado **Activo** para la regla del paquete.
5. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
6. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Para seleccionar una plantilla de regla predefinida, haga clic en el vínculo **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
7. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
8. Haga clic en el botón **Guardar**.

   La nueva regla de red se agregará a la lista.
9. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.
10. Guarde los cambios.

Cómo crear una regla de paquetes de red desde la configuración de Firewall en la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en el botón **Reglas de paquetes**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
4. Haga clic en el botón **Agregar**.

   Se abren las propiedades de la regla de red.
5. Establezca el estado **Activo** para la regla del paquete.
6. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Para seleccionar una plantilla de regla predefinida, haga clic en el vínculo **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
8. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
9. Haga clic en el botón **Guardar**.

   La nueva regla de red se agregará a la lista.
10. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.
11. Guarde los cambios.

Cómo crear una regla de paquetes de red 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.
6. En la sección **Configuración de Firewall**, haga clic en el botón **Configuración**.

   Se abre una lista con las reglas de paquetes de red y otra lista con las reglas de red para aplicaciones.
7. Seleccione la pestaña **Reglas de paquetes de red**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
8. Haga clic en el botón **Agregar**.

   Esto abre las propiedades de las reglas de paquete.
9. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
10. Configure los parámetros de la regla de red (vea la tabla de más abajo).

    Si hace clic en el botón , podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de las reglas de red se completará automáticamente.
11. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
12. Haga clic en el botón **Guardar**.

    La nueva regla de red se agregará a la lista.
13. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.
14. Guarde los cambios.

Firewall controlará los paquetes de red según lo indique la regla. Para que Firewall deje de procesar una regla, en lugar de eliminarla de la lista, puede deshabilitarla. Para hacerlo, desactive la casilla ubicada junto al objeto.

Cómo crear una regla de paquetes de red mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **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 básica contra amenazas** → **Firewall**.
5. En el bloque **Configuración de Firewall**, haga clic en el vínculo **Reglas de paquetes de red**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
6. Haga clic en el botón **Agregar**.

   Esto abre las propiedades de las reglas de paquete.
7. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
8. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Si hace clic en el vínculo **Seleccionar plantilla**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
9. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
10. Haga clic en el botón **Guardar**.

    La nueva regla de red se agregará a la lista.
11. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.
12. Guarde los cambios.

Firewall controlará los paquetes de red según lo indique la regla. Para que Firewall deje de procesar una regla, en lugar de eliminarla de la lista, puede deshabilitarla. Use el interruptor de la columna **Estado** para habilitar o deshabilitar la regla de paquetes.

Parámetros de las reglas de paquetes de red

| Parámetro | Descripción |
|---|---|
| **Acción** | **Permitir**.<br>**Bloquear**.<br>**Por reglas de la aplicación**. Si elige esta opción, Firewall aplicará las reglas de red de aplicaciones a la conexión de red. |
| **Protocolo** | Controlar el tráfico de red asociado al protocolo elegido (TCP, UDP, ICMP, ICMPv6, IGMP o GRE).<br>Si se selecciona ICMP o ICMPv6 como protocolo, puede definir el tipo y el código del paquete ICMP.<br>Si selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto que usarán el equipo local y el equipo remoto para establecer la conexión a supervisar. Los puertos deben escribirse separados por comas. |
| **Sentido** | **Entrante (paquete)**. Firewall aplica la regla de red a todos los paquetes de red entrantes. |

| | |
|---|---|
| | **Entrante**. Firewall aplica la regla de red a todos los paquetes de red enviados a través de una conexión establecida por un equipo remoto.<br>**Entrante/saliente**. Firewall aplica la regla de red a todos los paquetes de red (sean entrantes o salientes), con independencia de si la conexión tuvo su origen en el equipo del usuario o en un equipo remoto.<br>**Saliente (paquete)**. Firewall aplica la regla de red a todos los paquetes de red salientes.<br>**Saliente**. Firewall aplica la regla de red a todos los paquetes de red enviados a través de una conexión establecida por el equipo del usuario.<br>El protocolo TCP permite establecer conexiones. Los sentidos disponibles para TCP son **Entrante**, **Saliente** y **Entrante/saliente**. Los demás protocolos se utilizan para enviar paquetes, no para establecer conexiones. En estos otros casos, los sentidos disponibles son **Entrante (paquete)**, **Saliente (paquete)** y **Entrante/saliente**. |
| **Adaptadores de red** | Adaptadores de red disponibles para enviar o recibir paquetes de red. Al especificar la configuración de los adaptadores de red, es posible diferenciar entre paquetes de red enviados o recibidos por adaptadores de red con direcciones IP idénticas. |
| **Período de vida (TTL)** | Restringir el control de paquetes de red según su período de vida (TTL). |
| **Direcciones remotas** | Direcciones de red asignadas a equipos remotos que pueden enviar y recibir paquetes de red. Firewall aplicará la regla de red a las direcciones de red remotas que estén dentro del intervalo especificado. Puede optar por incluir todas las direcciones IP en una regla de red, crear una lista de direcciones IP separada o seleccionar una subred (Redes de confianza, Redes locales o Redes públicas). |
| **Direcciones locales** | Direcciones de red asignadas a equipos que pueden enviar y recibir paquetes de red. Firewall aplica una regla de red al rango especificado de direcciones de redes locales. Puede optar por incluir todas las direcciones IP en una regla de red o por crear una lista de direcciones IP separada.<br>A veces no puede obtenerse la dirección local para las aplicaciones. Cuando esto ocurre, este parámetro no se tiene en cuenta. |

## Habilitación o deshabilitación de una regla de paquetes de red

*Para habilitar o deshabilitar una regla de paquetes de red:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en el botón **Reglas de paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminados que son establecidas por el Firewall.
4. Seleccione la regla de paquetes de red necesaria en la lista.
5. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la regla.

6. Guarde los cambios.

## Cambio de la acción del Firewall para una regla de paquetes de red

*Para cambiar la acción del Firewall que se aplica a una regla de paquetes de red.*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en el botón **Reglas de paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminados que son establecidas por el Firewall.
4. Selecciónela en la lista de reglas de paquetes de red y haga clic en el botón **Editar**.
5. En la lista desplegable **Acción**, seleccione la acción que debe realizar el Firewall al detectar este tipo de actividad de red:
   - **Permitir**.
   - **Bloquear**.
   - **Por reglas de la aplicación**.
6. Guarde los cambios.

## Cambio de la prioridad de una regla de paquetes de red

La prioridad de una regla de paquetes de red se determina por su posición en la lista de reglas de paquetes de red. La regla de paquetes de red superior de la lista de reglas de paquetes de red tiene la prioridad mayor.

Toda regla de paquetes de red creada manualmente se agrega al final de la lista de reglas de paquetes de red y es de prioridad menor.

El Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba a abajo. Según la regla de paquetes de red procesada que se aplica a una conexión de red en particular, el Firewall permite o bloquea el acceso a la red a la dirección y al puerto que se indican en la configuración de la conexión de red.

*Para modificar la prioridad de la regla de paquetes de red:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en el botón **Reglas de paquetes**.

   Esto abre una lista de reglas de paquetes de red predeterminados que son establecidas por el Firewall.
4. En la lista, seleccione la regla de paquetes de red cuya prioridad quiera cambiar.

5. Use los botones **Subir** y **Bajar** para mover la regla de paquetes de red al punto deseado en la lista de reglas de paquetes de red.

6. Guarde los cambios.

## Exportar e importar reglas de paquetes de red

Puede exportar la lista de reglas de paquetes de red a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de reglas del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de paquetes de red o para migrar la lista a otro servidor.

**Cómo exportar e importar una lista de reglas de paquetes de red a la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.

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

4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.

5. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.

6. Para exportar la lista de reglas de paquetes de red:

   a. Seleccione la regla de acceso que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.

   Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.

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

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Haga clic en el botón **Guardar**.

   Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.

7. Para importar una lista de reglas para paquetes de red:

   a. Haga clic en el vínculo **Importar**.

   En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

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

   Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

8. Guarde los cambios.

[Cómo exportar e importar una lista de reglas de paquetes de red en Web Console y Cloud Console]

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desee exportar o importar la lista de reglas.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Protección básica contra amenazas** → **Firewall**.
5. Haga clic en el vínculo **Reglas de paquetes de red**.
6. Para exportar la lista de reglas de paquetes de red:
   a. Seleccione la regla de acceso que desea exportar.
   b. Haga clic en el botón **Exportar**.
   c. Confirme que desea exportar solo las reglas seleccionadas, o bien exporte la lista completa.
   d. Haga clic en el botón **Exportar**.

      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 para paquetes de red:
   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
8. Guarde los cambios.

## Administración de reglas de red para aplicaciones

Por defecto, Kaspersky Endpoint Security agrupa todas las aplicaciones instaladas en el equipo por el nombre del proveedor de software cuya actividad de archivos o red se supervisa. A su vez, los grupos de aplicaciones se categorizan en grupos de confianza. Todas las aplicaciones y grupos de aplicaciones heredan propiedades de su grupo principal: reglas de control de aplicaciones, reglas de red para aplicaciones y su prioridad de ejecución.

Al igual que el componente Prevención contra intrusos, de forma predeterminada, el componente Firewall aplica las reglas de red para un grupo de aplicaciones al filtrar la actividad de red de todas las aplicaciones dentro del grupo. Las reglas de red del grupo de aplicaciones definen los permisos de las aplicaciones del grupo para el acceso a diferentes conexiones de red.

Por defecto, el Firewall crea un conjunto de reglas de red para cada grupo de aplicaciones detectado por Kaspersky Endpoint Security en el equipo. Puede cambiar la acción que el Firewall aplica a las reglas de red del grupo de aplicaciones creadas por defecto. No puede editar, eliminar, deshabilitar ni modificar la prioridad de las reglas de red del grupo de aplicaciones creadas por defecto.

También puede crear una regla de red para una aplicación en particular. Dicha regla tendrá una prioridad más alta que la regla de red del grupo al cual pertenece la aplicación.

## Creación de una regla de red para una aplicación

Por defecto, la actividad de una aplicación se controla mediante las reglas de red definidas para su grupo de confianza. El grupo de confianza de una aplicación se determina cuando esta se ejecuta por primera vez. En función de sus necesidades, puede crear reglas de red para todo un grupo de confianza, para una aplicación en particular o para un grupo de aplicaciones que pertenezcan a un grupo de confianza determinado.

Las reglas de red que se definen manualmente tienen mayor prioridad que las que se han determinado para un grupo de confianza. En otras palabras, cuando una aplicación está alcanzada por una regla definida manualmente y por una regla definida para su grupo de confianza, Firewall controla la actividad de la aplicación basándose en la regla definida manualmente.

De manera predeterminada, Firewall crea las siguientes reglas de red para cada aplicación:

- Cualquier actividad de red en Redes de confianza.
- Cualquier actividad de red en Redes locales.
- Cualquier actividad de red en Redes públicas.

Kaspersky Endpoint Security aplica las reglas predefinidas del siguiente modo para controlar la actividad de red de las aplicaciones:

- De confianza y Restricción mínima: se permite todo tipo de actividad de red.
- Restricción máxima y No confiables: no se permite ningún tipo de actividad de red.

Las reglas predefinidas no se pueden editar ni eliminar.

Si necesita crear una regla de red para una aplicación, cuenta con distintos métodos:

- Utilizar la herramienta Monitor de red.

  El *Monitor de red* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de red del equipo de un usuario. Si opta por utilizar esta herramienta, no necesitará configurar todos los ajustes de la regla. Algunos de los ajustes de Firewall se tomarán de los datos del Monitor de red y se insertarán automáticamente. Para usar el Monitor de red, debe tener acceso a la interfaz de la aplicación.

- Configurar los ajustes de Firewall.

  Este método permite configurar cada parámetro de Firewall en detalle. Podrá crear reglas que cubran cualquier clase de actividad de red, aunque se trate de tráfico que no se haya registrado al momento de crear la regla.

A la hora de crear una regla de red para una aplicación, no olvide que estas tienen menor prioridad que las reglas de paquetes de red.

**Cómo usar la herramienta Monitor de red desde la interfaz de la aplicación para crear una regla de red para una aplicación**

1. En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Monitor de red**.
2. Seleccione las fichas **Actividad de la red** o **Puertos abiertos**.

   En la ficha **Actividad de la red** se muestran todas las conexiones de red actuales del equipo. Se muestran las conexiones de red entrantes y salientes.

   La ficha **Puertos abiertos** enumera todos los puertos de red del equipo que se encuentran abiertos.
3. En el menú contextual de una conexión de red, seleccione **Crear regla de la aplicación**.

   Se abre la ventana de propiedades y reglas de la aplicación.
4. Seleccione la pestaña **Reglas de red**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
5. Haga clic en el botón **Agregar**.

   Se abren las propiedades de la regla de red.
6. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
7. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Para seleccionar una plantilla de regla predefinida, haga clic en el vínculo **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
8. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
9. Haga clic en el botón **Guardar**.

   La nueva regla de red se agregará a la lista.
10. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.
11. Guarde los cambios.

**Cómo crear una regla de red para una aplicación desde la configuración de Firewall en la interfaz de la aplicación**

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.
3. Haga clic en el botón **Reglas de aplicaciones**.

   Se abre una lista con las reglas de red que Firewall establece por defecto.
4. En la lista de aplicaciones, seleccione la aplicación (o el grupo de aplicaciones) a la que corresponderá la nueva regla de red.
5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.
6. Seleccione la pestaña **Reglas de red**.
7. Haga clic en el botón **Agregar**.

   Se abren las propiedades de la regla de red.
8. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
9. Configure los parámetros de la regla de red (vea la tabla de más abajo).

   Para seleccionar una plantilla de regla predefinida, haga clic en el vínculo **Plantilla de regla de red**. Las plantillas de reglas describen las conexiones de red más utilizadas.

   Toda la configuración de las reglas de red se completará automáticamente.
10. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
11. Haga clic en el botón **Guardar**.

    La nueva regla de red se agregará a la lista.
12. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.
13. Guarde los cambios.

Cómo crear una regla de red para una aplicación 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección básica contra amenazas** → **Firewall**.
6. En la sección **Configuración de Firewall**, haga clic en el botón **Configuración**.

   Se abre una lista con las reglas de paquetes de red y otra lista con las reglas de red para aplicaciones.
7. Seleccione la pestaña **Reglas de red de aplicaciones**.
8. Haga clic en el botón **Agregar**.
9. En la ventana que se abre, escriba un criterio para hallar la aplicación a la que corresponderá la nueva regla de red.

   Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
10. Haga clic en el botón **Actualizar**.

    Kaspersky Endpoint Security buscará la aplicación en una lista consolidada, en la que se recogen las aplicaciones instaladas en los equipos administrados. Las aplicaciones que coincidan con los criterios de búsqueda se mostrarán en una lista.
11. Seleccione la aplicación necesaria.
12. En la lista desplegable **Agregar las aplicaciones seleccionadas al grupo <grupo de confianza>**, seleccione **Grupos por defecto** y haga clic en **Aceptar**.

    La aplicación se agregará al grupo por defecto.
13. Seleccione la aplicación de su interés, abra al menú contextual de la misma y haga clic en el elemento **Derechos 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 con las reglas de red que Firewall establece por defecto.
15. Haga clic en el botón **Agregar**.

    Se abren las propiedades de la regla de red.
16. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
17. Configure los parámetros de la regla de red (vea la tabla de más abajo).

    Si hace clic en el botón , podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de las reglas de red se completará automáticamente.
18. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

19. Haga clic en el botón **Guardar**.

    La nueva regla de red se agregará a la lista.

20. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.

21. Guarde los cambios.

[Cómo crear una regla de red para una aplicación en Web Console y Cloud Console]

1. En la ventana principal de Web Console, seleccione **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 básica contra amenazas** → **Firewall**.
5. En el bloque **Configuración de Firewall**, haga clic en el vínculo **Reglas de red de aplicaciones**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
6. Seleccione la ficha **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.
7. Haga clic en el botón **Agregar**.

   Se inicia un asistente para agregar la aplicación a un grupo de confianza.
8. Haga clic en el vínculo **Grupo de destino seleccionado** para elegir el grupo de confianza para la aplicación.
9. Seleccione el tipo **Aplicación**. Haga clic en **Siguiente**.

   Si desea crear una regla de red para más de una aplicación, seleccione el tipo **Grupo** y escriba un nombre para el grupo de aplicaciones.
10. En la lista de aplicaciones, seleccione las aplicaciones a las que corresponderá la nueva regla de red.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
11. Haga clic en **Aceptar** para cerrar el asistente.

    La aplicación se agregará al grupo de confianza.
12. En la parte izquierda de la ventana, seleccione la aplicación de su interés.
13. En la parte derecha de la ventana, dentro de la lista desplegable, elija el elemento **Reglas de red**.

    Se abre una lista con las reglas de red que Firewall establece por defecto.
14. Haga clic en el botón **Agregar**.

    Se abren las propiedades de la regla.
15. Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.
16. Configure los parámetros de la regla de red (vea la tabla de más abajo).

    Si hace clic en el vínculo **Seleccionar plantilla**, podrá seleccionar una plantilla de regla predefinida. Las plantillas de reglas describen las conexiones de red más utilizadas.

    Toda la configuración de las reglas de red se completará automáticamente.
17. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.
18. Haga clic en el botón **Guardar**.

La nueva regla de red se agregará a la lista.

19. Defina la prioridad de la regla de red con los botones **Subir** y **Bajar**.

20. Guarde los cambios.

Parámetros de las reglas red para aplicaciones

| Parámetro | Descripción |
|---|---|
| **Acción** | **Permitir**.<br>**Bloquear**. |
| **Protocolo** | Controlar el tráfico de red asociado al protocolo elegido (TCP, UDP, ICMP, ICMPv6, IGMP o GRE).<br>Si se selecciona ICMP o ICMPv6 como protocolo, puede definir el tipo y el código del paquete ICMP.<br>Si selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto que usarán el equipo local y el equipo remoto para establecer la conexión a supervisar. Los puertos deben escribirse separados por comas. |
| **Sentido** | **Entrante**.<br>**Entrante/saliente**.<br>**Saliente**. |
| **Direcciones remotas** | Direcciones de red asignadas a equipos remotos que pueden enviar y recibir paquetes de red. Firewall aplicará la regla de red a las direcciones de red remotas que estén dentro del intervalo especificado. Puede optar por incluir todas las direcciones IP en una regla de red, crear una lista de direcciones IP separada o seleccionar una subred (Redes de confianza, Redes locales o Redes públicas). |
| **Direcciones locales** | Direcciones de red asignadas a equipos que pueden enviar y recibir paquetes de red. Firewall aplica una regla de red al rango especificado de direcciones de redes locales. Puede optar por incluir todas las direcciones IP en una regla de red o por crear una lista de direcciones IP separada.<br>A veces no puede obtenerse la dirección local para las aplicaciones. Cuando esto ocurre, este parámetro no se tiene en cuenta. |

## Activación y desactivación de una regla de red para aplicaciones

*Para habilitar o deshabilitar una regla de red para aplicaciones:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en el botón **Reglas de aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el cual quiera crear o editar una regla de red.

5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la pestaña **Reglas de red**.

7. En la lista de reglas de red para un grupo de aplicaciones, seleccione la regla de red relevante.

   Se abre la ventana de propiedades de la regla de red.

8. Configure el estado **Activo** o **Inactivo** para la regla de red.

   No se puede deshabilitar una regla de red de un grupo de aplicaciones creada por el Firewall de manera predeterminada.

9. Guarde los cambios.

## Cambio de la acción del Firewall para una regla de red para aplicaciones

Puede modificar la acción del Firewall que se aplica a todas las reglas de red correspondientes a una aplicación o a un grupo de aplicaciones que se crearon por defecto, y modificar la acción del Firewall para una sola regla de red personalizada para una aplicación o un grupo de aplicaciones.

*Para cambiar la acción del Firewall para todas las reglas de red correspondientes a una aplicación o a un grupo de aplicaciones:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en el botón **Reglas de aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. Si quiere cambiar la acción del Firewall que se aplica a todas las reglas de red que se crearon de forma predeterminada, seleccione una aplicación o un grupo de aplicaciones en la lista. Las reglas de red creadas manualmente no se modifican.

5. Haga clic derecho para abrir el menú contextual, seleccione **Reglas de red** y luego seleccione la acción que desea asignar:

   - **Heredar**.
   - **Permitir**.
   - **Bloquear**.

6. Guarde los cambios.

*Para cambiar la respuesta del Firewall para una regla de red correspondiente a una aplicación o a un grupo de aplicaciones:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en el botón **Reglas de aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el cual quiera cambiar la acción correspondiente a una regla de red.

5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la pestaña **Reglas de red**.

7. Seleccione la regla de red para la cual quiera cambiar la acción del Firewall.

8. En la columna **Permiso**, haga clic con el botón derecho para mostrar el menú contextual y seleccione la acción que desea asignar:

   - **Heredar.**
   - **Permitir**.
   - **Bloquear**.
   - **Registrar eventos**.

9. Guarde los cambios.

## Cambio de la prioridad de una regla de red para aplicaciones

La prioridad de una regla de red es determinada por su posición en la lista de reglas de red. El Firewall ejecuta las reglas en el orden en el que aparecen en la lista de reglas de red, de arriba a abajo. Según cada regla de red procesada que corresponde a una conexión de red específica, el Firewall permite o bloquea el acceso de red a la dirección y al puerto que se indican en la configuración de dicha conexión de red.

Las reglas de red creadas manualmente tienen una prioridad más alta que las predeterminadas.

No puede cambiar la prioridad de las reglas de red para un grupo de aplicaciones creadas por defecto.

*Para cambiar la prioridad de una regla de red:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Firewall**.

3. Haga clic en el botón **Reglas de aplicaciones**.

   Esto abre la lista de reglas de la aplicación.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el cual quiera cambiar la prioridad de una regla de red.

5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Detalles y reglas**.

   Se abre la ventana de propiedades y reglas de la aplicación.

6. Seleccione la pestaña **Reglas de red**.

7. Seleccione la regla de red cuya prioridad quiera cambiar.

8. Use los botones **Subir** y **Bajar** para mover la regla de red al punto deseado en la lista de reglas de red.

9. Guarde los cambios.

## Monitor de red

El *Monitor de red* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de red del equipo de un usuario.

*Para iniciar el Monitor de red:*

En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Monitor de red**.

Se abre la ventana **Monitor de red**. En esta ventana, se muestra la información sobre la actividad de red del equipo en cuatro fichas:

- En la ficha **Actividad de la red** se muestran todas las conexiones de red actuales del equipo. Se muestran las conexiones de red entrantes y salientes. Desde esta ficha también se pueden crear las reglas de paquetes de red con las que opera el Firewall.
- La ficha **Puertos abiertos** enumera todos los puertos de red del equipo que se encuentran abiertos. Desde esta ficha también se pueden crear las reglas de paquetes de red y las reglas para aplicaciones con las que opera el Firewall.
- En la ficha **Tráfico de red** se muestra el volumen del tráfico de red entrante y saliente entre el equipo del usuario y otros equipos de la red a la cual se encuentre conectado el usuario.
- En la ficha **Equipos bloqueados** se enumeran las direcciones IP de los equipos remotos cuya actividad de red ha sido bloqueada por el componente Protección contra amenazas de red después de detectar intentos de ataques de red desde estas direcciones IP.

## Prevención de ataques BadUSB

Algunos virus modifican el firmware de los dispositivos USB para hacer que el sistema operativo considere que el dispositivo USB es un teclado. De esta manera, el virus puede ejecutar comandos en su cuenta de usuario para descargar malware, por ejemplo.

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

Cuando un dispositivo USB se conecta al equipo y es identificado por el sistema operativo como un teclado, la aplicación le solicita al usuario que ingrese un código numérico generado por la aplicación desde este teclado, o con un Teclado en pantalla, si está disponible (vea la siguiente imagen). Este procedimiento se conoce como autorización del teclado.

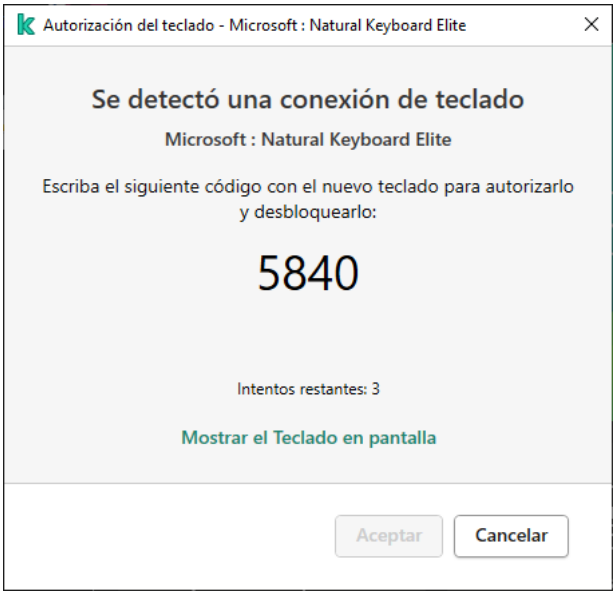
Si el código se ha ingresado correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al cual se ha conectado) en la lista de teclados autorizados. No es necesario repetir la autorización cuando el teclado vuelve a conectarse o después del reinicio del sistema operativo.

Si el teclado autorizado se conecta a otro puerto USB del equipo, la aplicación mostrará otra vez una solicitud de autorización para este teclado.

Si se ha ingresado incorrectamente el código numérico, la aplicación genera un nuevo código. Puede haber tres intentos para ingresar el código numérico. Si el código numérico se ingresa incorrectamente tres veces consecutivas o se cierra la venta **Autorización del teclado <Nombre del teclado>**, la aplicación bloquea la entrada desde este teclado. Cuando el teclado vuelve a conectarse o cuando se reinicia el sistema operativo, la aplicación le solicita al usuario que lleve a cabo nuevamente la autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea un teclado que no haya sido autorizado.

El componente Prevención de ataques BadUSB no se instala por defecto. Si desea utilizarlo, agréguelo en las propiedades del paquete de instalación antes de instalar la aplicación. Si la aplicación ya está instalada, modifique la selección de componentes disponibles.




*Autorización del teclado*

## Habilitación y deshabilitación de Prevención de ataques BadUSB

Los dispositivos USB identificados por el sistema operativo como teclados y conectados al equipo antes de la instalación del componente de Prevención de ataques BadUSB se consideran autorizados después de la instalación del componente.

*Para habilitar o deshabilitar la Prevención de ataques BadUSB:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.
3. Use el interruptor **Prevención de ataques BadUSB** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

De esta manera, si Prevención de ataques BadUSB está habilitado, Kaspersky Endpoint Security requiere la autorización de un dispositivo USB conectado identificado como un teclado por el sistema operativo. El usuario no podrá usar un teclado no autorizado hasta que lo autorice.

## Usar el Teclado en pantalla para la autorización de dispositivos USB

El teclado en pantalla debería usarse únicamente para autorización de dispositivos USB que no sean compatibles con la entrada de caracteres aleatorios (p. ej., lectoras de códigos de barra). No se recomienda el uso del teclado en pantalla para la autorización de dispositivos USB desconocidos.

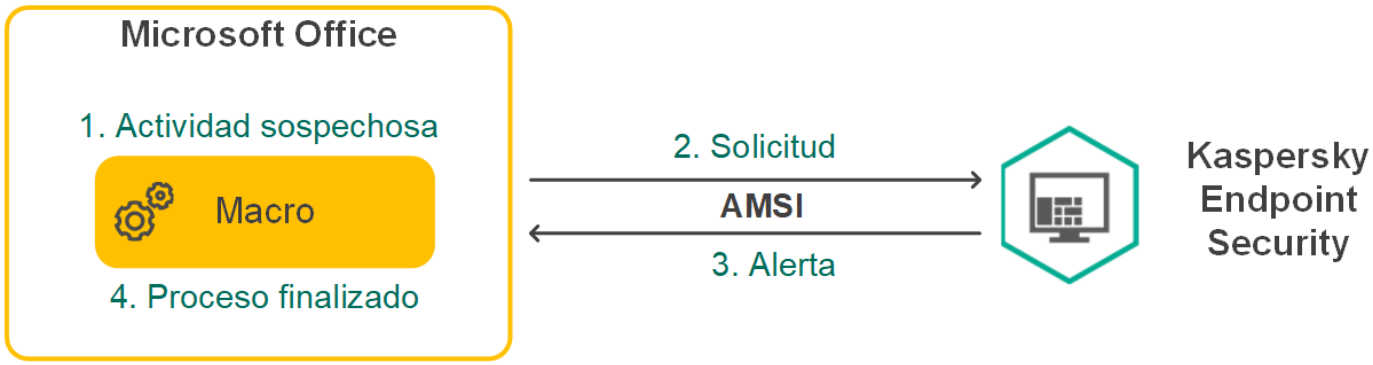
*Para permitir o prohibir el uso del teclado en pantalla para autorización:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Prevención de ataques BadUSB**.
3. Use la casilla **No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB** para permitir o bloquear el uso del teclado en pantalla para la autorización.
4. Guarde los cambios.

## Protección vía AMSI

El componente Protección vía AMSI está diseñado para admitir la interfaz de análisis antimalware 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 información sobre AMSI, consulte la *documentación de Microsoft*.

La Protección vía AMSI únicamente puede detectar amenazas y notificárselo a la aplicación. La aplicación de terceros después de recibir una notificación de una amenaza no le permite realizar acciones maliciosas (por ejemplo, la finaliza).




Ejemplo del funcionamiento de AMSI

El componente Protección vía AMSI puede rechazar una solicitud de una aplicación de terceros, por ejemplo, si esta aplicación excede el número máximo de solicitudes dentro de un intervalo específico. Cuando esto ocurre, Kaspersky Endpoint Security envía información al respecto al Servidor de administración. El componente Protección vía AMSI no rechaza las solicitudes que provienen de aplicaciones de terceros para las que se ha seleccionado la casilla **No bloquear la interacción con el Proveedor de protección para AMSI**

La Protección vía AMSI está disponible para los siguientes sistemas operativos para estaciones de trabajo y servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter

## Habilitar y deshabilitar la Protección vía AMSI

De manera predeterminada, la Protección vía AMSI está habilitada.

*Para habilitar o deshabilitar la Protección vía AMSI:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección básica contra amenazas** → **Protección vía AMSI**.
3. Utilice el interruptor **Protección vía AMSI** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

## Uso de Protección vía 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 u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis.

*Para configurar los análisis con Protección vía AMSI de archivos compuestos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección básica contra amenazas → Protección vía 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 la sección **Límite de tamaño**, realice una de las siguientes acciones:
   - Para que el componente Protección vía AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos grandes** y especifique el valor que considere apropiado en el campo **Tamaño máximo de archivo**. El componente Protección vía AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.
   - Para permitir que el componente Protección vía AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **No desempaquetar archivos compuestos grandes**.

   El componente Protección vía AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.
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 malintencionado. El ataque permite al exploit instalar malware sin autorización.

Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

## Habilitación y deshabilitación de la Prevención de exploits

De manera predeterminada, la Prevención de exploits está habilitada y se ejecuta en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede deshabilitar la Prevención de exploits.

*Para habilitar o deshabilitar la Prevención de exploits, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Prevención de exploits**.

3. Use el interruptor **Prevención de exploits** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

De esta manera, si la Prevención de exploits está habilitada, Kaspersky Endpoint Security supervisará los archivos ejecutados por aplicaciones vulnerables. Si Kaspersky Endpoint Security detecta que no fue el usuario quien ejecutó un archivo de una aplicación vulnerable, Kaspersky Endpoint Security realizará la acción seleccionada (por ejemplo, bloqueará la operación).

## Selección de una acción para realizar cuando se detecta un exploit

Por defecto, al detectar un exploit, Kaspersky Endpoint Security bloquea las operaciones que ha intentado realizar el exploit.

*Para seleccionar una acción a realizar cuando se detecta un exploit:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Prevención de exploits**.

3. Seleccione la acción correspondiente en el bloque **Al detectarse un exploit**:

   - **Bloquear operación**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.

   - **Informar**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security, registra una entrada con información del exploit y añade información sobre este exploit a la lista de amenazas activas.

4. Guarde los cambios.

## Protección de la memoria de procesos del sistema

Por defecto, la protección de la memoria de procesos del sistema está habilitada.

*Para habilitar o deshabilitar la protección de la memoria de procesos del sistema:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Prevención de exploits**.

3. Utilice el interruptor **Habilitar la protección de la memoria de procesos del sistema** para habilitar o deshabilitar esta característica.

4. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security bloqueará los procesos externos que intenten acceder a los procesos del sistema.

## Detección de comportamientos

El componente Detección de comportamientos recibe datos sobre las acciones de las aplicaciones del equipo y transmite esta información a los demás componentes de protección para mejorar su rendimiento.

El componente Detección de comportamientos utiliza firmas de patrones de comportamiento para aplicaciones. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Endpoint Security realiza la acción de respuesta especificada. Las funcionalidades de Kaspersky Endpoint Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo.

## Habilitación y deshabilitación de la Detección de comportamientos

De manera predeterminada, el componente Detección de comportamientos está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede deshabilitar la Detección de comportamientos.

No se recomienda deshabilitar la Detección de comportamientos a menos que sea absolutamente necesario, ya que hacerlo reduciría la eficacia de los componentes de protección. Los componentes de protección pueden solicitar datos recopilados por el componente Detección de comportamientos para detectar amenazas.

*Para habilitar o deshabilitar la Detección de comportamientos, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Detección de comportamiento**.
3. Use el interruptor **Detección de comportamiento** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

De esta manera, si la opción Detección de comportamiento está habilitada, Kaspersky Endpoint Security utilizará firmas de patrones de comportamiento para analizar la actividad de las aplicaciones en el sistema operativo.

## Selección de la acción que se realizará al detectarse actividades malintencionadas

*Para definir qué ocurrirá si una aplicación comienza a realizar acciones malintencionadas, haga lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Detección de comportamiento**.
3. Seleccione la acción correspondiente en el bloque **Al detectar actividad de malware**:

- **Eliminar archivo**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.

- **Finalizar la aplicación**. Si este elemento se encuentra seleccionado, Kaspersky Endpoint Security cierra la aplicación al detectar alguna actividad de software malintencionado.

- **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Endpoint Security agrega información sobre la actividad de malware a la lista de amenazas activas.

4. Guarde los cambios.

## Protección de carpetas compartidas contra cifrado externo

Este componente supervisa solamente las operaciones realizadas con los archivos almacenados en dispositivos de almacenamiento masivo con el sistema de archivos NTFS y que no están cifrados con EFS.

La protección de las carpetas compartidas contra el cifrado externo permite el análisis de la actividad en carpetas compartidas. Cuando la actividad coincide con una firma de patrones de comportamiento que suele verse en actos de cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.

De forma predeterminada, la protección de carpetas compartidas contra el cifrado externo está deshabilitada.

Después de instalar Kaspersky Endpoint Security, la protección de carpetas compartidas contra cifrado externo será limitada hasta que se reinicie el equipo.

## Habilitación y deshabilitación de la protección de carpetas compartidas contra el cifrado externo

Después de instalar Kaspersky Endpoint Security, la protección de carpetas compartidas contra cifrado externo será limitada hasta que se reinicie el equipo.

*Para habilitar o deshabilitar la protección de carpetas compartidas contra el cifrado externo, realice lo siguiente:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Detección de comportamiento**.

3. Utilice el interruptor **Habilitar protección de carpetas compartidas contra el cifrado externo** para habilitar o deshabilitar la detección de actividad típica del cifrado externo.

4. Guarde los cambios.

## Selección de la acción para realizar ante la detección del cifrado externo de carpetas compartidas

*Para seleccionar la acción para realizar ante la detección del cifrado externo de carpetas compartidas, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Detección de comportamiento**.
3. Seleccione la acción correspondiente en el bloque **Protección de carpetas compartidas contra el cifrado externo**:
   - **Bloquear conexión por N minutos**. 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 la actividad de red del equipo responsable por el intento de modificación.
     - Crea copias de seguridad de los archivos que se están modificando.
     - Agrega 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 habilitado, los archivos modificados se restaurarán de sus copias de seguridad.
   - **Informar**. Si se selecciona esta opción, al detectar un intento de modificar los archivos de las carpetas compartidas, Kaspersky Endpoint Security realiza las siguientes acciones:
     - Agrega una entrada en los informes de la interfaz local de la aplicación.
     - Agrega 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 contra el cifrado externo

Excluir una carpeta puede reducir la cantidad de falsos positivos si su organización utiliza el cifrado de datos cuando se intercambian archivos utilizando carpetas compartidas. Por ejemplo, Detección de comportamiento puede generar falsos positivos cuando el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Dicha actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, agregue esa carpeta a las exclusiones.

**Cómo crear una exclusión para la protección de carpetas compartidas 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 que se abre, seleccione la pestaña **Exclusiones de análisis**.

   Esto abre una ventana que contiene una lista de exclusiones.
8. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
9. Seleccione la casilla **Permitir el uso de aplicaciones 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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de deshabilitar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
10. Haga clic en el botón **Agregar**.
11. En la sección **Propiedades**, seleccione la casilla **Archivo o carpeta**.
12. Haga clic en el vínculo al **archivo o carpeta** en la sección **Descripción de la exclusión de análisis (haga clic en los elementos subrayados para editarlos)** para abrir la ventana **Nombre de archivo o carpeta**.
13. Haga clic en **Examinar** y seleccione la carpeta compartida.

    También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Carpeta`, excepto la `Carpeta` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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 necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

15. Haga clic en **cualquier** vínculo en la sección **Descripción de la exclusión de análisis (haga clic en los elementos subrayados para editarlos)** para activar el vínculo para **seleccionar componentes**.

16. Haga clic en el vínculo para **seleccionar componentes** para abrir la ventana **Componentes de protección**.

17. Seleccione la casilla junto al componente **Detección de comportamiento**.

18. Guarde los cambios.

Cómo crear una exclusión para la protección de carpetas compartidas 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** → **Exclusiones**.
5. En el bloque **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el vínculo **Exclusiones de análisis**.
6. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
7. Seleccione la casilla **Permitir el uso de aplicaciones 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, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de deshabilitar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
8. Haga clic en el botón **Agregar**.
9. Seleccione cómo desea agregar el **Archivo o carpeta** de exclusión
10. Haga clic en **Examinar** y seleccione la carpeta compartida.

    También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Carpeta`, excepto la `Carpeta` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
    - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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 comportamientos**.

12. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

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 las carpetas compartidas en la interfaz de la aplicación]

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

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

3. En el bloque **Exclusiones**, haga clic en el vínculo **Administrar exclusiones**.

4. Haga clic en el botón **Agregar**.

5. Haga clic en **Examinar** y seleccione la carpeta compartida.

   También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite los caracteres `*` y `?` al ingresar una máscara:

   - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Carpeta\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Carpeta`, excepto la `Carpeta` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

   - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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 comportamientos**.

7. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

8. Seleccione el estado **Activo** para la exclusión.

   Puede usar el interruptor para detener una exclusión en cualquier momento.

9. Guarde los cambios.

## Configuración de las direcciones de las exclusiones de la protección de carpetas compartidas contra el cifrado externo

El servicio Audit Logon debe estar habilitado para permitir realizar exclusiones de direcciones desde Protección de carpetas compartidas contra el cifrado externo. De manera predeterminada, el servicio Inicio de sesión de auditoría está deshabilitado (para obtener información detallada sobre la habilitación del servicio Inicio de sesión de auditoría, visite el sitio web de Microsoft).

La funcionalidad para la exclusión de direcciones desde Protección de carpetas compartidas no funcionará en un equipo remoto si dicho equipo estaba encendido antes de iniciar Kaspersky Endpoint Security. Puede reiniciar el equipo remoto después de haber iniciado Kaspersky Endpoint Security para asegurarse de que la funcionalidad de excluir direcciones desde la protección de carpetas compartidas funcione en este equipo remoto.

*Para excluir equipos remotos que llevan a cabo el cifrado externo de carpetas compartidas:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Detección de comportamiento**.
3. En el bloque **Exclusiones**, haga clic en el vínculo **Configurar las direcciones de las exclusiones**.
4. Si desea agregar una Dirección IP o nombre de equipo a la lista de exclusiones, haga clic en el botón **Añadir**.
5. Escriba la Dirección IP o el nombre del equipo desde el cual no se deben gestionar los intentos de cifrado.
6. Guarde los cambios.

## Exportar e importar una lista de exclusiones de la protección de carpetas compartidas contra el cifrado externo

Puede exportar la lista de exclusiones a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de exclusiones en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva **Protección avanzada contra amenazas** → **Detección de comportamiento**.
6. En la sección **Protección de carpetas compartidas contra el cifrado externo**, 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 vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.
      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.
      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
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 correspondiente a los equipos en los que desea importar o exportar una lista de exclusiones.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Protección avanzada contra amenazas** → **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 bien exporte la lista completa de exclusiones.
   d. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   e. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
7. Guarde los cambios.

## Prevención contra intrusos

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El componente Prevención contra intrusos impide que las aplicaciones realicen acciones que puedan ser peligrosas para el sistema operativo y garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus y el servicio de nube Kaspersky Security Network.

Para controlar el funcionamiento de las aplicaciones, el componente se basa en los *derechos* que estas tienen asignados. Los siguientes parámetros de acceso son algunos de esos derechos:

- Acceso a los recursos del sistema operativo (claves del Registro, opciones de ejecución automática, etc.)
- Acceso a datos personales (archivos, aplicaciones, etc.)

Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

Cuando una aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host hace lo siguiente:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.
2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Prevención de intrusiones en el host, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los *grupos de confianza*: De confianza, Restricción mínima, Restricción máxima o No confiables.

   Los grupos de confianza determinan los derechos en los que Kaspersky Endpoint Security se basa para controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea las acciones de la aplicación tomando como referencia el grupo de confianza al que pertenece. Por ejemplo, las aplicaciones del grupo Restricción máxima no pueden acceder a los módulos del sistema operativo.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

## Habilitación y deshabilitación de la Prevención contra intrusos

De manera predeterminada, el componente Prevención contra intrusos está habilitado y se ejecuta en el modo recomendado por los expertos de Kaspersky.

### Cómo habilitar o deshabilitar el componente Prevención de intrusiones en el host mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. Utilice la casilla **Prevención de intrusiones en el host** para habilitar o deshabilitar el componente.
7. Guarde los cambios.

### Cómo habilitar o deshabilitar el componente Prevención de intrusiones en el host mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas → Prevención de intrusiones en el host**.
5. Utilice el interruptor **Prevención de intrusiones en el host** para habilitar o deshabilitar el componente.
6. Guarde los cambios.

### Cómo habilitar o deshabilitar el componente Prevención de intrusiones en el host mediante la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
3. Utilice el interruptor **Prevención de intrusiones en el host** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

Si habilita el componente Prevención de intrusiones en el host, Kaspersky Endpoint Security definirá el grupo de confianza de una aplicación teniendo en cuenta lo peligrosa que pueda resultar para el equipo. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo.

## Administración de grupos de confianza de aplicaciones

Cuando se inicia cada aplicación por primera vez, el componente Prevención contra intrusos comprueba la seguridad de la aplicación y la ubica en uno de los grupos de confianza.

En la primera etapa del análisis de aplicaciones, Kaspersky Endpoint Security busca en la base de datos interna de aplicaciones conocidas una entrada coincidente y, simultáneamente, envía una solicitud a la base de datos de Kaspersky Security Network (si hay alguna conexión a Internet disponible). En función de los resultados de la búsqueda en la base de datos interna y la base de datos de Kaspersky Security Network, se ubica a la aplicación en un grupo de confianza. Cada vez que se inicia la aplicación, Kaspersky Endpoint Security envía una consulta nueva a la base de datos de KSN y ubica la aplicación en un grupo de confianza diferente si ha cambiado la reputación de la aplicación en las bases de datos de KSN.

Puede seleccionar el grupo de confianza al que Kaspersky Endpoint Security asignará las aplicaciones desconocidas automáticamente. Las aplicaciones que se inician antes que Kaspersky Endpoint Security se mueven automáticamente al grupo de confianza definido en la ventana de configuración del componente Prevención de intrusiones en el host.

Para aplicaciones que se iniciaron antes de Kaspersky Endpoint Security, solamente se supervisa la actividad de red. El control se realiza utilizando las reglas de red definidas en la configuración de Firewall.

## Modificación del grupo de confianza de una aplicación

Cuando se inicia cada aplicación por primera vez, el componente Prevención contra intrusos comprueba la seguridad de la aplicación y la ubica en uno de los grupos de confianza.

Los especialistas de Kaspersky no recomiendan mover las aplicaciones del grupo de confianza asignado automáticamente a un grupo diferente. Considere, en cambio, modificar los derechos de una aplicación en particular cuando resulte necesario.

**Cómo cambiar el grupo de confianza de una aplicación mediante la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones**, haga clic en el botón **Agregar**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
7. Seleccione la ficha **Derechos de aplicaciones**.
8. Haga clic en el botón **Agregar**.
9. En la ventana que se abre, escriba un criterio de búsqueda para dar con la aplicación cuyo grupo de confianza desee cambiar.

   Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
10. Haga clic en el botón **Actualizar**.

    Kaspersky Endpoint Security buscará la aplicación en una lista consolidada, en la que se recogen las aplicaciones instaladas en los equipos administrados. Las aplicaciones que coincidan con los criterios de búsqueda se mostrarán en una lista.
11. Seleccione la aplicación necesaria.
12. En la lista desplegable **Agregar las aplicaciones seleccionadas al grupo <grupo de confianza>**, seleccione un grupo de confianza para la aplicación.
13. Guarde los cambios.

[Cómo cambiar el grupo de confianza de una aplicación mediante Web Console y Cloud Console]

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
6. Seleccione la ficha **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.
7. Haga clic en el botón **Agregar**.

   Se inicia un asistente para agregar la aplicación a un grupo de confianza.
8. Haga clic en el vínculo **Grupo de destino seleccionado** para elegir el grupo de confianza para la aplicación.
9. Seleccione el tipo **Aplicación**. Haga clic en **Siguiente**.

   Para cambiar el grupo de confianza de más de una aplicación, seleccione el tipo **Grupo** y escriba un nombre para el grupo de aplicaciones.
10. En la lista de aplicaciones que se abre, seleccione las aplicaciones para las que se cambiará el grupo de confianza.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
11. Haga clic en **Aceptar** para cerrar el asistente.

    La aplicación se agregará al grupo de confianza.
12. Guarde los cambios.

[Cómo cambiar el grupo de confianza de una aplicación mediante la interfaz de la aplicación]

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **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 necesaria.
5. En el menú contextual de la aplicación, seleccione **Restricciones** → <γρυπο δε χονφιανζα>.
6. Guarde los cambios.

La aplicación se agregará al nuevo grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo. La aplicación pasará a tener el estado *(definido por el usuario)*. El componente Prevención de intrusiones en el host mantendrá la aplicación en el grupo definido por el usuario incluso si la reputación de la misma se modifica en Kaspersky Security Network.

## Configuración de los derechos disponibles en los grupos de confianza

De manera predeterminada, los grupos de confianza tienen definidos los derechos óptimos para cada categoría de aplicaciones. Los grupos de aplicaciones que forman parte de un grupo de confianza heredan de este la configuración de sus derechos.

**Cómo cambiar los derechos de un grupo de confianza mediante la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones**, haga clic en el botón **Agregar**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
7. Seleccione la ficha **Derechos de aplicaciones**.
8. Seleccione el grupo de confianza necesario.
9. En el menú contextual del grupo de confianza, haga clic en **Derechos del grupo**.

   Se abren las propiedades del grupo de confianza.
10. Realice una de las siguientes acciones:

    - Abra la pestaña **Archivos y Registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.
    - Abra la pestaña **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

    Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.
11. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Autorizar** (✓) o **Rechazar** (⊘).
12. Seleccione la opción **Guardar en informe** (✓ / ⊘) si le interesa monitorear cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.
13. Guarde los cambios.

Cómo cambiar los derechos de un grupo de confianza mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
6. Seleccione la ficha **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.
7. En la parte izquierda de la ventana, seleccione el grupo de confianza pertinente.
8. En la parte derecha de la ventana, en la lista desplegable, realice una de las siguientes acciones:

   - Seleccione **Archivos y Registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.
   - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

   Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.
9. Busque el recurso en el que esté interesado y seleccione una opción en la columna con la acción pertinente: **Heredar**, **Autorizar** (  ) o **Rechazar** (  ).
10. Seleccione la opción **Guardar en informe** (  /  ) si le interesa monitorear cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.
11. Guarde los cambios.

Cómo cambiar los derechos de un grupo de confianza mediante la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **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 necesario.
5. En el menú contextual del grupo de confianza, seleccione **Detalles y reglas**.

   Se abren las propiedades del grupo de confianza.
6. Realice una de las siguientes acciones:

   - Abra la pestaña **Archivos y Registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.
   - Abra la pestaña **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

   Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.
7. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Autorizar** () o **Rechazar** ().
8. Seleccione la opción **Guardar en informe** () si le interesa monitorear cómo se utilizan los recursos del equipo.

   Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.
9. Guarde los cambios.

Se cambiarán los derechos del grupo de confianza. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo. El grupo pasará a tener el estado  (*Configuración del usuario*).

## Selección de un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security

Para aplicaciones que se iniciaron antes de Kaspersky Endpoint Security, solamente se supervisa la actividad de red. El control se realiza utilizando las reglas de red definidas en la configuración de Firewall. Para especificar qué reglas de red se deben aplicar a la supervisión de la actividad de red para dichas aplicaciones, debe seleccionar un grupo de confianza.

### Cómo seleccionar un grupo de confianza para las aplicaciones que se inicien antes que Kaspersky Endpoint Security mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones**, haga clic en el botón **Modificar**.
7. Seleccione un grupo de confianza para el ajuste **Las aplicaciones que se inicien antes que Kaspersky Endpoint Security para Windows se moverán automáticamente a este grupo de confianza**.
8. Guarde los cambios.

### Cómo seleccionar un grupo de confianza para las aplicaciones que se inicien antes que Kaspersky Endpoint Security mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas → Prevención de intrusiones en el host**.
5. Seleccione un grupo de confianza para el ajuste **Las aplicaciones que se inicien antes que Kaspersky Endpoint Security para Windows se moverán automáticamente a este grupo de confianza**.
6. Guarde los cambios.

### Cómo seleccionar un grupo de confianza para las aplicaciones que se inicien antes que Kaspersky Endpoint Security mediante la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
3. Seleccione un grupo de confianza en el bloque **Las aplicaciones que se inicien antes que Kaspersky Endpoint Security para Windows se moverán automáticamente a este grupo de confianza**.
4. Guarde los cambios.

Como resultado, cualquier aplicación que se inicie antes que Kaspersky Endpoint Security se ubicará en el grupo de confianza que acaba de definir. Kaspersky Endpoint Security bloqueará las acciones de la aplicación tomando como criterio este grupo.

## Selección del grupo de confianza para aplicaciones desconocidas

Cuando una aplicación se ejecuta por primera vez, el componente Prevención de intrusiones en el host la asigna a un grupo de confianza. De manera predeterminada, cuando una aplicación no está registrada en Kaspersky Security Network, se la agrega al grupo Restricción mínima. Lo mismo ocurre cuando el equipo no tiene acceso a Internet. Si KSN incorpora, en algún momento, datos sobre una aplicación que originariamente se consideró desconocida, Kaspersky Endpoint Security modificará los derechos de la misma. De ocurrir esto, podrá modificar los derechos manualmente.

**Cómo seleccionar el grupo de confianza para aplicaciones desconocidas mediante la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la lista desplegable **Grupo de confianza para las aplicaciones que no pudieron agregarse a grupos ya existentes** para seleccione el grupo de confianza que desee.

   Si ha optado por participar en Kaspersky Security Network, cada vez ejecuta una aplicación, Kaspersky Endpoint Security envía una consulta a KSN para determinar la reputación de la misma. En función de la respuesta recibida, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración del componente Prevención contra intrusos.
7. Utilice la casilla **Actualizar derechos para aplicaciones anteriormente desconocidas usando las bases de datos de KSN** para determinar si los derechos de las aplicaciones desconocidas deberán actualizarse automáticamente.
8. Guarde los cambios.

Cómo seleccionar el grupo de confianza para aplicaciones desconocidas mediante Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la lista desplegable **Grupo de confianza para las aplicaciones que no pudieron agregarse a grupos ya existentes** para seleccione el grupo de confianza que desee.

   Si ha optado por participar en Kaspersky Security Network, cada vez ejecuta una aplicación, Kaspersky Endpoint Security envía una consulta a KSN para determinar la reputación de la misma. En función de la respuesta recibida, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración del componente Prevención contra intrusos.
6. Utilice la casilla **Actualizar derechos para aplicaciones anteriormente desconocidas usando las bases de datos de KSN** para determinar si los derechos de las aplicaciones desconocidas deberán actualizarse automáticamente.
7. Guarde los cambios.

Cómo seleccionar el grupo de confianza para aplicaciones desconocidas mediante la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.
3. En el bloque **Grupo de confianza para las aplicaciones desconocidas**, seleccione el grupo de confianza correspondiente.

   Si ha optado por participar en Kaspersky Security Network, cada vez ejecuta una aplicación, Kaspersky Endpoint Security envía una consulta a KSN para determinar la reputación de la misma. En función de la respuesta recibida, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración del componente Prevención contra intrusos.
4. Utilice la casilla **Actualizar derechos para aplicaciones anteriormente desconocidas usando las bases de datos de KSN** para determinar si los derechos de las aplicaciones desconocidas deberán actualizarse automáticamente.
5. Guarde los cambios.

## Selección del grupo de confianza para aplicaciones con firma digital

Kaspersky Endpoint Security siempre coloca las aplicaciones firmadas por certificados de Microsoft Office o Kaspersky en el grupo de confianza.

**Cómo seleccionar un grupo de confianza para las aplicaciones con firma digital mediante la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la casilla **Confiar en aplicaciones que tienen firma digital** para indicar si las aplicaciones que tengan la firma digital de un proveedor de confianza deberán asignarse automáticamente al grupo De confianza.

   Se considera proveedor de confianza a todo aquel que Kaspersky ha incluido en el grupo de confianza. Si lo desea, puede agregar manualmente el certificado de un proveedor al almacén de confianza de certificados del sistema.

   Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que las aplicaciones con firma digital sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.
7. Guarde los cambios.

**Cómo seleccionar un grupo de confianza para las aplicaciones con firma digital mediante Web Console y Cloud Console**

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la casilla **Confiar en aplicaciones que tienen firma digital** para indicar si las aplicaciones que tengan la firma digital de un proveedor de confianza deberán asignarse automáticamente al grupo De confianza.

   Se considera proveedor de confianza a todo aquel que Kaspersky ha incluido en el grupo de confianza. Si lo desea, puede agregar manualmente el certificado de un proveedor al almacén de confianza de certificados del sistema.

   Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que las aplicaciones con firma digital sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.
6. Guarde los cambios.

**Cómo seleccionar un grupo de confianza para las aplicaciones con firma digital mediante la interfaz de la aplicación**

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.
3. En el bloque **Reglas de procesamiento de aplicaciones**, utilice la casilla **Confiar en aplicaciones que tienen firma digital** para indicar si las aplicaciones que tengan la firma digital de un proveedor de confianza deberán asignarse automáticamente al grupo De confianza.

   Se considera proveedor de confianza a todo aquel que Kaspersky ha incluido en el grupo de confianza. Si lo desea, puede agregar manualmente el certificado de un proveedor al almacén de confianza de certificados del sistema.

   Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que las aplicaciones con firma digital sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará.
4. Guarde los cambios.

## Administración de los derechos de las aplicaciones

Por defecto, la actividad de una aplicación se controla a través de los derechos de aplicaciones definidos para el grupo de confianza al que la aplicación pertenece. El grupo de confianza de una aplicación se determina cuando se la ejecuta por primera vez. Si lo necesita, puede modificar los derechos de todo un grupo de confianza, de una aplicación individual o de un grupo de aplicaciones pertenecientes a un grupo de confianza determinado.

Los derechos que se definen manualmente tienen mayor prioridad que los que se han determinado para un grupo de confianza. En otras palabras, cuando una aplicación tiene derechos que se han definido para ella manualmente y derechos que ha heredado de su grupo de confianza, el componente Prevención de intrusiones en el host toma como válidos los derechos definidos manualmente y controla la actividad de la aplicación basándose en ellos.

Las reglas que se crean para una aplicación son heredadas por las aplicaciones secundarias. Esto quiere decir, por ejemplo, que si bloquea por completo las actividades de red para cmd.exe, el acceso a la red también estará bloqueado para notepad.exe si dicho programa se inicia a través de cmd.exe. Cuando una aplicación es iniciada de manera indirecta por otra, pero esta primera aplicación no es secundaria de la que la inició, la aplicación iniciada en forma indirecta no hereda ninguna regla.

Cómo cambiar los derechos de una aplicación 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones**, haga clic en el botón **Agregar**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
7. Seleccione la ficha **Derechos de aplicaciones**.
8. Haga clic en el botón **Agregar**.
9. En la ventana que se abre, escriba un criterio de búsqueda para dar con la aplicación cuyos derechos desee cambiar.

   Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
10. Haga clic en el botón **Actualizar**.

    Kaspersky Endpoint Security buscará la aplicación en una lista consolidada, en la que se recogen las aplicaciones instaladas en los equipos administrados. Las aplicaciones que coincidan con los criterios de búsqueda se mostrarán en una lista.
11. Seleccione la aplicación necesaria.
12. En la lista desplegable **Agregar las aplicaciones seleccionadas al grupo <grupo de confianza>**, seleccione **Grupos por defecto** y haga clic en **Aceptar**.

    La aplicación se agregará al grupo por defecto.
13. Seleccione la aplicación de su interés, abra al menú contextual de la misma y haga clic en el elemento **Derechos de la aplicación**.

    Se abren las propiedades de la aplicación.
14. Realice una de las siguientes acciones:

    - Abra la pestaña **Archivos y Registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.
    - Abra la pestaña **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

    Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

15. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Autorizar** (✓) o **Rechazar** (⊘).

16. Seleccione la opción **Guardar en informe** (✓ / ⊘) si le interesa monitorear cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

17. Guarde los cambios.

[Cómo cambiar los derechos de una aplicación mediante Web Console y Cloud Console]

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
6. Seleccione la ficha **Derechos de aplicaciones**.

   Verá una lista de grupos de confianza en el lado izquierdo de la ventana. Las propiedades de estos grupos se mostrarán en el lado derecho.
7. Haga clic en el botón **Agregar**.

   Se inicia un asistente para agregar la aplicación a un grupo de confianza.
8. Haga clic en el vínculo **Grupo de destino seleccionado** para elegir el grupo de confianza para la aplicación.
9. Seleccione el tipo **Aplicación**. Haga clic en **Siguiente**.

   Para cambiar el grupo de confianza de más de una aplicación, seleccione el tipo **Grupo** y escriba un nombre para el grupo de aplicaciones.
10. En la lista de aplicaciones que se abre, seleccione las aplicaciones cuyos derechos desee cambiar.

    Utilice un filtro. Puede introducir el nombre de la aplicación o el nombre de su desarrollador. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
11. Haga clic en **Aceptar** para cerrar el asistente.

    La aplicación se agregará al grupo de confianza.
12. En la parte izquierda de la ventana, seleccione la aplicación de su interés.
13. En la parte derecha de la ventana, en la lista desplegable, realice una de las siguientes acciones:

    - Seleccione **Archivos y Registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.
    - Seleccione **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.

    Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.
14. Busque el recurso en el que esté interesado y seleccione una opción en la columna con la acción pertinente: **Heredar**, **Autorizar** (✓) o **Rechazar** (✗).

15. Seleccione la opción **Guardar en informe** ( / ) si le interesa monitorear cómo se utilizan los recursos del equipo.

    Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

16. Guarde los cambios.

[Cómo cambiar los derechos de una aplicación mediante la interfaz de la aplicación]

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **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 necesaria.
5. En el menú contextual de la aplicación, seleccione **Detalles y reglas**.

   Se abren las propiedades de la aplicación.
6. Realice una de las siguientes acciones:

   - Abra la pestaña **Archivos y Registro del sistema** para cambiar las operaciones que las aplicaciones del grupo podrán realizar con el Registro del sistema operativo, los archivos de los usuarios y la configuración de las aplicaciones.
   - Abra la pestaña **Derechos** para modificar los derechos que rigen el acceso de las aplicaciones del grupo a los procesos y objetos del sistema operativo.
7. Busque el recurso en el que esté interesado y haga clic con el botón derecho en la columna de la acción que quiera modificar. En el menú contextual que se abrirá, seleccione una opción: **Heredar**, **Autorizar** (✓) o **Rechazar** (!).
8. Seleccione la opción **Guardar en informe** (📊) si le interesa monitorear cómo se utilizan los recursos del equipo.

   Si habilita esta opción, Kaspersky Endpoint Security guardará información sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.
9. Seleccione la pestaña **Exclusiones** y configure los parámetros avanzados de la aplicación (vea la tabla de más abajo).
10. Guarde los cambios.

Parámetros avanzados de la aplicación

| Parámetro | Descripción |
|---|---|
| **No analizar archivos abiertos** | Kaspersky Endpoint Security no analizará ningún archivo que la aplicación abra. Por ejemplo, si utiliza aplicaciones para realizar copias de seguridad de archivos, esta función ayuda a reducir el consumo de recursos de Kaspersky Endpoint Security. |
| **No supervisar la actividad de la aplicación** | Kaspersky Endpoint Security no supervisará la actividad de la red y los archivos de la aplicación en el sistema operativo. La actividad de la aplicación se supervisa través de los siguientes componentes: Detección de comportamiento, Prevención de exploits, Prevención de intrusiones en el host, Motor de reparación y Firewall. |
| **No heredar restricciones del proceso principal (aplicación)** | Kaspersky Endpoint Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal lo inicia una aplicación para la que se configuran los derechos de aplicaciones (Prevención de intrusiones en el host) y las reglas de red de aplicaciones (Firewall). |
| **No se** | Kaspersky Endpoint Security no supervisará las actividades de red ni las |

| | |
|---|---|
| **supervisa la actividad de aplicaciones secundarias** | operaciones de archivo que realicen las aplicaciones iniciadas por la aplicación. |
| **Permitir la interacción con la interfaz de Kaspersky Endpoint Security** | La Autoprotección de Kaspersky Endpoint Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona esta casilla, se permite que la aplicación de acceso remoto administre la configuración de Kaspersky Endpoint Security a través de la interfaz de Kaspersky Endpoint Security. |
| **No analizar el tráfico cifrado / No analizar todo el tráfico** | Kaspersky Endpoint Security no analizará el tráfico de red que tenga origen en la aplicación. Puede excluir de los análisis todo el tráfico o solo el tráfico cifrado. También puede excluir direcciones IP y números de puerto individuales de los análisis. |

## Protección de recursos del sistema operativo y datos personales

El componente Prevención contra intrusos administra los derechos de aplicaciones de realizar acciones en varias categorías de recursos del sistema operativo y datos personales. Los especialistas de Kaspersky han establecido categorías predefinidas de recursos protegidos. Por ejemplo, la categoría *Sistema operativo* tiene una subcategoría llamada *Configuración de inicio*, en la que se reúnen todas las claves del Registro asociadas a la autoejecución de aplicaciones. No puede modificar ni eliminar las categorías predefinidas de recursos protegidos o los recursos protegidos que están dentro de estas categorías.

**Cómo agregar un recurso protegido mediante la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Derechos de aplicaciones**, haga clic en el botón **Agregar**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
7. Seleccione la pestaña **Recursos protegidos**.

   En la parte izquierda de la ventana, verá una lista de recursos protegidos; los derechos para acceder a esos recursos estarán en el lado derecho. Los derechos varían según el grupo de confianza.
8. Seleccione la categoría de recursos protegidos a los que desea agregar un nuevo recurso protegido.

   Si desea agregar una subcategoría, haga clic en **Agregar → Categoría**.
9. Haga clic en el botón **Agregar**. En la lista desplegable, seleccione el tipo de recurso que desee agregar: **Archivo o carpeta** o **Clave del Registro**.
10. En la ventana que se abre, seleccione un archivo, una carpeta o una clave del registro.

    Puede ver cuáles son los derechos con los que cuentan las aplicaciones para acceder a los recursos agregados. Si selecciona un recurso en la parte izquierda de la ventana, Kaspersky Endpoint Security le mostrará los derechos de acceso correspondientes a cada grupo de confianza. Si no necesita controlar el uso que las aplicaciones hagan de un recurso nuevo, utilice la casilla ubicada junto al recurso en cuestión.
11. Guarde los cambios.

[Cómo agregar un recurso protegido 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. Seleccione **Protección avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Derechos de aplicaciones y recursos protegidos**, haga clic en el vínculo **Derechos de aplicaciones y recursos protegidos**.

   Se abre una ventana que permite configurar los derechos de las aplicaciones. La ventana contiene, además, una lista de recursos protegidos.
6. Seleccione la pestaña **Recursos protegidos**.

   En la parte izquierda de la ventana, verá una lista de recursos protegidos; los derechos para acceder a esos recursos estarán en el lado derecho. Los derechos varían según el grupo de confianza.
7. Haga clic en el botón **Agregar**.

   Se abre el asistente para agregar recursos.
8. Haga clic en el vínculo **Nombre del grupo** para seleccionar la categoría de recursos protegidos a la que se agregará el nuevo recurso protegido.

   Si desea agregar una subcategoría, seleccione la opción **Categoría de recursos protegidos**.
9. Seleccione el tipo de recurso que desea agregar: **archivo o carpeta** o **Clave del Registro** .
10. Seleccione un archivo, una carpeta o una clave del Registro.
11. Haga clic en **Aceptar** para cerrar el asistente.

    Puede ver cuáles son los derechos con los que cuentan las aplicaciones para acceder a los recursos agregados. Si selecciona un recurso en la parte izquierda de la ventana, Kaspersky Endpoint Security le mostrará los derechos de acceso correspondientes a cada grupo de confianza. Si no necesita controlar el uso que las aplicaciones hagan de los recursos, utilice la casilla ubicada en la columna **Estado**.
12. Guarde los cambios.

Cómo agregar un recurso protegido mediante la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **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 agregar un nuevo recurso protegido.

   Si desea agregar una subcategoría, haga clic en **Agregar** → **Categoría**.
5. Haga clic en el botón **Agregar**. En la lista desplegable, seleccione el tipo de recurso que desee agregar: **Archivo o carpeta** o **Clave del Registro**.
6. En la ventana que se abre, seleccione un archivo, una carpeta o una clave del registro.

   Puede ver cuáles son los derechos con los que cuentan las aplicaciones para acceder a los recursos agregados. Si selecciona un recurso en la parte izquierda de la ventana, Kaspersky Endpoint Security le mostrará una lista de aplicaciones con sus correspondientes derechos de acceso. Si no necesita controlar el uso que las aplicaciones hagan de los recursos, utilice el botón **Deshabilitar control** (), ubicado en la columna **Estado**.
7. Guarde los cambios.

Kaspersky Endpoint Security controlará el acceso a los recursos del sistema operativo y a los datos personales especificados. El acceso de las aplicaciones a cada recurso variará en función del grupo de confianza al que pertenezca la aplicación. El grupo de confianza de una aplicación puede modificarse.

## Eliminación de la información sobre las aplicaciones en desuso

En Kaspersky Endpoint Security, las actividades de las aplicaciones se controlan a través de derechos. Los derechos de una aplicación están determinados por su grupo de confianza. El grupo de confianza en el que Kaspersky Endpoint Security coloca una aplicación se determina cuando esta se ejecuta por primera vez. El grupo de confianza puede cambiarse manualmente. También es posible configurar manualmente los derechos de una aplicación específica. Kaspersky Endpoint Security almacena los derechos y el grupo de confianza de cada aplicación.

Para conservar recursos, Kaspersky Endpoint Security elimina automáticamente la información de las aplicaciones que ya no se utilizan. La información se elimina según las siguientes reglas:

- Cuando el grupo de confianza y los derechos de una aplicación se determinaron automáticamente, Kaspersky Endpoint Security elimina la información de esa aplicación luego de 30 días. El plazo de almacenamiento de la información no se puede modificar, y tampoco es posible desactivar la eliminación automática.
- Cuando el grupo de confianza o los derechos de acceso de una aplicación se determinaron manualmente, Kaspersky Endpoint Security elimina la información de esa aplicación después de 60 días (este es el plazo de almacenamiento predeterminado). En este caso, el plazo de almacenamiento sí puede modificarse, y también es posible desactivar la eliminación automática (encontrará instrucciones para tal fin más abajo).

Cuando inicie una aplicación cuya información se haya eliminado, Kaspersky Endpoint Security la analizará como si fuera la primera vez que se la ejecuta.

[Cómo configurar la eliminación automática de información vinculada a aplicaciones en desuso mediante la Consola de administración (MMC)]

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
6. En el bloque **Reglas de procesamiento de aplicaciones**, realice una de las siguientes acciones:
   - Si desea configurar la eliminación automática, active la casilla **Eliminar los derechos de las aplicaciones que no se inicien en más de N días** y especifique un número de días.

     Transcurrido el número de días que especifique, Kaspersky Endpoint Security eliminará la información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente. La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado automáticamente se eliminará luego de treinta días.
   - Si desea desactivar la eliminación automática, desactive la casilla **Eliminar los derechos de las aplicaciones que no se inicien en más de N días**.

     La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente se conservará por tiempo indefinido (es decir, el plazo de almacenamiento será ilimitado). Kaspersky Endpoint Security únicamente eliminará (luego de treinta días) la información de las aplicaciones cuyo grupo de confianza o cuyos derechos se hayan determinado automáticamente.
7. Guarde los cambios.

[Cómo configurar la eliminación automática de información vinculada a aplicaciones en desuso mediante Web Console y Cloud Console]

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Prevención de intrusiones en el host**.
5. En el bloque **Reglas de procesamiento de aplicaciones**, realice una de las siguientes acciones:

   - Si desea configurar la eliminación automática, active la casilla **Eliminar los derechos de las aplicaciones que no se inicien en más de N días** y especifique un número de días.

     Transcurrido el número de días que especifique, Kaspersky Endpoint Security eliminará la información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente. La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado automáticamente se eliminará luego de treinta días.

   - Si desea desactivar la eliminación automática, desactive la casilla **Eliminar los derechos de las aplicaciones que no se inicien en más de N días**.

     La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente se conservará por tiempo indefinido (es decir, el plazo de almacenamiento será ilimitado). Kaspersky Endpoint Security únicamente eliminará (luego de treinta días) la información de las aplicaciones cuyo grupo de confianza o cuyos derechos se hayan determinado automáticamente.
6. Guarde los cambios.

[Cómo configurar la eliminación automática de información vinculada a aplicaciones en desuso mediante la interfaz de la aplicación]

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Prevención de intrusiones en el host**.
3. En el bloque **Reglas de procesamiento de aplicaciones**, realice una de las siguientes acciones:
   - Si desea configurar la eliminación automática, active la casilla **Eliminar los derechos de las aplicaciones que no se inicien en más de N días** y especifique un número de días.

     Transcurrido el número de días que especifique, Kaspersky Endpoint Security eliminará la información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente. La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado automáticamente se eliminará luego de treinta días.
   - Si desea desactivar la eliminación automática, desactive la casilla **Eliminar los derechos de las aplicaciones que no se inicien en más de N días**.

     La información de las aplicaciones cuyo grupo de confianza o cuyos derechos de acceso se hayan determinado manualmente se conservará por tiempo indefinido (es decir, el plazo de almacenamiento será ilimitado). Kaspersky Endpoint Security únicamente eliminará (luego de treinta días) la información de las aplicaciones cuyo grupo de confianza o cuyos derechos se hayan determinado automáticamente.
4. Guarde los cambios.

## Monitoreo de Prevención de intrusiones en el host

La aplicación puede generar informes sobre el funcionamiento del componente Prevención de intrusiones en el host. En los informes generados, encontrará un registro de las operaciones permitidas o bloqueadas que la aplicación realice con los recursos del equipo. También hallará información sobre las aplicaciones que utilicen cada recurso.

Si desea monitorear las operaciones de Prevención de intrusiones en el host, active la creación de informes. Por ejemplo, puede habilitar el reenvío de los informes generados para aplicaciones específicas en la configuración del componente Prevención de intrusiones en el host.

A la hora de configurar el monitoreo, tenga en cuenta que reenviar eventos a Kaspersky Security Center significará más tráfico en la red. Si lo desea, puede optar por guardar los informes únicamente en el registro local de Kaspersky Endpoint Security.

## Protección del acceso a dispositivos de audio y video

Existen programas especiales que pueden darle a un atacante la capacidad de acceder a los dispositivos de grabación de audio y video de un equipo (por ejemplo, a los micrófonos y las cámaras web).
Kaspersky Endpoint Security puede detectar si una aplicación está recibiendo una señal de audio o de video y proteger esa información si la aplicación no está autorizada a captarla.

De manera predeterminada, Kaspersky Endpoint Security restringe el acceso a las señales de audio y video basándose en la categoría de la aplicación que busca acceder a ese contenido:

- Las aplicaciones de los grupos De confianza y Restricción mínima tienen permitido recibir las señales de audio y video de los dispositivos (por defecto).
- Las aplicaciones de los grupos Restricción máxima y No confiables no tienen permitido recibir las señales de audio y video de los dispositivos (por defecto).

Si necesita que una aplicación específica reciba una señal de audio o de video, puede brindarle acceso manualmente.

## Particularidades de la protección de audio

La protección de audio tiene las siguientes particularidades:

- Para que la característica funcione, el componente Prevención de intrusiones en el host debe estar habilitado.
- Si la aplicación comenzó a recibir la transmisión de audio antes de que se iniciara el componente Prevención contra intrusos, Kaspersky Endpoint Security permitirá que la aplicación reciba la transmisión de audio y no mostrará ninguna notificación.
- Si una aplicación se mueve al grupo No confiables o al grupo Restricción máxima una vez que ya ha comenzado a recibir una señal de audio, Kaspersky Endpoint Security no impedirá que la aplicación acceda a la señal de audio y no mostrará ninguna notificación al respecto.
- Si modifica los ajustes que rigen el acceso de una aplicación a los dispositivos de grabación de audio (por ejemplo, si prohíbe que la aplicación acceda a la señal de audio), deberá reiniciar dicha aplicación para que esta deje de tener acceso a la señal de audio.
- El control del acceso a la transmisión de audio desde dispositivos para grabar sonido no depende de la configuración de acceso a la cámara web de la aplicación.
- Kaspersky Endpoint Security protege el acceso solo a micrófonos incorporados y micrófonos externos. Los demás dispositivos de transmisión de audio no son compatibles.
- Kaspersky Endpoint Security no puede garantizar la protección de una transmisión de audio desde dispositivos como cámaras DSLR, videocámaras portátiles y cámaras de acción.
- Cuando ejecute aplicaciones de grabación o reproducción de audio y video por primera vez después de instalar Kaspersky Endpoint Security, es posible que se interrumpa la grabación o reproducción de audio y video. Esto es necesario a fin de habilitar la funcionalidad que controla el acceso de las aplicaciones a dispositivos para grabar audio. El servicio del sistema que controla el hardware de audio se reiniciará cuando se ejecute Kaspersky Endpoint Security por primera vez.

## Particularidades de la protección de acceso a la cámara web

La funcionalidad de protección de acceso a cámaras web tiene las siguientes consideraciones especiales y limitaciones:

- La aplicación controla video e imágenes fijas derivadas del procesamiento de datos de una cámara web.
- La aplicación controla la transmisión de audio si forma parte de la transmisión de video recibida de la cámara web.

- La aplicación controla solamente las cámaras web conectadas por medio de USB o IEEE1394 que se indican como **Dispositivos de imágenes** en el Administrador de dispositivos de Windows.
- Kaspersky Endpoint Security admite las siguientes cámaras web:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  Kaspersky no puede garantizar la compatibilidad con las cámaras web que no se especifican en esta lista.

## Motor de reparación

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

Al revertir la actividad del malware en el sistema operativo, Kaspersky Endpoint Security gestiona los siguientes tipos de actividad de malware:

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red).
  - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado.
  - Restaura los archivos que el malware ha modificado o eliminado.

  La capacidad de recuperar archivos está sujeta a algunas limitaciones.

- **Actividad del Registro**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina las claves del Registro que el malware ha creado.
  - No restaura las claves del Registro que el malware ha eliminado o modificado.

- **Actividad del sistema**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Finaliza los procesos iniciados por el malware.
  - Finaliza los procesos en los cuales ha penetrado una aplicación malintencionada.
  - No reanuda procesos que el malware haya suspendido.

- **Actividad de 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.

La reversión de las operaciones del malware afecta a un conjunto de datos estrictamente definido. La reversión no tiene efectos negativos en el sistema operativo ni en la integridad de los datos de su equipo.

**Cómo habilitar o deshabilitar el componente Motor de reparación mediante la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, vaya a **Protección avanzada contra amenazas** → **Motor de reparación**.
6. Use la casilla **Motor de reparación** para habilitar o deshabilitar el componente.
7. Guarde los cambios.

**Cómo habilitar o deshabilitar el componente Motor de reparación mediante Web Console y Cloud Console**

1. En la ventana principal de Web Console, seleccione **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 avanzada contra amenazas** → **Motor de reparación**.
5. Use el interruptor **Motor de reparación** para habilitar o deshabilitar el componente.
6. Guarde los cambios.

Cómo habilitar o deshabilitar el componente Motor de reparación mediante la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Motor de reparación**.
3. Use el interruptor **Motor de reparación** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

De esta manera, si la opción Motor de reparación está habilitada, Kaspersky Endpoint Security revertirá las acciones realizadas por aplicaciones maliciosas en el sistema operativo.

## Kaspersky Security Network

A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

*Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, 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 invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios pueden iniciar o discontinuar su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el sitio web de Kaspersky contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. Encontrará el texto de la Declaración de Kaspersky Security Network en el archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación.

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.* A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky Security Network, así como a otras clases de información estadística, sin enviar información de sus equipos a KSN. 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 manera predeterminada, Kaspersky Security Center utiliza KSN Global. Si desea utilizar KSN Privada, puede hacer los cambios de configuración pertinentes con la Consola de administración (MMC), a través de Kaspersky Security Center 12 Web Console o desde la línea de comandos. No es posible usar Kaspersky Security Center Cloud Console para este fin.

Para más información sobre KSN Privada, consulte la documentación de Kaspersky Private Security Network.

### Proxy de KSN

Los equipos de usuarios administrados por el Servidor de administración de Kaspersky Security Center pueden interactuar con KSN a través del servicio Proxy de KSN.

El servicio Proxy de KSN ofrece las siguientes capacidades:

- El equipo del usuario puede consultar KSN y enviarle información, incluso sin 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 *Guía de ayuda de Kaspersky Security Center*.

## Habilitación y deshabilitación del uso de Kaspersky Security Network

*Para habilitar o deshabilitar el uso de Kaspersky Security Network:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Protección avanzada contra amenazas** → **Kaspersky Security Network**.

3. Utilice el interruptor **Kaspersky Security Network** para habilitar o deshabilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Endpoint Security mostrará la Declaración de Kaspersky Security Network. Lea los términos de la Declaración de Kaspersky Security Network (KSN) y, si está de acuerdo con los mismos, acéptelos.

   De manera predeterminada, Kaspersky Endpoint Security utiliza el modo KSN extendido. El *modo KSN extendido* es un modo por el cual Kaspersky Endpoint Security remite información adicional a Kaspersky.

4. De ser necesario, desactive el interruptor **Habilitar el modo KSN extendido**.

5. Guarde los cambios.

De esta manera, si el uso de KSN está habilitado, Kaspersky Endpoint Security usa información sobre la reputación de los archivos, los recursos web y las aplicaciones recibida de Kaspersky Security Network.

## Limitaciones de KSN privada

KSN Privada (en lo sucesivo, también denominada 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 agregado a la base de datos de reputación local tiene mayor prioridad que uno agregado a KSN/KPSN. Por ejemplo, imagine que Kaspersky Endpoint Security está analizando un equipo y solicita la reputación de un archivo en KSN/KPSN. Si el archivo tiene una reputación "no confiable" en la base de datos de reputación local, pero tiene una reputación "confiable" en KSN/KPSN, Kaspersky Endpoint Security detectará el archivo como "no confiable" y realizará la acción definida para las amenazas detectadas.

Sin embargo, en algunos casos, es posible que Kaspersky Endpoint Security no solicite la reputación de un objeto en KSN/KPSN. Si este es el caso, Kaspersky Endpoint Security no recibirá datos de la base de datos de reputación local de KPSN. Es posible que Kaspersky Endpoint Security no solicite la reputación de un objeto en KSN/KPSN por las siguientes razones:

- Las aplicaciones de Kaspersky utilizan bases de datos de reputación sin conexión. Las bases de datos de reputación sin conexión están diseñadas para optimizar los recursos durante el funcionamiento de las aplicaciones de Kaspersky y para proteger los objetos de importancia crítica en el equipo. Expertos de Kaspersky se encargan de crear las bases de datos de reputación sin conexión basándose en datos de Kaspersky Security Network. Las aplicaciones de Kaspersky actualizan las bases de datos de reputación sin conexión con bases de datos antivirus de la aplicación específica. Si las bases de datos de reputación sin conexión contienen información sobre un objeto que se está analizando, la aplicación no solicita la reputación de este objeto a KSN/KPSN.

- Las exclusiones de análisis (zona de confianza) se configuran en la configuración de la aplicación. Si este es el caso, la aplicación no tiene en cuenta la reputación del objeto en la base de datos de reputación local.

- La aplicación 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 definir la configuración de optimización del análisis en la interfaz de la aplicación, por ejemplo, para el componente Protección contra archivos peligrosos.

## Habilitación y deshabilitación del modo nube para los componentes de protección

*Modo nube* es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky.

Al utilizar Kaspersky Private Security Network, la funcionalidad del modo nube está disponible para versiones superiores o iguales a Kaspersky Private Security Network versión 3.0.

*Para habilitar o deshabilitar el modo nube para los componentes de protección:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Protección avanzada contra amenazas → Kaspersky Security Network**.
3. Use el interruptor **Habilitar modo nube** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

   De esta manera, Kaspersky Endpoint Security descargará una versión ligera o una versión completa de las bases de datos antivirus durante la próxima actualización.

Si la versión ligera de bases de datos antivirus no está disponible para ser utilizada, Kaspersky Endpoint Security cambia automáticamente la versión premium de bases de datos antivirus.

## Verificación de la conexión con Kaspersky Security Network

La conexión a Kaspersky Security Network se puede perder por los siguientes motivos:

- No participa en Kaspersky Security Network;
- Su equipo no está conectado a Internet;
- El estado actual de la clave no permite la conexión con Kaspersky Security Network. Por ejemplo, una conexión a KSN puede no estar disponible debido a las siguientes razones:
  - La aplicación no está activada.
  - La licencia o la suscripción han caducado.
  - Se han identificado problemas de claves de licencia (por ejemplo, la clave se ha agregado a la lista de claves prohibidas).

*Para verificar la conexión con Kaspersky Security Network:*

En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Kaspersky Security Network**.

Se abre la ventana **Kaspersky Security Network**, en la que se muestra información sobre la actividad de Kaspersky Security Network. Las estadísticas de uso de KSN se descargan al momento de abrir la ventana **Kaspersky Security Network**. Las estadísticas globales de la infraestructura del servicio en la nube de Kaspersky Security Network y la hora de sincronización no se actualizan en tiempo real.

En la parte izquierda de la ventana **Kaspersky Security Network**, verá en qué estado se encuentra la conexión entre el equipo y Kaspersky Security Network. Los valores posibles son los siguientes:

- *Habilitada.*

  Este estado significa que Kaspersky Security Network se está utilizando en las operaciones de Kaspersky Endpoint Security, y que los servidores de KSN están disponibles.

- *Habilitada. Disponible con restricciones.*

  Este estado significa que Kaspersky Security Network se está utilizando en las operaciones de Kaspersky Endpoint Security, y que los servidores de KSN no están disponibles.

  Es posible que los servidores de KSN no estén disponibles debido a las siguientes razones:

  - El servicio de proxy de KSN (ksnproxy) se está ejecutando en el equipo.
  - El firewall bloquea el puerto 13111.

  Si el tiempo transcurrido desde la última sincronización con los servidores KSN es superior a 15 minutos o muestra el estado *Desconocido*, esto quiere decir que el estado de la conexión de Kaspersky Endpoint Security con Kaspersky Security Network toma el valor *Habilitada. No disponible*.

- *Desactivado.*

  Este estado significa que Kaspersky Security Network se está utilizando en las operaciones de Kaspersky Endpoint Security.

Si no es posible restaurar la conexión con los servidores de Kaspersky Security Network, le recomendamos que se ponga en contacto con el Servicio de soporte técnico o con su proveedor de servicios.

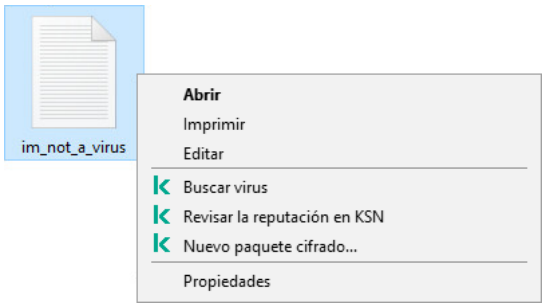
## Comprobación de la reputación de un archivo en Kaspersky Security Network

Si no sabe con certeza si un archivo es seguro, puede buscar su reputación en Kaspersky Security Network.

Para buscar la reputación de un archivo, debe aceptar los términos de la Declaración de Kaspersky Security Network.

*Para comprobar la reputación de un archivo en Kaspersky Security Network:*

Abra el menú contextual del archivo y elija la opción **Revisar la reputación en KSN** (vea la siguiente imagen).




Menú contextual del archivo

Kaspersky Endpoint Security muestra la reputación del archivo:

**De confianza**. La mayoría de los usuarios de Kaspersky Security Network confirman que el archivo es seguro.

**Software con fines lícitos que podría usarse para provocar daños en el equipo o en sus datos**. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre el software legal que los delincuentes pueden utilizar para dañar el equipo o los datos personales están disponibles en la Enciclopedia de Kaspersky. Estas aplicaciones pueden agregarse a la lista de aplicaciones de confianza.

**No confiables**. El archivo es un virus u otra clase de aplicación que supone un riesgo.

**Desconocida**. Kaspersky Security Network no cuenta con información sobre el archivo. Si desea analizarlo con las bases de datos antivirus, use la opción **Buscar virus** del menú contextual.

Kaspersky Endpoint Security mostrará qué solución de KSN se usó para determinar la reputación del archivo. Los valores posibles son *KSN Global* y *KSN Privada*.

Kaspersky Endpoint Security también mostrará información adicional sobre el archivo (vea la siguiente imagen).


Reputación de un archivo en Kaspersky Security Network

## Análisis de conexiones cifradas

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

Cuando termina la instalación de Kaspersky Endpoint Security, se agrega un certificado de Kaspersky al repositorio de certificados de confianza del sistema (tienda de certificados de Windows). El uso de este repositorio también se habilita en Firefox y Thunderbird para que el tráfico de estas aplicaciones pueda analizarse.

Los componentes Control Web, Protección contra amenazas de correo, Protección contra amenazas web pueden descifrar y analizar el tráfico de red que se transmite sobre conexiones cifradas en las que se utilizan los siguientes protocolos:

- SSL 3.0
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

## Configuración los parámetros del análisis de conexiones cifradas.

*Para configurar las opciones de análisis para conexiones cifradas:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección Análisis de conexiones cifradas, seleccione el modo de análisis de conexiones cifradas:
   - **No analizar las conexiones cifradas** Kaspersky Endpoint Security no tendrá acceso al contenido de los sitios web cuyas direcciones comienzan con `https://`.
   - **Analizar las conexiones cifradas si lo solicitan los componentes de protección**. Kaspersky Endpoint Security escaneará solo el tráfico cifrado cuando lo soliciten los componentes Protección contra archivos peligrosos, Protección contra amenazas de correo y Control Web.
   - **Analizar siempre las conexiones cifradas** Kaspersky Endpoint Security analizará el tráfico de red cifrado aunque los componentes de protección estén deshabilitados.

   Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por aplicaciones de confianza para las que el análisis de tráfico está desactivado. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza únicamente en la interfaz de Kaspersky Endpoint Security. No puede verla en la Consola de Kaspersky Security Center.
4. De ser necesario, agregue exclusiones de análisis para las direcciones y aplicaciones que considere de confianza.
5. Haga clic en el botón **Configuración avanzada**.
6. Configure los parámetros del análisis de conexiones cifradas (vea la tabla a continuación).
7. Guarde los cambios.

Parámetros del análisis de conexiones cifradas

| Parámetro | Descripción |
|---|---|
| **Cuando se visite un** | • **Permitir**. Cuando se elige esta opción y se visita un dominio cuyo certificado no es |

| | |
|---|---|
| **dominio cuyo certificado no sea de confianza** | de confianza, Kaspersky Endpoint Security permite que se establezca la conexión de red.<br><br>Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para advertirle que acceder a ese dominio en particular no es recomendable e indicarle por qué. La página contendrá un vínculo para obtener acceso al recurso web solicitado. Una vez que el usuario hace clic en el vínculo, dispone de una hora para visitar otros recursos alojados en el mismo dominio sin que Kaspersky Endpoint Security le advierta sobre la falta de confianza en el certificado.<br>• **Bloquear conexión**. 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.<br><br>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. |
| **Si se presentan errores al analizar una conexión cifrada** | • **Bloquear conexión**. Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red.<br><br>• **Agregar el dominio a las exclusiones**. Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security agrega 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 solo puede consultarse a través de la interfaz local de la aplicación. Para borrar el contenido de la lista, deberá seleccionar **Bloquear conexión**. |
| **Bloquear las conexiones SSL 2.0** | Cuando la casilla está activada, Kaspersky Endpoint Security bloquea las conexiones de red que se establecen con el protocolo SSL 2.0.<br><br>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. |
| **Descifrar conexiones cifradas a sitios web con certificado de EV** | 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.<br><br>Cuando esta casilla está activada, Kaspersky Endpoint Security descifra y controla las conexiones cifradas que se establecen con sitios web que utilizan certificados de EV.<br><br>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 basándose en la dirección del sitio web (por ejemplo, `https://facebook.com`).<br><br>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. |

## Analizar conexiones cifradas en Firefox y Thunderbird

Cuando termina la instalación de Kaspersky Endpoint Security, se agrega un certificado de Kaspersky al repositorio de certificados de confianza del sistema (tienda de certificados de Windows). De forma predeterminada, Firefox y Thunderbird utilizan su propio almacén de certificados patentado de Mozilla en lugar del almacén de certificados de Windows. Si Kaspersky Security Center está implementado en su organización y se está aplicando una directiva a un equipo, Kaspersky Endpoint Security habilita automáticamente el uso del almacén de certificados de Windows en Firefox y Thunderbird para analizar el tráfico de estas aplicaciones. Si no se aplica una directiva a un equipo, puede elegir el almacenamiento de certificados que utilizarán las aplicaciones de Mozilla. Si seleccionó el almacén de certificados de Mozilla, agregue 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 habilitar el Análisis de conexiones cifradas. Si el análisis de conexiones cifradas está deshabilitado, Kaspersky Endpoint Security no analiza el tráfico del navegador Mozilla Firefox ni el cliente de correo Thunderbird.

Antes de agregar un certificado a la tienda Mozilla, exporte el certificado de Kaspersky desde el Panel de control de Windows (propiedades del navegador). Para obtener más información sobre sobre cómo exportar el certificado de Kaspersky, consulte la Base de conocimientos del Servicio de soporte técnico. Para obtener detalles sobre cómo agregar un certificado al almacenamiento, visite el *sitio web de soporte técnico de Mozilla*.

Puede elegir el almacén de certificados solo en la interfaz local de la aplicación.

*Para elegir un almacén de certificados para analizar conexiones cifradas en Firefox y Thunderbird:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En el bloque **Mozilla Firefox y Thunderbird**, seleccione la casilla **Analizar el tráfico seguro en las aplicaciones de Mozilla**.
4. Seleccione una tienda de certificados:
   - **Usar almacén de certificados de Windows**. El certificado raíz de Kaspersky se agrega a esta tienda durante la instalación de Kaspersky Endpoint Security.
   - **Usar almacén de certificados de Mozilla**. Mozilla Firefox y Thunderbird utilizan sus propios almacenes de certificados. Si se selecciona el almacén de certificados de Mozilla, debe agregar manualmente el certificado raíz de Kaspersky a este almacén a través de las propiedades del navegador.
5. Guarde los cambios.

## Creación de exclusiones para el análisis de conexiones cifradas

La mayoría de los recursos web utilizan conexiones cifradas. Los especialistas de Kaspersky recomiendan habilitar la característica de análisis de conexiones cifradas. Si descubre que esta función interfiere con su trabajo, puede agregar las direcciones de los sitios web con los que tenga problemas como *direcciones de confianza*; al hacerlo, esos sitios web quedarán excluidos del análisis. De manera similar, si una aplicación que considera fiable utiliza una conexión cifrada, puede deshabilitar el análisis de conexiones cifradas para la misma. Un caso típico que puede requerir una exclusión sería el de una aplicación de almacenamiento en la nube que utilice su propio certificado para la autenticación de dos factores.

*Para excluir una dirección web de los análisis de conexiones cifradas:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección **Análisis de conexiones cifradas**, haga clic en el botón **Direcciones de confianza**.
4. Haga clic en el botón **Agregar**.
5. Escriba el nombre de dominio o la dirección IP. Kaspersky Endpoint Security no analizará las conexiones cifradas que se establezcan al visitar el dominio especificado.

   Kaspersky Endpoint Security admite el carácter `*` al ingresar una máscara de nombre de dominio.

   > Kaspersky Endpoint Security no admite máscaras para direcciones IP.

   Ejemplos:

   - `dominio.com`: esta entrada incluye las direcciones `https://dominio.com`, `https://www.dominio.com` y `https://dominio.com/pagina123`. Esta entrada no incluye subdominios (por ejemplo, `subdominio.dominio.com`).
   - `subdominio.dominio.com`: esta entrada incluye las direcciones `https://subdominio.dominio.com` y `https://subdominio.dominio.com/pagina123`. Esta entrada no incluye el dominio `dominio.com`.
   - `*.dominio.com`: esta entrada incluye las direcciones `https://peliculas.dominio.com` y `https://imagenes.dominio.com/pagina123`. Esta entrada no incluye el dominio `dominio.com`.
6. Guarde los cambios.

De manera predeterminada, si ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security desiste de analizar la conexión y agrega el dominio problemático a la lista *Dominios con errores de análisis*. Kaspersky Endpoint Security crea una lista separada para cada usuario. La información no se transmite a Kaspersky Security Center. Si lo prefiere, la aplicación puede en cambio bloquear las conexiones que no puede analizar correctamente. La lista de dominios con errores de análisis solo puede consultarse a través de la interfaz local de la aplicación.

- Guarde los cambios.

De manera predeterminada, si ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security desiste de analizar la conexión y agrega el dominio problemático a la lista *Dominios con errores de análisis*. Kaspersky Endpoint Security crea una lista separada para cada usuario. La información no se transmite a Kaspersky Security Center. Si lo prefiere, la aplicación puede en cambio bloquear las conexiones que no puede analizar correctamente. La lista de dominios con errores de análisis solo puede consultarse a través de la interfaz local de la aplicación.

*Para ver la lista de dominios con errores de análisis:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección **Análisis de conexiones cifradas**, haga clic en el botón **Dominios con errores de análisis**.

   Se abrirá una lista de dominios con errores de análisis. Si desea vaciar la lista, habilite el bloqueo de conexiones con errores de análisis en la directiva, aplique la directiva, restablezca el valor inicial del parámetro y aplique nuevamente la directiva.

La aplicación cuenta con una lista de *excepciones globales*, en la que los especialistas de Kaspersky recogen los sitios web que se consideran de confianza y que siempre estarán exceptuados de los análisis, independientemente de lo que indique la configuración de Kaspersky Endpoint Security.

*Para ver las exclusiones globales aplicadas al análisis de tráfico cifrado:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección **Análisis de conexiones cifradas**, haga clic en el vínculo **sitios web**.

Esto abre una lista de sitios web compilada por expertos de Kaspersky. Kaspersky Endpoint Security no analiza las conexiones protegidas para los sitios web de la lista. La lista puede modificarse cada vez que se actualizan las bases de datos y los módulos de Kaspersky Endpoint Security.

# Control Web

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

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 intente abrir un sitio web restringido por Control web, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia (vea la siguiente imagen).

Kaspersky Endpoint Security solo puede supervisar tráfico HTTP y HTTPS.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario habilitar 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. Puede impedir que sus usuarios accedan a sitios catalogados como “Redes sociales", por ejemplo, o a otras categorías.
- **Tipo de datos**. Puede restringir el acceso a ciertos tipos de datos y, por ejemplo, ocultar las imágenes de un sitio web. Kaspersky Endpoint Security determina los tipos de datos basándose en el formato de los archivos, no en sus extensiones.

  Kaspersky Endpoint Security no analiza el contenido de los archivos de almacenamiento. Por ello, si un grupo de imágenes está incluido en un archivo de almacenamiento, Kaspersky Endpoint Security considerará que el tipo de datos es "Archivos de almacenamiento" en lugar de "Archivos de imagen".

- **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 la web".

## Reglas de acceso a sitios web

Control web regula el acceso de los usuarios a los sitios web a través de *reglas de acceso*. Para cada una de estas reglas, puede configurar las siguientes opciones avanzadas:

- Usuarios alcanzados por la regla.

Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.

- Programación de la regla.

  Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

### Prioridad de las reglas de acceso

Cada regla tiene una prioridad. Cuanto más arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web "Redes sociales" y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.


Mensajes de Control web

## Habilitación y deshabilitación del Control Web

Por defecto, el Control Web está habilitado.

*Para habilitar y deshabilitar el Control web, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control web**.
3. Utilice el interruptor **Control web** para habilitar o deshabilitar el componente.

4. Guarde los cambios.

## Acciones con las reglas de acceso a recursos web

No se recomienda crear más de 1000 reglas de acceso a recursos web, ya que podría causar inestabilidades en el sistema.

Una regla de acceso a recursos web es un conjunto de filtros y acciones que Kaspersky Endpoint Security implementa cuando un usuario visita recursos web que están descritos en la regla durante el intervalo que se indica en la programación de la regla. Los filtros le permiten especificar con precisión un grupo de recursos web cuyo acceso está controlado mediante el componente Control web.

Están disponibles los siguientes filtros:

- **Filtrar por contenido**. Control web categoriza recursos web por contenido y tipo de datos. Puede controlar el acceso de los usuarios a los recursos web que tengan el contenido y los tipos de datos definidos en esas categorías. Cuando un usuario visita recursos web que pertenecen a la categoría de contenido o a la categoría de tipos de datos seleccionadas, Kaspersky Endpoint Security realiza la acción que se especifica en la regla.

- **Filtrar por direcciones de recursos web**. Puede controlar el acceso de los usuarios a todas las direcciones de recursos web, a direcciones de recursos web individuales o a grupos de direcciones de recursos web.

  Si se especifica el filtrado por contenido y por direcciones de recursos web y las direcciones o grupos de direcciones de recursos web especificados pertenecen a las categorías de contenido o tipos de datos seleccionadas, Kaspersky Endpoint Security no controla el acceso a todos los recursos web de las categorías de contenido o tipos de datos seleccionadas. En cambio, la aplicación solamente controla el acceso a las direcciones o grupos de direcciones de recursos web especificados.

- **Filtrar por nombres de usuarios y grupos de usuarios**. Puede especificar el nombre de los usuarios o grupos de usuarios para los cuales el acceso a los recursos web se controla conforme a la regla.

- **Programación de la regla**. Puede especificar la programación de la regla. La programación de reglas determina el intervalo durante el cual Kaspersky Endpoint Security controla el acceso a los recursos web cubiertos por la regla.

Una vez instalado Kaspersky Endpoint Security, la lista de reglas del componente Control web no está vacía. Existen dos reglas configuradas previamente:

- La regla de scripts y hojas de estilo, que permite que todos los usuarios tengan acceso en todo momento a los recursos web que en su dirección contengan nombres de archivos con las extensiones CSS, JS o VBS. Por ejemplo: http://www.example.com/style.css, http://www.ejemplo.com/style.css?mode=normal.

- La 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.

## Agregar una regla de acceso a recursos web

*Para agregar o editar una regla de acceso a recursos web:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **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, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de acceso a recursos web**.

5. En el campo **Nombre de la regla**, escriba el nombre de la regla.

6. Seleccione el estado **Activo** para la regla de acceso a recursos web.

   Puede usar el interruptor para deshabilitar la regla de acceso a recursos web en cualquier momento.

7. En el bloque **Acción**, seleccione la opción correspondiente:

   - **Permitir**. Si se selecciona este valor, Kaspersky Endpoint Security permite el acceso a recursos web que coinciden con los parámetros de la regla.
   - **Bloquear**. Si se selecciona este valor, Kaspersky Endpoint Security bloquea el acceso a recursos web que coinciden con los parámetros de la regla.
   - **Advertir**. Si se selecciona este valor, Kaspersky Endpoint Security mostrará una advertencia en la que se indica que un recurso web es no deseado cuando el usuario intente acceder a recursos web que coinciden con la regla. Mediante los vínculos del mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.

8. En el bloque **Tipo de 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 vínculo **Configurar**.

   b. Seleccione las casillas junto a los nombres de las categorías de contenido y/o tipos de datos que desee.

      Al seleccionar la casilla junto al nombre de una categoría de contenido y/o tipo de datos, Kaspersky Endpoint Security aplicará la regla para controlar el acceso a los recursos web que pertenecen a las categorías de contenido y/o tipos de datos seleccionados.

   c. Regrese a la ventana para configurar la regla de acceso a recursos web.

9. En el bloque **Direcciones**, seleccione el filtro de direcciones de recursos web relevante:

   - **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 **Agregar dirección** o **Agregar un grupo de direcciones**.

     b. En la ventana que se abre, 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 Análisis de conexiones cifradas está deshabilitado, en el caso del protocolo HTTPS, el filtrado solo puede hacerse por nombre de servidor.

10. En el bloque **Usuarios**, seleccione el filtro relevante para los usuarios:

- **A todos los usuarios**. Control web no filtrará recursos web para usuarios específicos.
- **A usuarios individuales o grupos**. Control web filtrará 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 **Agregar**.

b. En la ventana que se abre, 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 **Programación de la regla**, seleccione el nombre de la programación necesaria o genere una programación nueva basada en la programación de la regla seleccionada. Para hacerlo:

a. Haga clic en el botón **Administración de programaciones**.

b. En la ventana, haga clic en el botón **Agregar**.

c. En la ventana que se abre, ingrese el nombre de la programación de la regla.

d. Configure la programación de acceso a los recursos web para los usuarios.

e. Regrese a la ventana para configurar la regla de acceso a recursos web.

12. Guarde los cambios.

## Asignación de prioridades a las reglas de acceso a recursos web

Puede asignar prioridades a cada regla de la lista de reglas colocando las reglas en un orden determinado.

*Para asignar una prioridad a una regla de acceso a recursos web:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **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, seleccione la regla de paquetes de red cuya prioridad quiera cambiar.

5. Use los botones **Subir** y **Bajar** para mover la regla a la posición correspondiente en la lista de reglas de acceso a recursos web.

6. Guarde los cambios.

## Habilitación y deshabilitación de una regla de acceso a recursos web

*Para habilitar o deshabilitar una regla de acceso a recursos web:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **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, seleccione la regla que desea habilitar o deshabilitar.

5. En la columna **Estado**, haga lo siguiente:

   - Si desea habilitar el uso de la regla, seleccione el valor **Activo**.

   - Si desea deshabilitar el uso de la regla, seleccione el valor **Inactivo**.

6. Guarde los cambios.

## Exportar e importar la lista de direcciones web de confianza

Puede exportar la lista de reglas de administración de directivas web a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de direcciones del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de administración de directivas web o para migrar la lista a otro servidor.

Cómo exportar e importar una lista de reglas de administración de directivas web a la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Controles de seguridad** → **Administración de directivas web**.
6. Para exportar la lista de reglas de administración de directivas web:
   a. Seleccione la regla de acceso que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
   b. Haga clic en el vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.
      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.
7. Para importar la lista de reglas de administración de directivas web:
   a. Haga clic en el vínculo **Importar**.
      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.
      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
8. Guarde los cambios.

Cómo exportar e importar una lista de reglas de administración de directivas web a 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 correspondiente a los equipos en los que desee exportar o importar la lista de reglas.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** → **Administración de directivas web**.
5. Para exportar la lista de reglas, en el bloque **Lista de reglas**:
   a. Seleccione la regla de acceso que desea exportar.
   b. Haga clic en el botón **Exportar**.
   c. Confirme que desea exportar solo las reglas seleccionadas, o bien exporte la lista completa.
   d. Haga clic en el botón **Exportar**.

      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 vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
7. Guarde los cambios.

## Prueba de las reglas de acceso a recursos web

Para comprobar la coherencia de las reglas del Control Web, puede probarlas. Para ello, el Control Web incluye una función de Diagnóstico de las reglas.

*Para probar las reglas de acceso a recursos web:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control web**.
3. En el bloque **Configuración**, haga clic en el vínculo **Diagnóstico de las reglas**.

   Se abre la ventana **Diagnóstico de las reglas**.
4. Si desea probar las reglas que Kaspersky Endpoint Security usa para controlar el acceso a un recurso web específico, seleccione la casilla **Especificar dirección**. Escriba la dirección del recurso web en el campo que

aparece a continuación.

5. Si desea probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a recursos web de usuarios o grupos de usuarios especificados, especifique una lista de usuarios o grupos de usuarios.

6. Si desea probar las reglas que Kaspersky Endpoint Security usa para controlar el acceso a recursos web de categorías de contenido o categorías de tipos de datos especificadas, seleccione la casilla **Filtrar contenido** y elija la opción correspondiente en la lista desplegable (**Por categorías de contenido**, **Por tipos de datos** o **Por contenido y tipos de datos**).

7. Si desea probar las reglas teniendo en cuenta la hora y el día de la semana en que se intentó acceder a los recursos web que se especifican en las condiciones del diagnóstico de reglas, seleccione la casilla **Incluir momento de intento de acceso**. Luego, especifique el día de la semana y la hora.

8. Haga clic en el botón **Prueba**.

Al completarse la prueba, aparece un mensaje con información sobre la acción realizada por Kaspersky Endpoint Security según la primera regla que se aplica sobre el intento de acceso a los recursos web especificados (permitir, bloquear o advertir). La primera regla que se aplica es la que tiene un lugar en la lista de reglas del Control Web que es superior al de las otras reglas que cumplen las condiciones del diagnóstico. El mensaje se muestra a la derecha del botón **Prueba**. La siguiente tabla enumera las reglas activadas restantes, especificando la acción llevada a cabo por Kaspersky Endpoint Security. Las reglas están enumeradas en orden de prioridad decreciente.

## Exportación e importación de la lista de direcciones de recursos web

Si creó una lista de direcciones de recursos web en una regla de acceso a recursos web, puede exportarla a un archivo .txt. Posteriormente, puede importar la lista de este archivo para evitar crear una nueva lista de direcciones de recursos web manualmente cuando configure la regla de acceso. La opción de exportar e importar la lista de direcciones de recursos web puede ser útil si, por ejemplo, crea reglas de acceso con parámetros similares.

*Para importar o exportar una lista de direcciones de recursos web a un archivo:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → 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 cuyas direcciones de recursos web desea exportar o importar.

5. Para exportar la lista de direcciones web de confianza, haga lo siguiente en el bloque **Direcciones**:

   a. Seleccione las direcciones que desea exportar.

   Si no seleccionó ninguna dirección, Kaspersky Endpoint Security exportará todas las direcciones.

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

   c. En la ventana que se abre, escriba el nombre del archivo TXT en el que desea exportar la lista de direcciones de recursos web, y seleccione la carpeta en la que se guardará este archivo.

   d. Haga clic en el botón **Guardar**.

   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 que desea usar para importar la lista de recursos web.

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

      Cuando ya exista una lista de direcciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo TXT.

7. Guarde los cambios.

## Supervisión de las actividades de los usuarios en Internet

Kaspersky Endpoint Security puede registrar información sobre todos los sitios web que visitan los usuarios, incluso cuando se trata de sitios web permitidos. Ello hace posible obtener un historial de navegación completo. Kaspersky Endpoint Security envía los eventos sobre las actividades de los usuarios a Kaspersky Security Center, al registro local de Kaspersky Endpoint Security y al registro de eventos de Windows. Para recibir estos eventos en Kaspersky Security Center, deberá configurar los ajustes de los eventos en una directiva, ya sea a través de Web Console o con la Consola de administración. Dependiendo de la configuración, los eventos de Control web también pueden transmitirse por correo electrónico o mostrarse en el equipo del usuario a través de notificaciones en pantalla.

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 habilitar la supervisión de la actividad de Internet del usuario, debe hacer lo siguiente:

- Inyecte un script de interacción de la página web en el tráfico web (consulte las instrucciones a continuación). El script permite registrar eventos de Control web.
- Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario habilitar el análisis de conexiones cifradas.

*Para inyectar un script de interacción de página web en el tráfico web:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En el bloque **Procesamiento de tráfico**, seleccione la casilla **Inyectar script de interacción en el tráfico**.
4. Guarde los cambios.

De esta manera, Kaspersky Endpoint Security inyectará un script de interacción de la página web en el tráfico web. Esta secuencia de comandos permite el registro de eventos de Control web para el registro de eventos de la aplicación, el registro de eventos del sistema operativo y los informes.

*Para que los eventos de Control web se registren en el equipo del usuario:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana Configuración de la aplicación, seleccione la sección **Interfaz**.
3. En el bloque **Notificaciones**, haga clic en el botón **Reglas de notificación**.
4. En la ventana que se abre, elija la sección **Control web**.

   Se abrirá una tabla con los eventos de Control web y los distintos métodos de notificación.
5. Configure el método de notificación para cada evento: **Guardar en informe local** o **Guardar en registro de eventos de Windows**.

   Para que se registren las visitas a sitios web permitidos, también deberá hacer cambios en la configuración de Control web (consulte las instrucciones más abajo).

   A través de la tabla de eventos también podrá habilitar las notificaciones en pantalla y las notificaciones por correo electrónico. Para que la aplicación envíe notificaciones por correo electrónico, deberá configurar los ajustes del servidor SMTP. Para obtener más información sobre el envío de notificaciones por correo electrónico, consulte la *Ayuda de Kaspersky Security Center*.
6. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security comenzará a registrar los eventos relacionados con las actividades en Internet del usuario.

Control web comunica las actividades de los usuarios a Kaspersky Security Center de este modo:

- Cuando se utiliza Kaspersky Security Center, Control web envía un evento por cada objeto que forma parte de una página web. Por este motivo, cada página web bloqueada podría dar lugar a más de un evento. Por ejemplo, si se bloquea la página web http://www.example.com, Kaspersky Endpoint Security podría transmitir eventos sobre los objetos http://www.example.com, http://www.example.com/icono.ico, http://www.example.com/archivo.js, etc.
- Cuando se utiliza Kaspersky Security Center Cloud Console, Control web agrupa los eventos y transfiere solo el protocolo y el dominio del sitio web. Por ejemplo, si un usuario visita las páginas web no recomendadas http://www.example.com/principal, http://www.example.com/contacto y http://www.example.com/fotos, Kaspersky Endpoint Security enviará un único evento, con el objeto http://www.example.com.

*Para que se registren las visitas a sitios web permitidos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → 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 del Control Web

Según el tipo de acción que se especifique en las propiedades de las reglas de Control Web, Kaspersky Endpoint Security muestra un mensaje de uno de los siguientes tipos cuando los usuarios intentan acceder a recursos de Internet (la aplicación sustituye una página HTML con un mensaje para la respuesta del servidor HTTP):

- Mensaje de advertencia. Este mensaje advierte al usuario que la visita al recurso web no es recomendable o no cumple con la directiva de seguridad corporativa. Kaspersky Endpoint Security muestra un mensaje de advertencia si la opción **Advertir** está seleccionada en la lista desplegable **Acción** de la configuración de la regla que describe este recurso web.

  Si el usuario considera que la advertencia es errónea, puede hacer clic en el vínculo de la advertencia para enviar un mensaje generado previamente al administrador de la red corporativa local.

- Mensaje sobre el bloqueo de un recurso web. Kaspersky Endpoint Security muestra un mensaje en el que se indica que un recurso web está bloqueado si la opción **Bloquear** está seleccionada en la lista desplegable **Acción** de la configuración de la regla que describe este recurso web.

  Si el usuario considera que el recurso web fue bloqueado por error, puede hacer clic en el vínculo del mensaje de notificación de bloqueo del recurso web para enviar un mensaje generado previamente al administrador de la red corporativa local.

Se ofrecen plantillas especiales para el mensaje de advertencia, para el mensaje en el que se informa que un recurso web está bloqueado y para el mensaje que se envía enviar al administrador de la red LAN. Puede modificar el contenido de estas plantillas.

*Para cambiar a la plantilla de mensajes de Control Web:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control web**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control web:
   - **Advertencias**. El campo de entrada consiste en una plantilla del mensaje que se muestra si se activa una regla de advertencia acerca de intentos para acceder a un recurso web no deseado.
   - **Bloqueo**. El campo de entrada contiene la plantilla del mensaje que se muestra si se activa una regla que bloquea el acceso a un recurso web.
   - **Mensaje para el administrador**. El campo de entrada contiene la plantilla del mensaje que se enviará al administrador de la red de área local si el usuario considera que se ha bloqueado por error.
4. Guarde los cambios.

## Edición de máscaras para direcciones de recursos web

El uso de una *máscara para direcciones de recursos web* (también denominada "máscara de dirección") puede ser útil si necesita escribir varias direcciones de recursos web similares cuando crea una regla de acceso a recursos web. Si está bien diseñada, una máscara de dirección puede sustituir a una gran cantidad de direcciones de recursos web.

Al crear una máscara de dirección, siga las reglas a continuación:

1. El carácter `*` reemplaza cualquier secuencia que no tenga caracteres o que tenga uno o más caracteres.

Por ejemplo, si crea una regla de acceso con la máscara `*abc*`, la regla se aplicará a todos los recursos web que tengan la secuencia `abc` en su dirección. Ejemplo: `http://www.example.com/pagina_0-9abcdef.html`.

2. El par de caracteres `*.` (combinación conocida como *máscara de dominio*) permite abarcar todos los dominios de una dirección. La máscara de dominio `*.` representa cualquier nombre de dominio, subdominio o línea en blanco.

   Ejemplo: la máscara `*.example.com` representa las siguientes direcciones:

   - `http://fotos.example.com`. La máscara de dominio `*.` representa `fotos.`
   - `http://usuario.fotos.example.com`. La máscara de dominio `*.` representa `fotos.` y `usuario.`
   - `http://example.com`. La máscara de dominio `*.` se interpreta como línea en blanco.

3. La secuencia de caracteres `www.` al comienzo de la máscara de dirección se interpreta como una secuencia `*.`

   Ejemplo: la máscara `www.example.com` se interpreta como `*.example.com`. La máscara comprende las direcciones `www2.example.com` y `www.fotos.example.com`.

4. Si una máscara de dirección no comienza con el carácter `*`, el contenido de la máscara de dirección es equivalente al mismo contenido con el prefijo `*.`.

5. Si una máscara de dirección termina con un carácter que no sea `/` o `*`, el contenido de la máscara de dirección es equivalente al mismo contenido con el postfijo `/*`.

   Ejemplo: la máscara `http://www.example.com` comprende direcciones como `http://www.example.com/abc` (entendiéndose que `a`, `b` y `c` pueden ser cualquier carácter).

6. Si una máscara de dirección termina con el carácter `/`, el contenido de la máscara de dirección es equivalente al mismo contenido con el postfijo `/*.`.

7. La secuencia de caracteres `/*` al final de una máscara de dirección se interpreta como `/*` o como una cadena vacía.

8. Las direcciones de recursos web se comprueban con una máscara de dirección, teniendo en cuenta el protocolo (http o https):

   - Si la máscara de dirección no contiene un protocolo de red, esta máscara de red abarca las direcciones con cualquier protocolo de red.

     Ejemplo: la máscara de dirección `example.com` comprende las direcciones `http://example.com` y `https://example.com`.

   - Si la máscara de dirección contiene un protocolo de red, esta máscara de dirección solo abarca las direcciones que tienen el mismo protocolo de red que la máscara de dirección.

     Ejemplo: la máscara `http://*.example.com` comprende la dirección `http://www.example.com`, pero no la dirección `https://www.example.com`.

9. Una máscara de dirección encerrada entre comillas dobles se trata sin considerar ninguna sustitución adicional, excepto el carácter `*` si se lo ha incluido inicialmente en la máscara de dirección. Las reglas 5 y 7 no se aplican a máscaras de dirección entre comillas dobles (consulte los ejemplos 14 al 18 de la tabla que se incluye a continuación).

10. El nombre de usuario y la contraseña, el puerto de conexión y las mayúsculas o minúsculas de los caracteres no se tienen en cuenta durante la comparación con la máscara de dirección de un recurso web.

Ejemplos de uso de reglas para crear máscaras de dirección

| Número | Máscara de dirección | Dirección de recurso web para comprobar | ¿La máscara de dirección abarca la dirección? | Comentario |
|---|---|---|---|---|
| 1 | *.ejemplo.com | http://www.123ejemplo.com | No | Consulte la regla 1. |
| 2 | *.ejemplo.com | http://www.123.example.com | Sí | Consulte la regla 2. |
| 3 | *ejemplo.com | http://www.123ejemplo.com | Sí | Consulte la regla 1. |
| 4 | *ejemplo.com | http://www.123.example.com | Sí | Consulte la regla 1. |
| 5 | http://www.*.ejemplo.com | http://www.123ejemplo.com | No | Consulte la regla 1. |
| 6 | www.ejemplo.com | http://www.example.com | Sí | Consulte las reglas 3, 2, 1. |
| 7 | www.ejemplo.com | https://www.ejemplo.com | Sí | Consulte las reglas 3, 2, 1. |
| 8 | http://www.*.ejemplo.com | http://123.example.com | Sí | Consulte las reglas 3, 4, 1. |
| 9 | www.ejemplo.com | http://www.ejemplo.com/abc | Sí | Consulte las reglas 3, 5, 1. |
| 10 | ejemplo.com | http://www.example.com | Sí | Consulte las reglas 3, 1. |
| 11 | http://ejemplo.com/ | http://ejemplo.com/abc | Sí | Consulte la regla 6. |
| 12 | http://ejemplo.com/* | http://example.com | Sí | Consulte la regla 7. |
| 13 | http://example.com | https://ejemplo.com | No | Consulte la regla 8. |
| 14 | "ejemplo.com" | http://www.example.com | No | Consulte la regla 9. |
| 15 | "http://www.ejemplo.com" | http://www.ejemplo.com/abc | No | Consulte la regla 9. |
| 16 | "*.ejemplo.com" | http://www.example.com | Sí | Consulte las reglas 1, 9. |
| 17 | "http://www.ejemplo.com/*" | http://www.ejemplo.com/abc | Sí | Consulte las reglas 1, 9. |
| 18 | "www.ejemplo.com" | http://www.example.com; https://www.example.com | Sí | Consulte las reglas 9, 8. |
| 19 | www.ejemplo.com/abc/123 | http://www.ejemplo.com/abc | No | Una máscara de dirección contiene más información que la dirección de un recurso web. |

## Migración de reglas de acceso a recursos web a partir de versiones anteriores de la aplicación

Cuando Kaspersky Endpoint Security 10 Service Pack 2 para Windows (o una versión anterior) se actualiza a Kaspersky Endpoint Security para Windows 11.6.0, se siguen estos criterios para migrar las reglas de acceso a recursos web basadas en categorías de contenido de recursos web:

- Las reglas de acceso a recursos web basadas en una o más de las categorías de contenido de recursos web de las listas "Chats y foros", "Correo electrónico basado en la 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 más de las categorías de contenido de recursos web de las listas "Tiendas electrónicas" y "Sistemas de pago" migran a la categoría de contenido de recursos web "Tiendas en línea, bancos y sistemas de pago".
- Las reglas de acceso a recursos web basadas en la categoría de contenido de recursos web "Juegos de azar" migran a la categoría de contenido "Juegos de azar, loterías, sorteos".
- Las reglas de acceso a recursos web basadas en la categoría de contenido de recursos web "Juegos de Navegador" migran a la categoría de contenido "Juegos de computadora".
- Las reglas de acceso a recursos web basadas en las categorías de contenido de recursos web que no se enumeran en la lista anterior se migran sin cambios.

# Control de dispositivos

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El Control de dispositivos administra el acceso de los usuarios a los dispositivos que se instalan o se conectan al equipo (por ejemplo, discos duros, cámaras o módulos Wi-Fi). Esto impide la infección del equipo cuando se conectan dichos dispositivos y evita las pérdidas o fugas de datos.

## Niveles de acceso a dispositivos

El Control de dispositivos controla el acceso a los siguientes niveles:

- **Tipo de dispositivo**. Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

  Puede configurar el acceso a los dispositivos de la siguiente manera:

  - Permitir – .
  - Bloquear – .
  - Depende del bus de conexión (excepto Wi-Fi) – .
  - Bloquear con excepciones (solamente con Wi-Fi) – .

- **Bus de conexión**. El *bus de conexión* es una interfaz utilizada para conectar dispositivos al equipo (por ejemplo, USB o FireWire). De esta forma, puede restringir la conexión de todos los dispositivos, por ejemplo, a través de USB.

  Puede configurar el acceso a los dispositivos de la siguiente manera:

- Permitir – ✓.
- Bloquear – ⊘.

- **Dispositivos de confianza**. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

  Puede agregar dispositivos de confianza en función de los siguientes datos:

  - **Dispositivos por Id.** Cada dispositivo tiene un identificador único (id. de hardware, también denominado HWID). Puede ver el Id. en las propiedades del dispositivo usando las herramientas del sistema operativo. Un id. de dispositivo típico podría ser `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id.

  - **Dispositivos por modelo**. Cada dispositivo tiene un id. de proveedor (VID) y un id. de producto (PID). Puede ver los ID. en las propiedades del dispositivo usando las herramientas del sistema operativo. Los valores VID y PID deben especificarse en este formato: `VID_1234&PID_5678`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.

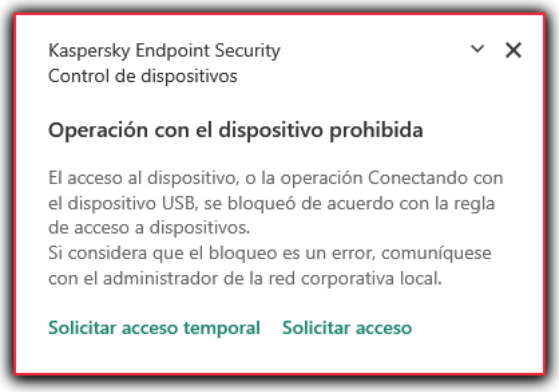
  - **Dispositivos por máscara de id.** Si tiene dispositivos con identificadores similares, puede agregarlos a la lista de dispositivos de confianza utilizando máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Una máscara típica podría ser `WDC_C*`.

  - **Dispositivos por máscara de modelo**. Si tiene dispositivos con identificadores VID o PID similares (por ejemplo, dispositivos de un mismo fabricante), puede utilizar máscaras para agregarlos a la lista de dispositivos de confianza. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `VID_05AC & PID_ *`.

El Control de dispositivos regula el acceso de los usuarios a los dispositivos usando *reglas de acceso*. El Control de dispositivos también le permite guardar eventos relacionados con la conexión/desconexión de dispositivos. Para guardar eventos, tiene que configurar el registro de eventos en una directiva.

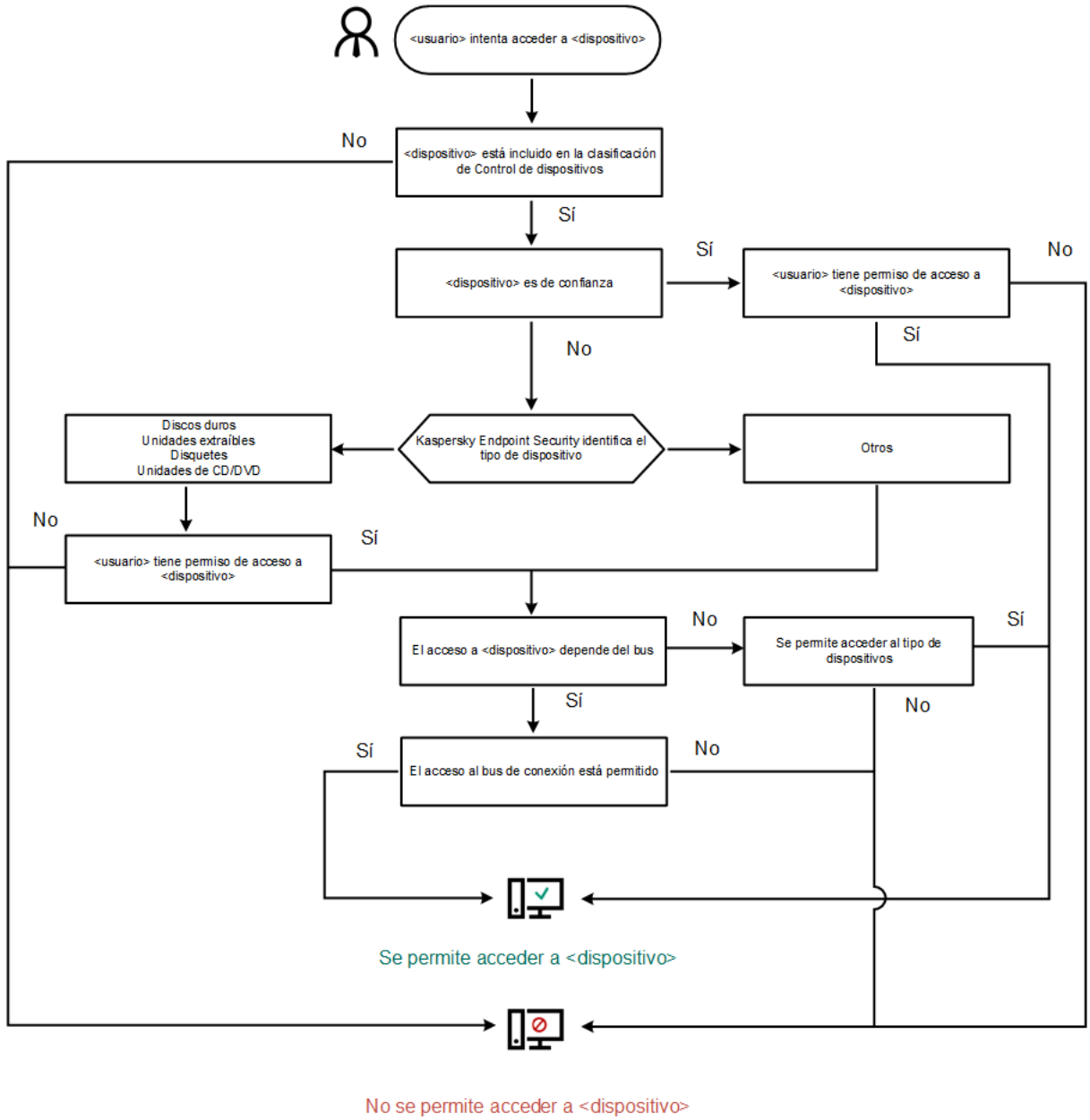
Cuando el acceso a un dispositivo dependa del bus de conexión (estado ), Kaspersky Endpoint Security no guardará ningún evento relacionado con la conexión o desconexión del dispositivo. Para que Kaspersky Endpoint Security guarde los eventos relacionados con la conexión/desconexión de dispositivos, autorice el acceso al tipo de dispositivo correspondiente (estado ✓) o agregue el dispositivo a la lista de dispositivos de confianza.

Cuando se conecta al equipo un dispositivo que está bloqueado por el Control de dispositivos, Kaspersky Endpoint Security bloqueará el acceso y mostrará que una notificación (consulte la figura a continuación).



## Algoritmo de funcionamiento del Control de dispositivos

Kaspersky Endpoint Security decide si permitirá el acceso a un dispositivo después de que el usuario conecta el dispositivo al equipo de la siguiente imagen.




Algoritmo de funcionamiento del Control de dispositivos

Si conecta un dispositivo y se le permite acceder a él, puede editar la regla de acceso y bloquear la posibilidad de utilizarlo. Cuando alguien intente acceder al dispositivo nuevamente (por ejemplo, para ver la estructura de carpetas o para realizar una operación de lectura o escritura), Kaspersky Endpoint Security bloqueará el acceso. Un dispositivo sin un sistema de archivos se bloqueará solo la próxima vez que el dispositivo se conecte.

Si un usuario del equipo con Kaspersky Endpoint Security instalado debe solicitar acceso a un dispositivo que cree fue bloqueado por error, envíe al usuario las instrucciones para solicitar acceso.

# Habilitación y deshabilitación del Control de dispositivos

Por defecto, el Control de dispositivos está habilitado.

*Para habilitar y deshabilitar el Control de dispositivos, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. Utilice el interruptor **Control de dispositivos** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

Por lo tanto, si el Control de dispositivos está habilitado, la aplicación transmite información sobre los dispositivos conectados a Kaspersky Security Center. Puede ver la lista de dispositivos conectados en Kaspersky Security Center en la carpeta **Hardware**.

# Acerca de las reglas de acceso

Las *reglas de acceso* comprenden un grupo de configuraciones que determinan qué usuarios pueden acceder a los dispositivos que están instalados o conectados al equipo. No puede agregar un dispositivo que esté fuera de la clasificación del Control de dispositivos. Está permitido el acceso de todos los usuarios a dichos dispositivos.

## Reglas de acceso a dispositivos

El grupo de configuraciones para una regla de acceso varía según el tipo de dispositivo (consulte la tabla a continuación).

Configuración de las reglas de acceso

| Dispositivos | Control de acceso | Programación de acceso a un dispositivo | Asignación de usuarios y/o un grupo de usuarios | Prioridad | Lea/escriba el permiso |
|---|---|---|---|---|---|
| Discos duros | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unidades extraíbles | ✓ | ✓ | ✓ | ✓ | ✓ |
| Impresoras | ✓ | – | – | – | – |
| Disquetes | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unidades de CD/DVD | ✓ | ✓ | ✓ | ✓ | ✓ |
| Módems | ✓ | – | – | – | – |
| Dispositivos de cinta | ✓ | – | – | – | – |
| Dispositivos multifunción | ✓ | – | – | – | – |
| Lectores de tarjetas inteligentes | ✓ | – | – | – | – |
| Dispositivos USB ActiveSync de Windows CE | ✓ | – | – | – | – |
| 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.

El acceso a los dispositivos ADB y iTunes está sujeto a las siguientes consideraciones especiales:

- No es posible definir una programación de acceso para estos dispositivos. Aun cuando existan reglas que restrinjan el acceso a los dispositivos (es decir, cuando el estado sea ), siempre será posible acceder a los dispositivos ADB y iTunes.
- No es posible configurar permisos de acceso (lectura/escritura) ni regular el acceso a estos dispositivos por parte de usuarios específicos. Aun cuando existan reglas que restrinjan el acceso a los dispositivos (es decir, cuando el estado sea ), todos los usuarios tendrán permisos ilimitados para acceder a los dispositivos ADB y iTunes.
- No es posible regular el acceso a dispositivos ADB o iTunes de confianza por parte de usuarios específicos. Si un dispositivo ADB o iTunes se considera de confianza, todos los usuarios tendrán acceso al mismo.
- Si conecta un dispositivo al equipo y luego instala las aplicaciones ADB o iTunes, el identificador único de dicho dispositivo podría restablecerse. Si esto ocurre, Kaspersky Endpoint Security lo identificará como dispositivo nuevo. Si el dispositivo estaba catalogado como de confianza, deberá agregarlo a la lista de dispositivos de confianza una segunda vez.

Por defecto, las reglas de acceso les otorgan acceso completo a todos los usuarios a los dispositivos en todo momento si está habilitado el acceso a los buses de conexión para los tipos de dispositivos correspondientes ( estado).

## Reglas de acceso para redes Wi-Fi

Una regla de acceso para redes Wi-Fi determina si se permite ( estado) o se prohíbe ( estado) el uso de redes Wi-Fi. Puede agregar una *red Wi-Fi de confianza* ( estado) a una regla. El uso de una red Wi-Fi de confianza está permitido sin restricciones. Por defecto, una regla del acceso para redes Wi-Fi permite el acceso a cualquier red Wi-Fi.

## Reglas de acceso a los buses de conexión

Las reglas del acceso a los buses de conexión determinan si se permite ( estado) o se prohíbe ( estado) la conexión de dispositivos. Por defecto, se crean reglas que permiten el acceso a los buses para todos los buses de conexión incluidos en la clasificación del componente Control de dispositivos.

## Edición de una regla de acceso a dispositivos

Una *regla de acceso a dispositivos* un grupo de configuraciones que determinan de qué forma los usuarios pueden acceder a los dispositivos que están instalados o conectados al equipo. Estas configuraciones incluyen el acceso a un dispositivo específico, una programación de acceso y permisos de lectura o escritura.

*Para editar una regla de acceso a dispositivos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración de acceso**, haga clic en el botón **Dispositivos y redes Wi-Fi**.

   La ventana que se abre muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
4. En el bloque **Acceso a 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 ajustar configuraciones de acceso adicionales. Por defecto, una regla de acceso a dispositivos otorga a todos los usuarios acceso completo al tipo de dispositivos especificado en cualquier momento.

   a. En el bloque **Acceso**, seleccione la opción de acceso al dispositivo correspondiente:

   - **Permitir**.
   - **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 una programación para el acceso al dispositivo.

   b. En el bloque **Derechos de los usuarios**, haga clic en el botón **Agregar**.

   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 agregado un usuario a varios grupos, Kaspersky Endpoint Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Endpoint Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

   Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Endpoint Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

d. Seleccione el estado **Habilitado** para la regla de acceso al dispositivo.

e. Configure los permisos de acceso al dispositivo de los usuarios: lectura y/o escritura.

f. Seleccione los usuarios o el grupo de usuarios a los que desea aplicar la regla de acceso al dispositivo.

g. Configure una programación de acceso al dispositivo para los usuarios.

h. Haga clic en el botón **Agregar**.

5. En el bloque **Acceso a dispositivos externos**, seleccione la regla y configure el acceso: **Permitir**, **Denegar** o **Depende del bus de conexión**. Si es necesario, configure el acceso al bus de conexión.

6. En el bloque **Acceso a redes Wi-Fi**, haga clic en el vínculo **Wi-Fi** y configure el acceso: **Permitir**, **Bloquear** o **Bloquear con excepciones**. Si es necesario, agregue redes Wi-Fi a la lista de confianza.

7. Guarde los cambios.

## Edición de una regla de acceso a buses de conexión

*Para editar una regla de acceso a buses de conexión:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración**, haga clic en el botón **Buses de conexión**.

   La ventana que se abre muestra las reglas de acceso para todos los buses de conexión que se incluyen en la clasificación del componente Control de dispositivos.

4. Seleccione la regla de acceso que desea editar.

5. En la columna **Acceso**, seleccione si desea permitir o no el acceso al bus de conexión: **Permitir** o **Rechazar**.

6. Guarde los cambios.

## Incorporación de una red Wi-Fi a la lista de confianza

Puede permitir que los usuarios se conectan a las redes Wi-Fi que considera seguras, por ejemplo: una red Wi-Fi corporativa. Para hacerlo, debe agregar la red a la lista de redes Wi-Fi de confianza. El Control de dispositivos bloqueará el acceso a todas las redes Wi-Fi salvo por las especificadas en la lista de confianza.

*Para incorporar una red Wi-Fi a la lista de confianza:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso para dispositivos y redes Wi-Fi**.

   La ventana que se abre muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

4. En el bloque **Acceso a redes Wi-Fi**, haga clic en el vínculo **Wi-Fi**.

   La ventana que se abre muestra las reglas de acceso a la red Wi-Fi.

5. En la columna **Acceso**, seleccione **Bloquear con excepciones**.

6. Haga clic en el botón **Agregar** en el bloque de **Red Wi-Fi de confianza**.

7. En la ventana que se abre, realice una de las siguientes acciones:

   a. En el campo **Nombre de red**, especifique el nombre de la red Wi-Fi que quiera agregar a la lista de confianza.

   b. En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación que se utiliza al conectarse a la red Wi-Fi de confianza.

   c. En la lista desplegable **Tipo de cifrado**, seleccione el tipo de cifrado que se utiliza para asegurar el tráfico de la red Wi-Fi de confianza.

   d. En el campo **Comentario**, puede especificar cualquier información sobre la red Wi-Fi que acaba de agregar.

   Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

8. Guarde los cambios.

## Supervisar el uso de unidades extraíbles

*Para habilitar la supervisión del uso de unidades extraíbles:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.

3. En el bloque **Configuración**, haga clic en el botón **Reglas de acceso para dispositivos y redes Wi-Fi**.

   La ventana que se abre muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

4. En el bloque **Acceso a dispositivos de almacenamiento**, seleccione **Unidades extraíbles**.

5. Haga clic en el vínculo **Seguimiento**.

6. En la ventana que se abre, seleccione la pestaña **Seguimiento**.

7. Active el interruptor **Seguimiento**.

8. En el bloque **Operaciones sobre archivos**, seleccione las operaciones que desea supervisar: **Escribir**, **Eliminar**.

9. En el bloque **Filtrar por formatos de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas debe seguir Control de dispositivos.

10. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.

11. Guarde los cambios.

De esta manera, cuando los usuarios escriban en archivos ubicados en unidades extraíbles o eliminen archivos de unidades extraíbles, Kaspersky Endpoint Security guardará la información sobre dichas operaciones en el registro de eventos y enviará un mensaje al Servidor de administración de Kaspersky Security Center. Puede ver eventos asociados con archivos en unidades extraíbles en la Consola de administración de Kaspersky Security Center en el espacio de trabajo del nodo del **Servidor de administración** en la ficha **Eventos**. Para que se muestren los eventos en el registro de eventos local de Kaspersky Endpoint Security, debe seleccionar la casilla **Operación sobre 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. A continuación, Control de dispositivos permite o bloquea la acción de acuerdo con la configuración de Kaspersky Endpoint Security.

Control de dispositivos guarda información sobre eventos durante un período de tiempo específico llamado *período de almacenamiento en caché*. Si la información sobre un evento se almacena en caché y este evento se repite, no es necesario notificarlo a Kaspersky Endpoint Security ni mostrar otro mensaje para otorgar acceso a la acción correspondiente, como conectar un dispositivo. Esto hace que sea más conveniente trabajar con un dispositivo.

Un evento se considera un evento duplicado si todas las configuraciones de eventos siguientes coinciden con el registro en la caché:

- Id. de dispositivo
- SID de la cuenta de usuario que intenta acceder
- Categoría de dispositivo
- Acción realizada con el dispositivo
- Veredicto de permiso de solicitud para esta acción: permitido o rechazado
- Ruta del proceso utilizado para realizar la acción
- Archivo al que se accede

Antes de cambiar el período de almacenamiento en caché, deshabilite la Autoprotección de Kaspersky Endpoint Security. Después de cambiar el período de almacenamiento en caché, habilite la Autoprotección.

*Para cambiar el período de almacenamiento en caché:*

1. Abra el editor de registro en el equipo.

2. En el editor de registro, vaya a la siguiente sección:

   - Para sistemas operativos de 64 bits:
     [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]

   - Para sistemas operativos de 32 bits:
     [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]

3. Abra DeviceControlEventsCachePeriod para editarlo.

4. Defina la cantidad de minutos durante los que Control de dispositivos debe guardar información sobre un evento antes de eliminarla.

## Acciones con dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

Puede conceder acceso a los dispositivos de confianza a un usuario específico, a un grupo de usuarios o a todos los usuarios de su organización.

Por ejemplo, si usar unidades extraíbles está prohibido en su organización, pero los administradores necesitan utilizarlas, puede permitir su uso solo para un grupo de administradores. Para ello, deberá agregar las unidades extraíbles a la lista de dispositivos de confianza y configurar los permisos de acceso de los usuarios.

Kaspersky Endpoint Security ofrece distintos métodos para agregar un dispositivo a la lista de dispositivos de confianza:

- Si no utiliza Kaspersky Security Center en su organización, puede conectar el dispositivo a un equipo y agregarlo a la lista de dispositivos de confianza a través de los ajustes de la aplicación. Para distribuir esta lista a todos los equipos de la organización, use el procedimiento de exportación e importación o permita que las listas de las directivas se combinen.

- Si utiliza Kaspersky Security Center en su organización, puede detectar todos los dispositivos conectados y crear una lista de dispositivos de confianza en la directiva. La lista de dispositivos de confianza estará disponible en todos los equipos que estén sujetos a la directiva.

Kaspersky Endpoint Security 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 anteriores. 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. Si lo prefiere, también puede enviar una solicitud con una descripción de lo que ocurre al servicio de soporte técnico (a través de Kaspersky CompanyAccount).

- 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 con una descripción de lo que necesita al servicio de soporte técnico (a través de Kaspersky CompanyAccount).

## Añadir un dispositivo a la lista De confianza desde la interfaz de la aplicación

Por defecto, cuando se agrega un dispositivo a la lista de dispositivos de confianza, el acceso a ese dispositivo se otorga a todos los usuarios (el grupo de usuarios Todos).

*Para añadir un dispositivo a la lista De confianza desde la interfaz de la aplicación:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración**, 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 selecciona en la lista desplegable **Mostrar dispositivos conectados**.
5. En la lista de dispositivos, seleccione el dispositivo que desea agregar a la lista de confianza.
6. En el campo **Comentario**, puede proporcionar toda la 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.

## Añadir un dispositivo a la lista De confianza desde Kaspersky Security Center

Cuando Kaspersky Endpoint Security está instalado en los equipos y el componente Control de dispositivos está habilitado, Kaspersky Security Center recibe información sobre los dispositivos. Para que un dispositivo pueda agregarse a la lista De confianza, Kaspersky Security Center debe tener información sobre el mismo.

Para agregar un dispositivo a la lista De confianza, pueden usarse los siguientes datos:

- **Dispositivos por Id.** Cada dispositivo tiene un identificador único (id. de hardware, también denominado HWID). Puede ver el Id. en las propiedades del dispositivo usando las herramientas del sistema operativo. Un id. de dispositivo típico podría ser `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id.
- **Dispositivos por modelo**. Cada dispositivo tiene un id. de proveedor (VID) y un id. de producto (PID). Puede ver los ID. en las propiedades del dispositivo usando las herramientas del sistema operativo. Los valores VID y PID deben especificarse en este formato: `VID_1234&PID_5678`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.
- **Dispositivos por máscara de id.** Si tiene dispositivos con identificadores similares, puede agregarlos a la lista de dispositivos de confianza utilizando máscaras. El carácter `*` le permitirá representar cuantos caracteres sea

necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Una máscara típica podría ser `WDC_C*`.

- **Dispositivos por máscara de modelo**. Si tiene dispositivos con identificadores VID o PID similares (por ejemplo, dispositivos de un mismo fabricante), puede utilizar máscaras para agregarlos a la lista de dispositivos de confianza. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `VID_05AC & PID_ *`.

*Para agregar 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 ficha **Dispositivos de confianza**.
7. Active la casilla **Combinar valores al heredar** si desea crear una lista de dispositivos de confianza unificada para todos los equipos de la empresa.

   La lista de dispositivos de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Los dispositivos de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlos. No podrá modificarlos ni eliminarlos.
8. Haga clic en el botón **Agregar** y seleccione el método que desee usar para agregar los dispositivos a la lista.
9. Para filtrar los dispositivos, seleccione un tipo de dispositivo en la lista desplegable **Tipo de dispositivo** (por ejemplo, **Unidades extraíbles**).
10. En el campo **Nombre o modelo**, escriba un identificador, modelo (VID y PID) o máscara de dispositivo, según el método que haya elegido para agregar los dispositivos.

    La opción de agregar dispositivos por máscara de modelo (VID y PID) funciona del siguiente modo: cuando se introduce una máscara de modelo que no se corresponde con ningún modelo, Kaspersky Endpoint Security busca una correspondencia entre la máscara y el id. de dispositivo (HWID). Para ello tiene en cuenta únicamente la parte del id. que determina cuál es el tipo de dispositivo y quién es su fabricante (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Si se encuentra una coincidencia entre la máscara de modelo y esta parte del id. de dispositivo, los dispositivos alcanzados por la máscara se agregarán a la lista de dispositivos de confianza del equipo. Paralelamente, la lista de dispositivos en Kaspersky Security Center se mantendrá vacía cuando haga clic en el botón **Actualizar**. Para que la lista de dispositivos se muestre correctamente, deberá agregar los dispositivos utilizando una máscara de id. de dispositivo.
11. Para filtrar los dispositivos, en el campo **Equipo** escriba el nombre del equipo (o la máscara del nombre del equipo) al que se encuentre conectado el dispositivo.

    El carácter `*` le permitirá representar cuantos caracteres sea necesario. El carácter `?` representa cualquier carácter individual.

12. Haga clic en el botón **Actualizar**.

    En la tabla, verá una lista con los dispositivos que cumplan con las condiciones de filtrado.

13. Active las casillas adyacentes a los dispositivos que desee agregar a la lista De confianza.

14. En el campo **Comentario**, indique por qué decidió agregar los dispositivos a la lista de dispositivos de confianza.

15. Haga clic en el botón **Seleccionar**, ubicado a la derecha del campo **Autorizar a los siguientes usuarios o grupos de usuarios**.

16. Seleccione un usuario o grupo de Active Directory y confirme su elección.

    De manera predeterminada, el grupo Everyone tiene acceso a los dispositivos de confianza.

17. Guarde los cambios.

Cuando se conecte un dispositivo, Kaspersky Endpoint Security revisará la lista de dispositivos de confianza en nombre del usuario autorizado. Si el dispositivo conectado es de confianza, Kaspersky Endpoint Security permitirá que se acceda al mismo sin restricciones de permisos, incluso si el acceso a ese tipo de dispositivo o a su bus de conexión se encuentra bloqueado. Si el dispositivo no es de confianza y no se permite acceder a él, existe un procedimiento para solicitar acceso a dispositivos bloqueados.

## Exportar e importar la lista de dispositivos de confianza

Si desea distribuir la lista de dispositivos de confianza a todos los equipos de la organización, puede usar el procedimiento de exportación/importación.

Por ejemplo, si necesita distribuir una lista de unidades extraíbles de confianza, haga lo siguiente:

1. Conecte las unidades extraíbles a su propio equipo, una tras otra.

2. En la configuración de Kaspersky Endpoint Security, agregue las unidades extraíbles a la lista de dispositivos de confianza. Si lo considera necesario, configure los permisos de acceso para los usuarios. Por ejemplo, limite el uso de unidades extraíbles a los administradores.

3. Exporte la lista de dispositivos de confianza mediante la interfaz de Kaspersky Endpoint Security (consulte las instrucciones más abajo).

4. Distribuya el archivo con la lista de dispositivos de confianza a los demás equipos de la red. Para ello, copie el archivo a una carpeta compartida o utilice el método que considere conveniente.

5. Importe la lista de dispositivos de confianza en la configuración de Kaspersky Endpoint Security de los demás equipos de la organización (consulte las instrucciones más abajo).

*Para importar o exportar la lista de dispositivos de confianza:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control de dispositivos**.

3. En el bloque **Configuración**, haga clic en el botón **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.

4. Para exportar la lista de dispositivos de confianza.

a. Seleccione los dispositivos de confianza que desea exportar.

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

c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista exportada. Seleccione también la carpeta en la que se guardará este archivo.

d. Haga clic en el botón **Guardar**.

Kaspersky Endpoint Security exportará la lista de dispositivos de confianza completa al archivo XML.

5. Para importar la lista de dispositivos de confianza:

a. En la lista desplegable **Importar**, seleccione la acción correspondiente: **Importar y agregar a existente(s)** o **Importar y reemplazar existente(s)**.

b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de dispositivos de confianza.

c. Haga clic en el botón **Abrir**.

Cuando ya exista una lista de dispositivos de confianza en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

6. Guarde los cambios.

Cuando se conecte un dispositivo, Kaspersky Endpoint Security revisará la lista de dispositivos de confianza en nombre del usuario autorizado. Si el dispositivo conectado es de confianza, Kaspersky Endpoint Security permitirá que se acceda al mismo sin restricciones de permisos, incluso si el acceso a ese tipo de dispositivo o a su bus de conexión se encuentra bloqueado.

## Obtención de acceso a un dispositivo bloqueado

Al configurar el componente Control de dispositivos, existe el riesgo de bloquear inadvertidamente el acceso a un dispositivo que se necesita para trabajar.

Si no utiliza Kaspersky Security Center en su organización, puede brindar acceso a un dispositivo a través de los ajustes de Kaspersky Endpoint Security. Por ejemplo, puede agregar el dispositivo a la lista de dispositivos de confianza o deshabilitar el componente Control de dispositivos en forma temporal.

Si en su organización sí utilizan Kaspersky Security Center y los equipos tienen una directiva aplicada, puede otorgar acceso al dispositivo a través de la Consola de administración.

### Modo con conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo con conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. También es necesario que el equipo pueda comunicarse con el Servidor de administración.

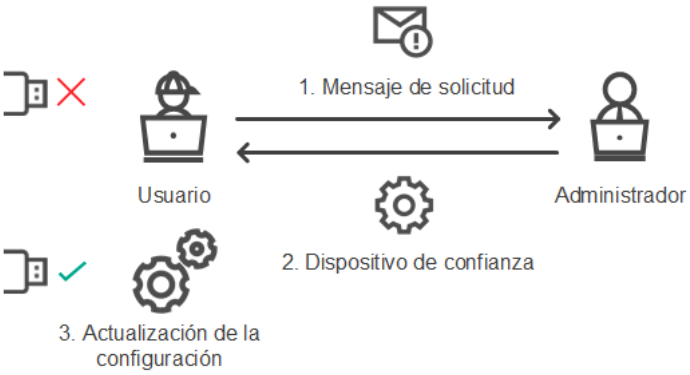
Estos son los pasos para otorgar acceso a un dispositivo en el modo con conexión:

1. El usuario envía un mensaje con una solicitud de acceso al administrador.

2. El administrador agrega el dispositivo a la lista de dispositivos de confianza.

Para agregar un dispositivo de confianza, existen dos alternativas: modificar una directiva aplicada al grupo de administración o modificar la configuración local de la aplicación instalada en un equipo específico.

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.

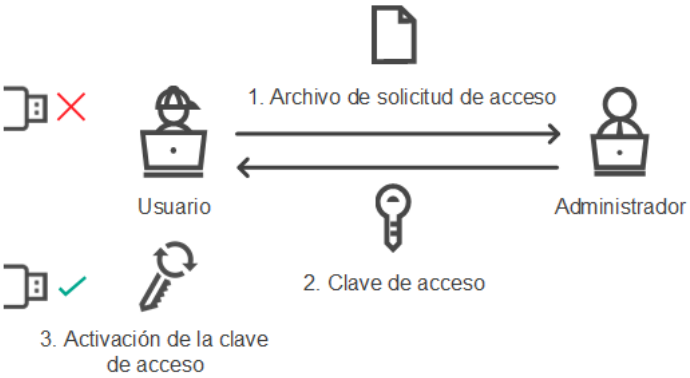
Si necesita otorgar acceso temporal a un dispositivo, pero no puede agregarlo a la lista de dispositivos de confianza, puede utilizar el modo sin conexión. Este modo permite otorgar acceso a un dispositivo bloqueado aun cuando un equipo no tiene conexión a la red o se encuentra fuera de la red corporativa.

Estos son los pasos para otorgar acceso a un dispositivo en el modo sin conexión:

1. El usuario crea un archivo de solicitud de acceso y se lo envía al administrador.

2. Con el archivo de solicitud de acceso, el administrador crea una clave de acceso y se la envía al usuario.

3. El usuario activa la clave de acceso.




Esquema para otorgar acceso a un dispositivo en el modo sin conexión

# Modo con conexión para otorgar acceso

Para que se pueda otorgar acceso a un dispositivo bloqueado utilizando el modo con conexión, Kaspersky Security Center debe estar instalado en la organización y el equipo debe tener una directiva aplicada. También es necesario que el equipo pueda comunicarse con el Servidor de administración.

*Para solicitar acceso a un dispositivo bloqueado como usuario:*

1. Conecte el dispositivo al equipo.

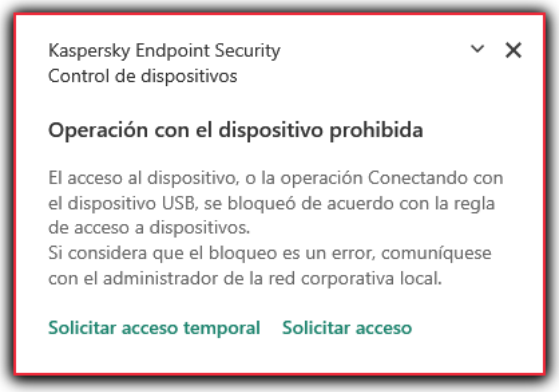
   Kaspersky Endpoint Security mostrará una notificación para indicar que el acceso al dispositivo está bloqueado (vea la imagen de más abajo).

2. Haga clic en el vínculo **Solicitar acceso**.

   Se abrirá la ventana **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 agregue a la lista de dispositivos de confianza y la configuración de Kaspersky Endpoint Security se actualice en el equipo.




Notificación del 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 solicitudes de acceso temporal** debe estar activada.

*Para solicitar acceso a un dispositivo bloqueado como usuario:*

1. Conecte el dispositivo al equipo.

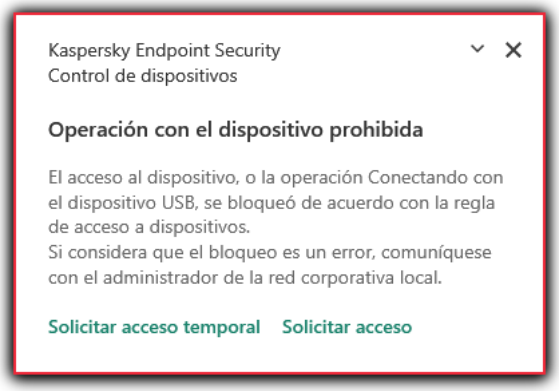
   Kaspersky Endpoint Security mostrará una notificación para indicar que el acceso al dispositivo está bloqueado (vea la imagen de más abajo).

2. Haga clic en el vínculo **Solicitar acceso temporal**.

Se abrirá la ventana **Solicitar acceso al dispositivo**, en la que encontrará una lista de dispositivos conectados.

3. En la lista de dispositivos conectados, seleccione el dispositivo al que desee obtener acceso.
4. Haga clic en el botón **Generar archivo de solicitud de acceso**.
5. En el campo **Duración del acceso**, especifique el período durante el cual quiera tener acceso al dispositivo.
6. Guarde el archivo en el equipo.

Como resultado, se descargará al equipo un archivo de solicitud de acceso (cuya extensión será *.akey). Envíe este archivo al administrador de la LAN corporativa utilizando cualquier método a su disposición.




Notificación del Control de dispositivos

*Para crear una clave de acceso para un dispositivo bloqueado como administrador:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenece el equipo cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la lista de equipos cliente, seleccione el equipo a cuyo usuario se le debe otorgar acceso temporal a un dispositivo bloqueado.
5. En el menú contextual del equipo, seleccione el elemento **Otorgar acceso en el modo fuera de línea**.
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 de acceso** es el mismo que indicó el usuario al crear el archivo de solicitud de acceso.
9. Especifique el valor de **Activar antes de**.

   Esta configuración define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado con la clave de acceso provista.
10. Guarde el archivo de clave de acceso en el equipo.

Como resultado, se descargará al equipo una clave de acceso para el dispositivo bloqueado. Los archivos de clave de acceso tienen la extensión *.acode. Envíe el archivo de clave de acceso al usuario utilizando cualquier método a su disposición.

*Para activar una clave de acceso como usuario:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Solicitar 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. Haga clic en el botón **Abrir**.

   Se abrirá una ventana con información sobre el acceso que le han otorgado.
6. Haga clic en **Aceptar**.

Como resultado, el usuario obtendrá acceso al dispositivo por el tiempo que haya definido el administrador. El usuario tendrá acceso completo (derechos de lectura y de escritura) al dispositivo. Cuando la clave caduque, se bloqueará el acceso al dispositivo. Si el usuario necesita acceso permanente al dispositivo, agregue el dispositivo a la lista de dispositivos de confianza.

## Edición de plantillas de mensajes del Control de dispositivos

Cuando el usuario intenta acceder a un dispositivo bloqueado, Kaspersky Endpoint Security muestra un mensaje en el que se indica que el acceso al dispositivo está bloqueado o que la operación con el contenido del dispositivo está prohibida. Si el usuario cree que el acceso al dispositivo se bloqueó por error o que una operación con contenido del dispositivo se prohibió por equivocación, puede enviar un mensaje al administrador de la red corporativa local haciendo clic en el vínculo presente en el mensaje en pantalla sobre la acción bloqueada.

Se dispone de plantillas para los mensajes sobre acceso bloqueado a dispositivos u operaciones prohibidas con contenido del dispositivo, y para los mensajes que se envían al administrador. Puede modificar las plantillas de mensajes.

*Para modificar las plantillas de mensajes del Control de dispositivos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control de dispositivos:

   - **Mensaje para bloqueos**. Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo.
   - **Mensaje para el administrador**. Plantilla del mensaje que se envía al administrador de la red de área local cuando el usuario considera que el acceso a un dispositivo se ha bloqueado por error o, de manera similar, que la posibilidad de realizar una operación con el contenido de un dispositivo se ha bloqueado por error.

4. Guarde los cambios.

## Anti-Bridging

Anti-Bridging impide establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red. La finalidad es resguardar la red de la empresa de los ataques que puedan realizarse a través de redes desprotegidas y no autorizadas.

Para regular la posibilidad de establecer conexiones de red, Anti-Bridging utiliza *reglas de conexión*.

Las reglas de conexión se crean para los siguientes tipos predeterminados de dispositivos:

- Adaptadores de red
- Adaptadores Wi-Fi
- Módems

Si se habilita una regla de conexión, Kaspersky Endpoint Security:

- Bloquea la conexión activa al establecer una nueva conexión, si el tipo de dispositivo especificado en la regla se usa para ambas conexiones.
- Bloquea las conexiones establecidas mediante la utilización de los tipos de dispositivo para los cuales se utilizan las reglas de menor prioridad.

## Habilitar Anti-Bridging

Por defecto, el componente Anti-Bridging está deshabilitado.

*Para habilitar Anti-Bridging:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control de dispositivos**.
3. En el bloque **Configuración**, haga clic en el botón **Anti-Bridging**.
4. Use el interruptor **Habilitar Anti-Bridging** para habilitar o deshabilitar esta característica.
5. Guarde los cambios.

Una vez habilitada la protección Anti-Bridging, Kaspersky Endpoint Security bloquea las conexiones ya establecidas de conformidad con las reglas de conexión.

## Edición del estado de una regla de conexiones

*Para cambiar el estado de una regla de conexión:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración**, 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 habilitar o deshabilitar la regla.
6. Guarde los cambios.

## Cambio de prioridad de una regla de conexión

*Para cambiar la prioridad de una regla de conexión:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de dispositivos**.
3. En el bloque **Configuración**, haga clic en el botón **Anti-Bridging**.
4. En el bloque **Reglas para los dispositivos**, seleccione la regla cuya prioridad desea cambiar.
5. Utilice los botones **Subir**/**Bajar** para configurar la prioridad de la regla de conexión.

   Cuanto más arriba está una regla en la tabla, mayor es su prioridad. El componente Anti-Bridging bloquea todas las conexiones excepto una conexión establecida usando el tipo de dispositivo para el cual se utiliza la regla de la prioridad más alta.
6. Guarde los cambios.

## Control de anomalías adaptativo

Este componente solo está disponible en Kaspersky Endpoint Security for Business Advanced y Kaspersky Total Security for Business. Para más información sobre Kaspersky Endpoint Security for Business, visite el *sitio web de Kaspersky*.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos conectados a una red corporativa. Para ello utiliza una serie de reglas, diseñadas para buscar comportamientos que no se consideran usuales (por ejemplo, la regla *Inicio de Microsoft PowerShell desde una aplicación de ofimática*). Los especialistas de Kaspersky crean estas reglas basándose en casos característicos de actividad maliciosa. La manera en que el Control de anomalías adaptativo responde ante cada regla es configurable; esto significa que, por ejemplo, es posible permitir la ejecución de scripts de PowerShell que se hayan creado para automatizar ciertos aspectos de un flujo de trabajo. Las reglas se actualizan junto con las bases de datos de Kaspersky Endpoint Security. No obstante, las actualizaciones para las reglas deben confirmarse manualmente.

## Configuración del Control de anomalías adaptativo

Los pasos para configurar el Control de anomalías adaptativo son los siguientes:

1. Usar el modo de aprendizaje del Control de anomalías adaptativo.

   Una vez que el Control de anomalías adaptativo se habilita, sus reglas entran en un *modo de aprendizaje*. Mientras dicho modo está activo, el Control de anomalías adaptativo monitorea la activación de las reglas y envía los eventos de activación a Kaspersky Security Center. El tiempo de aprendizaje varía según la regla. Quienes definen la duración son los expertos de Kaspersky. Lo normal es que el modo de aprendizaje esté activo por dos semanas.

   Si una regla no se activa en lo absoluto durante el período de aprendizaje, el componente considerará que las acciones asociadas con la regla son atípicas. En consecuencia, Kaspersky Endpoint Security bloqueará cualquier acción vinculada con esa regla.

   Si una regla sí se activa durante el período de aprendizaje, Kaspersky Endpoint Security dejará constancia de los eventos en el informe de activación de las reglas y en el repositorio **Activación de reglas en modo Aprendizaje inteligente**.

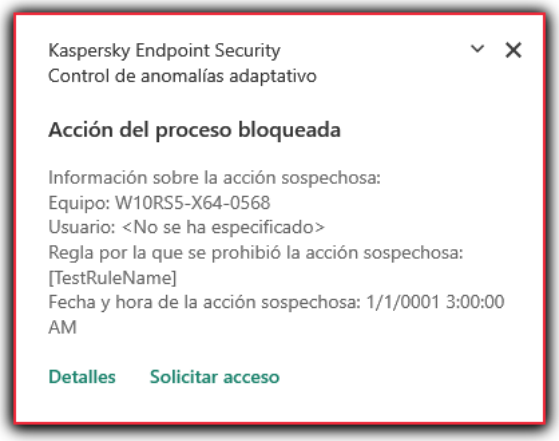
2. Analizar el informe de activación de las reglas.

   El administrador analiza el informe de activación de las reglas o el contenido del repositorio **Activación de reglas en modo Aprendizaje inteligente**. A continuación, selecciona cómo reaccionará el Control de anomalías adaptativo cuando se active una regla; las opciones posibles son permitir y bloquear. El administrador también puede optar por seguir controlando el funcionamiento de la regla y extender la duración del modo de aprendizaje. Si el administrador no realiza ninguna acción, la aplicación seguirá operando en modo de aprendizaje. El plazo de aprendizaje se reiniciará.

El componente Control de anomalías adaptativo se configura en tiempo real. Los canales de configuración son los siguientes:

- El Control de anomalías adaptativo comienza a bloquear automáticamente las acciones asociadas con las reglas que nunca se activaron en el modo de aprendizaje.
- Kaspersky Endpoint Security agrega reglas nuevas o elimina las que han quedado obsoletas.
- El administrador configura el funcionamiento del Control de anomalías adaptativo tras revisar el informe de activación de reglas y el contenido del repositorio **Activación de reglas en modo Aprendizaje inteligente**. Se recomienda revisar el informe de activación de reglas y el contenido **del repositorio Activación de reglas en modo Aprendizaje inteligente**.

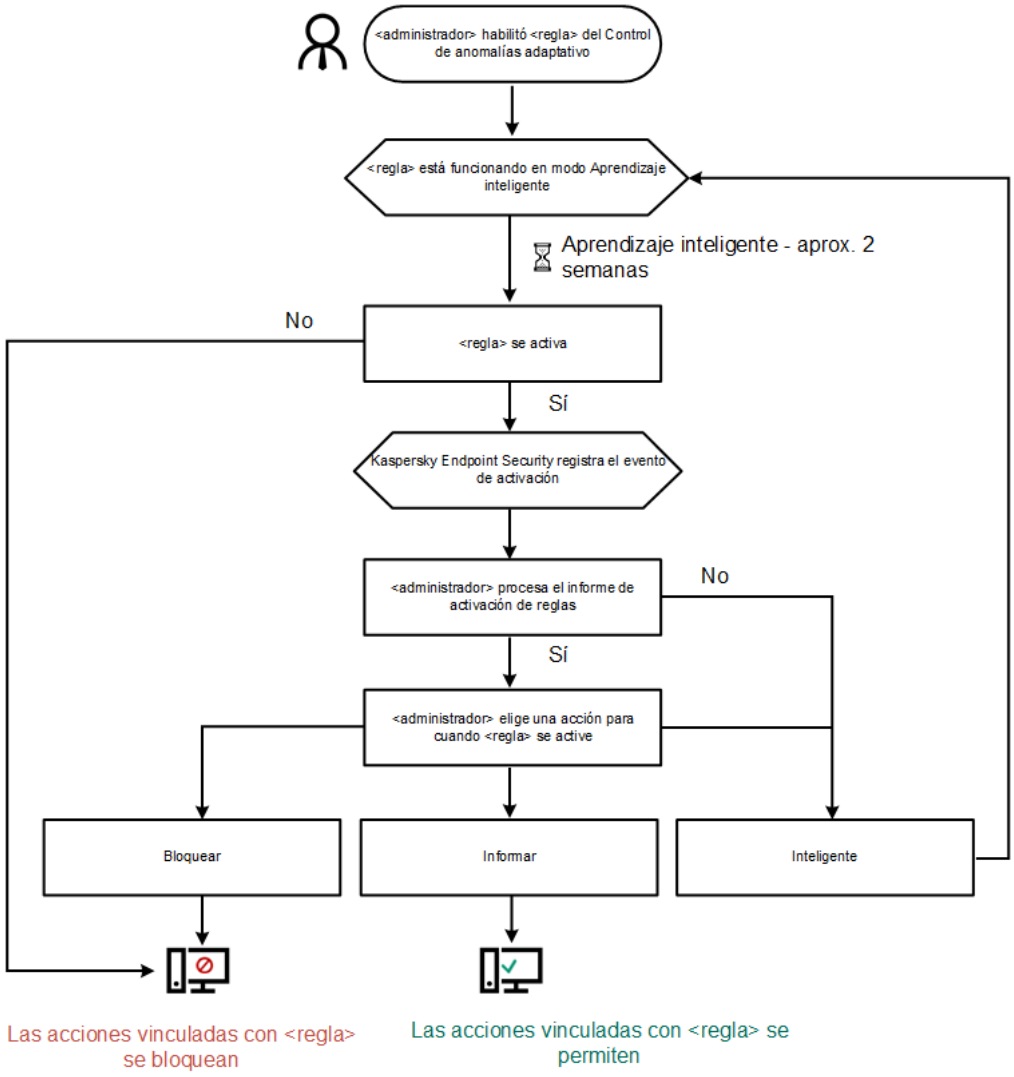
Cuando una aplicación maliciosa intente realizar una acción, Kaspersky Endpoint Security bloqueará el intento y mostrará una notificación (consulte la siguiente imagen).




Notificación del Control de anomalías adaptativo

## Algoritmo de funcionamiento del Control de anomalías adaptativo

Para determinar si una acción asociada a una regla debe permitirse o bloquearse, Kaspersky Endpoint Security usa el algoritmo de la siguiente imagen.




Algoritmo de funcionamiento del Control de anomalías adaptativo

## Habilitación y deshabilitación del Control de anomalías adaptativo

De manera predeterminada, el Control de anomalías adaptativo está habilitado.

*Para habilitar o deshabilitar el Control de anomalías adaptativo:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de anomalías adaptativo**.
3. Utilice el interruptor **Control de anomalías adaptativo** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

## Habilitación y deshabilitación de una regla del Control de anomalías adaptativo

*Para habilitar o deshabilitar una regla del Control de anomalías adaptativo:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **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 ofimática*) y amplíe el conjunto.
5. Seleccione una regla (por ejemplo, Iniciar *Windows PowerShell desde aplicaciones de ofimática*).
6. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la regla de Control de anomalías adaptativo.
7. Guarde los cambios.

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

*Para cambiar lo que ocurre cuando se activa una regla del Control de anomalías adaptativo:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **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 **Modificar**.

   Se abre la ventana de propiedades del Control de anomalías adaptativo.

6. En el bloque **Acción**, seleccione una de las siguientes opciones:

   - **Inteligente**. Si elige esta opción, la regla del Control de anomalías adaptativo funcionará en un modo de aprendizaje inteligente durante un plazo que han definido los expertos de Kaspersky. En este modo, cuando una regla del Control de anomalías adaptativo se activa, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y agrega una entrada de registro en el repositorio **Activación de reglas en modo de aprendizaje inteligente** del Servidor de administración de Kaspersky Security Center. Cuando concluye el período de aprendizaje inteligente, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y agrega una entrada de registro con información sobre la actividad.

   - **Bloquear**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security bloquea la actividad alcanzada por la regla y deja registro de la actividad.

   - **Informar**. Cuando se activa una regla del Control de anomalías adaptativo y esta es la acción seleccionada, Kaspersky Endpoint Security permite la actividad alcanzada por la regla y deja registro de la actividad.

7. Guarde los cambios.

## Crear una exclusión para una regla del Control de anomalías adaptativo

No es posible crear más de 1000 exclusiones para las reglas del Control de anomalías adaptativo. No se recomienda crear más de 200 exclusiones. Si necesita reducir el número de exclusiones que utiliza, considere usar máscaras en la configuración de las exclusiones.

Una exclusión de una regla del Control de anomalías adaptativo incluye una descripción de los objetos de origen y de destino. El *objeto de origen* es el que realiza las acciones. El *objeto de destino* es el que se ve afectado por dichas acciones. Por ejemplo, abre un archivo de nombre `archivo.xlsx`. Por lo tanto, se carga un archivo de la biblioteca con la extensión DLL en la memoria del equipo. Un navegador utiliza esta biblioteca (cuyo archivo ejecutable es `navegador.exe`). En 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.

*Si desea crear una exclusión para una regla del Control de anomalías adaptativo:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control de anomalías adaptativo**.

3. En el bloque **Reglas**, haga clic en el botón **Modificar reglas**.

   Se abre la lista de reglas de Control de anomalías adaptativo.

4. Seleccione una regla en la tabla.

5. Haga clic en el botón **Modificar**.

Se abre la ventana de propiedades del Control de anomalías adaptativo.

6. En el bloque **Exclusiones**, haga clic en el botón **Agregar**.

   Se abre la ventana de propiedades de la exclusión.

7. Seleccione el usuario en el cual desea configurar una exclusión.

   El Control de anomalías adaptativo no admite exclusiones para grupos de usuarios. Si selecciona un grupo de usuarios, Kaspersky Endpoint Security no aplica la exclusión.

8. En el campo **Descripción**, describa la exclusión.

9. Defina los parámetros del objeto de origen o del proceso de origen iniciado por el objeto:

   - **Proceso de origen**. Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, `C:\Dir\Archivo.exe` o `Dir\*.exe`).
   - **Hash del proceso de origen**. Código hash de 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 de archivo.

   La regla del Control de anomalías adaptativo no se aplicará a las acciones que el objeto realice o a los procesos que el objeto inicie.

10. Especifique los parámetros del objeto de destino o de los procesos de destino iniciados en los que el objeto esté involucrado.

    - **Proceso de destino**. Ruta (o máscara de ruta) de acceso al archivo o a una carpeta con archivos (por ejemplo, `C:\Dir\Archivo.exe` o `Dir\*.exe`).
    - **Hash del proceso de destino**. Código hash de archivo.
    - **Objeto de destino**. Comando para iniciar el proceso de destino. Para especificar el comando, utilice la plantilla `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 del objeto de destino**. Código hash de archivo.

    La regla del Control de anomalías adaptativo no se aplicará a las acciones que afecten al objeto o a los procesos en los que el objeto esté involucrado.

11. Guarde los cambios.

## Exportar e importar exclusiones para reglas del Control de anomalías adaptativo

*Si desea exportar o importar la lista de exclusiones para las reglas seleccionadas:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **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 la regla cuyas excepciones desea exportar.
   b. Haga clic en el botón **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Confirme que desea exportar solo las exclusiones seleccionadas, o bien exporte la lista completa de exclusiones.
   e. Haga clic en el botón **Guardar**.
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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
6. Guarde los cambios.

## Actualización de las reglas del Control de anomalías adaptativo

Cuando se actualizan las bases de datos antivirus, la tabla de reglas del Control de anomalías adaptativo puede modificarse: puede ocurrir que se incorporen reglas nuevas y que se eliminen otras existentes. Si hay una actualización de reglas que está pendiente de aplicarse, Kaspersky Endpoint Security distingue las reglas del Control de anomalías adaptativo que van a agregarse o eliminarse.

Hasta que se aplica una actualización, las reglas pendientes de eliminarse se siguen mostrando en la tabla de reglas, pero Kaspersky Endpoint Security les asigna el estado *Deshabilitado*. No es posible cambiar la configuración de estas reglas.

*Para actualizar las reglas del Control de anomalías adaptativo:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → 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 del Control de anomalías adaptativo, Kaspersky Endpoint Security muestra un mensaje que indica que las acciones potencialmente dañinas están bloqueadas. Si el usuario cree que la acción está bloqueada por error, puede usar el vínculo incluido en el texto del mensaje para enviar un mensaje al administrador de la red corporativa local.

Hay plantillas especiales disponibles para el mensaje sobre el bloqueo de acciones potencialmente dañinas y para que el mensaje se envíe al administrador. Puede modificar las plantillas de mensajes.

*Para modificar una plantilla de mensaje:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control de anomalías adaptativo**.
3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control de anomalías adaptativo:
   - **Bloqueo**. Plantilla del mensaje que se le mostrará al usuario cuando se active una regla del Control de anomalías adaptativo para bloquear una acción atípica.
   - **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la red local corporativa si considera que una acción se bloqueó por error.
4. Guarde los cambios.

## Visualización de los informes del Control de anomalías adaptativo

*Para visualizar los informes del Control de anomalías adaptativo:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la sección **Controles de seguridad**, elija la subsección **Control de anomalías adaptativo**.

   En la parte derecha de la ventana, verá las opciones del componente Control de anomalías adaptativo.
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 el botón **Informe de estado de las reglas**.
   - Si desea ver un informe sobre la activación de las reglas del Control de anomalías adaptativo, haga clic en el botón **Informe de activación de las reglas**.
7. Se inicia el proceso de generación del informe.

El informe se muestra en una ventana nueva.

## Control de aplicaciones

El componente Control de aplicaciones se utiliza para gestionar la ejecución de aplicaciones en los equipos de los usuarios. Permite, con ello, implementar una política de seguridad corporativa que regule el uso de aplicaciones. Gracias a las restricciones de acceso, el componente también ayuda a reducir el riesgo de que los equipos se infecten.

Los pasos para configurar Control de aplicaciones son los siguientes:

1. Creación de categorías de aplicaciones.

   El administrador crea categorías con las aplicaciones que desea controlar. Las categorías de aplicaciones impactan en todos los equipos de una red corporativa, independientemente del grupo de administración al que pertenecen. Las categorías se crean sobre la base de distintos criterios: categoría KL (por ejemplo, *Navegadores*), hash del archivo, proveedor de la aplicación y otros.
2. Creación de reglas de Control de aplicaciones.

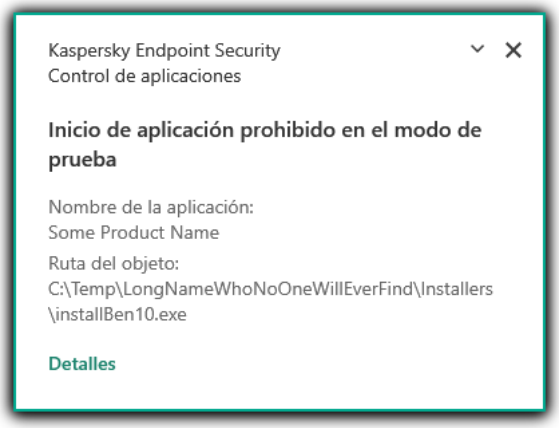
   El administrador crea reglas de Control de aplicaciones dentro de la directiva asignada a un grupo de administración. Las reglas contienen las distintas categorías de aplicaciones y el estado de ejecución (inicio permitido o bloqueado) asignado a las aplicaciones de esas categorías.
3. Selección del modo de Control de aplicaciones.

   El administrador decide el modo para trabajar con aplicaciones que no están contempladas en ninguna de las reglas (lista de autorización y de bloqueo).

Cuando un usuario intenta ejecutar una aplicación prohibida, Kaspersky Endpoint Security se lo impide y le muestra una notificación (vea la imagen de más abajo).

Existe un *modo de prueba*, diseñado para verificar la configuración de Control de aplicaciones. Cuando se utiliza este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite que se ejecute cualquier aplicación, esté o no prohibida.
- Muestra una notificación cuando se inicia una aplicación prohibida y agrega el evento al informe almacenado en el equipo del usuario.
- Transfiere información sobre la ejecución de aplicaciones prohibidas a Kaspersky Security Center.




Notificación de Control de aplicaciones

## Modos de funcionamiento de Control de aplicaciones

El componente Control de aplicaciones funciona en dos modos:

- **Lista de bloqueo**. En este modo, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto por las que se hayan prohibido a través de las reglas de Control de aplicaciones.

  Este modo de Control de aplicaciones está habilitado por defecto.

- **Lista de autorización**. En este modo, Control de aplicaciones no permite que ningún usuario inicie ninguna aplicación, excepto por las que se hayan permitido (y no prohibido) a través de las reglas de Control de aplicaciones.

  Si se configuran completamente las reglas de autorización del Control de aplicaciones, el componente bloquea el inicio de todas las aplicaciones nuevas que no han sido verificadas por el administrador de la red LAN, mientras que permite el funcionamiento del sistema operativo y de las aplicaciones de confianza de las que dependen los usuarios para hacer su trabajo.

  Puede leer las recomendaciones sobre cómo configurar las reglas de control de aplicaciones en el modo de lista de autorización.

El Control de aplicaciones se puede configurar para funcionar en estos modos, tanto a través de la interfaz local de Kaspersky Endpoint Security como por medio de Kaspersky Security Center.

Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas necesarias para las siguientes tareas:

- Creación de categorías de aplicaciones.

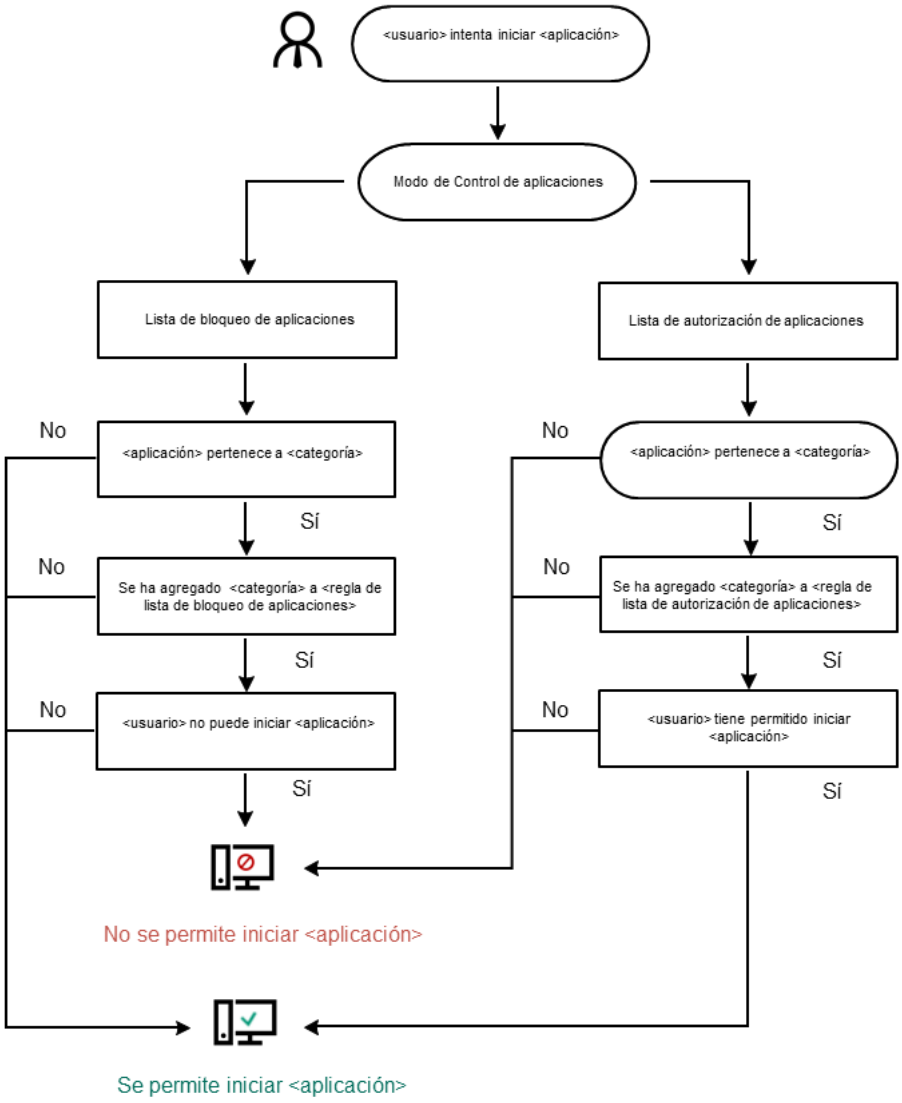
  Las reglas de Control de aplicaciones creadas en la Consola de administración de Kaspersky Security Center se basan en sus categorías de aplicaciones personalizadas, y no en condiciones de inclusión y exclusión como es el caso de la interfaz local de Kaspersky Endpoint Security.

- Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN.

Por este motivo se recomienda utilizar Kaspersky Security Center para configurar el funcionamiento del componente Control de aplicaciones.

### Algoritmo de funcionamiento de Control de aplicaciones

Kaspersky Endpoint Security utiliza un algoritmo para decidir si una aplicación podrá iniciarse (vea la siguiente imagen).




Algoritmo de funcionamiento de Control de aplicaciones

## Limitaciones de la funcionalidad del Control de aplicaciones

El funcionamiento del componente Control de aplicaciones está limitado en los casos siguientes:

- Cuando se actualiza la versión de la aplicación, no se admite la importación de los parámetros del componente Control de aplicaciones.

- Cuando se actualiza la versión de la aplicación, la importación de la configuración 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 11.6.0 para Windows.

  Cuando se actualizan versiones de la aplicación diferentes a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, la configuración de Control de aplicaciones se tiene que configurar de nuevo a fin de restaurar este componente a un estado operativo.

- Si no hay ninguna conexión con servidores de KSN, Kaspersky Endpoint Security recibe información sobre la reputación de las aplicaciones y sus módulos solo desde bases de datos locales.

  La lista de aplicaciones asignadas por Kaspersky Endpoint Security a la categoría KL **Aplicaciones de confianza en base a la reputación en KSN**, cuando hay una conexión a servidores KSN disponible, puede ser diferente a la lista de aplicaciones asignadas por Kaspersky Endpoint Security a la categoría KL **Aplicaciones de confianza en base a la reputación en KSN** cuando no hay conexión a KSN.

- En la base de datos de Kaspersky Security Center, se puede guardar información sobre 150 000 archivos procesados. Una vez que se alcance este número de registros, no se procesarán los archivos nuevos. Para reanudar operaciones del inventario, debe eliminar los archivos que se inventariaron anteriormente en la base de datos de Kaspersky Security Center desde el equipo en el cual está instalado Kaspersky Endpoint Security.

- El componente no controla el inicio de scripts a menos que el script se envíe al intérprete mediante la línea de comandos.

  Si las reglas de Control de aplicaciones permiten el inicio de un intérprete, el componente no bloqueará un script iniciado desde este intérprete.

  Si al menos uno de los scripts especificados en la línea de comandos del intérprete está bloqueado desde el inicio por las reglas de control de la aplicación, el componente bloquea todos los scripts, especificados en la línea de comandos del intérprete.

- El componente no controla el inicio de scripts desde intérpretes que no son admitidos por Kaspersky Endpoint Security.

  Kaspersky Endpoint Security admite los siguientes intérpretes:

  - Java
  - PowerShell

  Se admiten los siguientes tipos de intérpretes:

  - %ComSpec%;
  - %SystemRoot%\\system32\\regedit.exe;
  - %SystemRoot%\\regedit.exe;
  - %SystemRoot%\\system32\\regedt32.exe;
  - %SystemRoot%\\system32\\cscript.exe;

- %SystemRoot%\\system32\\wscript.exe;
- %SystemRoot%\\system32\\msiexec.exe;
- %SystemRoot%\\system32\\mshta.exe;
- %SystemRoot%\\system32\\rundll32.exe;
- %SystemRoot%\\system32\\wwahost.exe;
- %SystemRoot%\\syswow64\\cmd.exe;
- %SystemRoot%\\syswow64\\regedit.exe;
- %SystemRoot%\\syswow64\\regedt32.exe;
- %SystemRoot%\\syswow64\\cscript.exe;
- %SystemRoot%\\syswow64\\wscript.exe;
- %SystemRoot%\\syswow64\\msiexec.exe;
- %SystemRoot%\\syswow64\\mshta.exe;
- %SystemRoot%\\syswow64\\rundll32.exe;
- %SystemRoot%\\syswow64\\wwahost.exe.

## Habilitación y deshabilitación del Control de aplicaciones

De manera predeterminada, el componente Control de aplicaciones está deshabilitado.

*Para habilitar y deshabilitar el Control de aplicaciones, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de aplicaciones**.
3. Utilice el interruptor **Control de aplicaciones** para habilitar o deshabilitar el componente.
4. Guarde los cambios.

Por lo tanto, si Control de aplicaciones está habilitado, 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 *Inventario*.

## Selección del modo de Control de aplicaciones

*Para seleccionar el Modo de control de aplicaciones, realice lo siguiente:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control de aplicaciones**.

3. En el bloque **Modo de Control de inicio de aplicaciones**, seleccione una de las siguientes opciones:

   - **Lista de bloqueo**. Si se selecciona esta opción, el Control de aplicaciones permite que todos los usuarios inicien cualquier aplicación, excepto en casos en que las aplicaciones cumplan con las condiciones de las reglas de bloqueo de Control de aplicaciones.

   - **Lista de autorización**. Si se selecciona esta opción, el Control de aplicaciones bloquea a todos los usuarios de iniciar alguna aplicación, excepto en casos en que las aplicaciones cumplen con las condiciones de reglas de habilitación del Control de aplicaciones.

     La regla **Imagen de oro** y la regla **Actualizadores de confianza** se definen inicialmente para el modo Lista de autorización. Estas reglas de Control de aplicaciones corresponden a las categorías de KL. La categoría KL "Imagen de oro" incluye programas que aseguran el funcionamiento normal del sistema operativo. La categoría KL "Actualizadores de confianza" incluye actualizadores de los proveedores del software más respetables. No puede eliminar estas reglas. No se puede modificar la configuración de estas reglas. De forma predeterminada, la regla **Imagen de oro** está habilitada, y la regla **Actualizadores de confianza** está deshabilitada. A todos los usuarios se les permite iniciar aplicaciones que coincidan con las condiciones de activación de estas reglas.

   Todas las reglas creadas durante el modo seleccionado se guardan después de cambiar el modo, de manera que las reglas se puedan 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 cuando se intente ejecutar una aplicación bloqueada**, seleccione la acción que deberá realizar el componente cuando un usuario intente iniciar una aplicación que esté bloqueada por reglas de Control de aplicaciones.

5. Seleccione la casilla **Controlar la carga de módulos DLL** si quiere 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 el módulo se guardará en un informe.

   Kaspersky Endpoint Security solamente supervisa los módulos DLL y los controladores cargados desde que se seleccionó la casilla. Reinicie el equipo después de seleccionar la casilla si quiere que Kaspersky Endpoint Security supervise todos los módulos DLL y los controladores, incluidos los cargados antes de iniciar Kaspersky Endpoint Security.

   Si planea supervisar la carga de controladores y módulos DLL, asegúrese de que una de las siguientes reglas esté habilitada en la configuración de Control de aplicaciones: la **Imagen de oro** predeterminada u otra regla que contenga la categoría KL "Certificados de confianza" y que garantice que los módulos DLL y los controladores de confianza se carguen antes del arranque de Kaspersky Endpoint Security. Habilitar la supervisión de la carga de módulos DLL y controladores cuando la regla **Imagen de oro** está deshabilitada puede causar inestabilidad en el sistema operativo.

   Recomendamos activar la protección con contraseña para configurar las opciones de la aplicación, de modo que sea posible desactivar las reglas que bloquean el inicio de los módulos DLL críticos y los controladores, sin modificar la configuración de la directiva del 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 por parte de los usuarios mediante reglas. Una regla de Control de aplicaciones está formada por una serie condiciones de activación y una serie de acciones. Cuando una regla se activa, Control de aplicaciones realiza la acción que la regla le indica (permitir o impedir que los usuarios inicien una aplicación).

## Condiciones de activación de regla

Una condición que activa una regla tiene la siguiente correlación: "tipo de condición - criterio de la condición - valor de la condición". Según las condiciones de activación de la regla, Kaspersky Endpoint Security aplica (o no) una regla a la aplicación.

Los siguientes tipos de condiciones se utilizan en las reglas:

- *Condiciones de inclusión*. Kaspersky Endpoint Security aplica la regla a la aplicación si la aplicación coincide con al menos una condición de inclusión.
- *Condiciones de exclusión*. Kaspersky Endpoint Security no aplica la regla a la aplicación si la aplicación coincide con al menos una de las condiciones de exclusión y no coincide con ninguna condición de inclusión.

Las condiciones de activación de regla se crean usando criterios. Se utilizan los siguientes criterios para crear reglas en Kaspersky Endpoint Security:

- Ruta de acceso de la carpeta que contiene el archivo ejecutable de la aplicación o ruta de acceso del archivo ejecutable de la aplicación.
- Metadatos: nombre del archivo ejecutable de la aplicación, versión del archivo ejecutable de la aplicación, nombre de la aplicación, versión de la aplicación, proveedor de la aplicación.
- Hash del archivo ejecutable de la aplicación
- Certificado: emisor, asunto, huella digital.
- Inclusión de la aplicación en una categoría KL.
- Ubicación del archivo ejecutable de la aplicación en un disco extraíble.

Se debe especificar el valor del criterio para cada criterio usado en la condición. Si los parámetros de la aplicación que se está iniciando coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, el Control de aplicaciones lleva a cabo la acción especificada en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, el Control de aplicaciones no controla el inicio de la aplicación.

## Decisiones que toma el componente Control de aplicaciones cuando se activa una regla

Cuando se activa una regla, el Control de aplicaciones permite que los usuarios (o grupos de usuarios) inicien aplicaciones o bloquea el inicio de acuerdo con la regla. Usted puede seleccionar un usuario o un grupo de usuarios a los que se les permita o no iniciar aplicaciones que activen una regla.

Si una regla no especifica los usuarios autorizados para iniciar aplicaciones que cumplan con la regla, se denomina regla de *bloqueo*.

Una regla que no especifica ningún usuario que no esté autorizado para iniciar aplicaciones que cumplan con la regla se denomina regla de *autorización*.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. Por ejemplo, si se ha especificado una regla de autorización del Control de aplicaciones para un grupo de usuarios y también se ha especificado una regla de bloqueo de este componente para un usuario de este grupo de usuarios, este usuario no podrá iniciar la aplicación.

### Estado operativo de una regla

Las reglas de control de aplicaciones pueden tener uno de los siguientes estados operativos:

- **Activado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en funcionamiento.
- **Desactivado**. Este estado significa que la regla se omite cuando el componente Control de aplicaciones está en funcionamiento.
- **Prueba**. Este estado significa que Kaspersky Endpoint Security permite iniciar las aplicaciones a las cuales se aplican las reglas pero registra la información sobre el inicio de dichas aplicaciones en el informe.

## Agregar una regla de control de aplicaciones

*Para agregar una regla de control de aplicaciones:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de aplicaciones**.
3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Esto abre la lista de reglas de control de aplicaciones.
4. Haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de control de aplicaciones**.
5. En la pestaña **Configuración general**, defina la configuración principal de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. En el campo **Descripción**, escriba la descripción de la regla.

   c. Compile o edite una lista de usuarios o grupos de usuarios que estén autorizados o no autorizados a iniciar aplicaciones que cumplen con las condiciones de activación de las reglas. Para ello, haga clic en el botón **Agregar** 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 **Usuarios y sus derechos**, use el interruptor para definir el derecho de los usuarios a iniciar aplicaciones.

e. Seleccione la casilla **Denegar a los demás usuarios** si quiere que 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 coincidan con las condiciones de activación de las reglas.

> 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 las reglas como actualizadores de confianza autorizados a crear otros archivos ejecutables que se podrán ejecutar posteriormente, seleccione la casilla **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, realice lo siguiente:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de aplicaciones**.

3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Esto abre la lista de reglas de control de aplicaciones.

4. Seleccione la regla para la cual desea configurar una condición de activación.

   Se abren las propiedades de Regla de Control de aplicaciones.

5. Seleccione la pestaña **Condiciones** o **Exclusiones** y haga clic en el botón **Agregar**.

6. Seleccione las condiciones de activación para la Regla de Control de aplicaciones:

   - **Condiciones de las propiedades de las aplicaciones iniciadas**. En la lista de aplicaciones en ejecución, puede seleccionar las aplicaciones a las que se aplicará la Regla de Control de aplicaciones. Kaspersky Endpoint Security también enumera las aplicaciones que se estaban ejecutando anteriormente en el equipo. Debe seleccionar el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Código hash de archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a carpeta**.

   - **Condiciones "Categoría KL"**. Una *categoría KL* es una lista de aplicaciones que comparten atributos de temas. Los expertos de Kaspersky son los encargados de mantener la lista. Por ejemplo: la categoría KL

"Aplicaciones de ofimática" incluye todas las aplicaciones del conjunto de programas de Microsoft Office y Adobe® Acrobat®, entre otros.

- **Condición personalizada**. Puede seleccionar el archivo de la aplicación y seleccionar una de las condiciones de activación de la regla: **Código hash de archivo**, **Certificado**, **Metadatos** o **Ruta de acceso a archivo o carpeta**.

- **Condición por unidad de archivo (unidad extraíble)**. La regla de Control de aplicaciones se aplica solo a los archivos que se ejecutan en una unidad extraíble.

- **Condiciones de las propiedades de los archivos de la carpeta especificada**/ La regla de Control de aplicaciones se aplica solo a los archivos que residen dentro de la carpeta especificada. También puede incluir o excluir archivos de subcarpetas. Debe seleccionar el criterio que desea utilizar para crear una o varias condiciones de activación de reglas: **Código hash de archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a carpeta**.

7. Guarde los cambios.

Al agregar condiciones, tenga en cuenta las siguientes consideraciones especiales para Control de aplicaciones:

- Kaspersky Endpoint Security no admite un hash de archivo MD5 y no controla el inicio de aplicaciones basadas en un hash MD5. Se utiliza un hash SHA256 como condición de activación de la regla.

- No se recomienda usar solo los criterios de **Emisor** y **Sujeto** como condiciones de activación de la regla. Utilizar estos criterios no es confiable.

- Si está usando vínculos simbólicos en el campo **Ruta de acceso a archivo o carpeta**, le aconsejamos resolver el vínculo simbólico para que la regla de Control de aplicaciones funcione correctamente. Para ello, haga clic en el botón **Resolver vínculo simbólico**.

## Edición del estado de una regla de Control de aplicaciones

*Para cambiar el estado de una regla de Control de aplicaciones, realice lo siguiente:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de aplicaciones**.

3. Haga clic en el botón **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

   Esto abre la lista de reglas de control de aplicaciones.

4. En la columna **Estado**, abra el menú contextual y seleccione una de estas opciones:

   - **Activado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en ejecución.

   - **Desactivado**. Este estado significa que la regla se ignora cuando el componente Control de aplicaciones está en funcionamiento.

   - **Pruebas**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica esta regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

5. Guarde los cambios.

# Administrar Reglas de Control de aplicaciones en Kaspersky Security Center

Kaspersky Endpoint Security controla el inicio de las aplicaciones por parte de los usuarios mediante reglas. Una regla de Control de aplicaciones está formada por una serie condiciones de activación y una serie de acciones. Cuando una regla se activa, Control de aplicaciones realiza la acción que la regla le indica (permitir o impedir que los usuarios inicien una aplicación).

## Condiciones de activación de regla

Una condición que activa una regla tiene la siguiente correlación: "tipo de condición - criterio de la condición - valor de la condición". Según las condiciones de activación de la regla, Kaspersky Endpoint Security aplica (o no) una regla a la aplicación.

Los siguientes tipos de condiciones se utilizan en las reglas:

- *Condiciones de inclusión*. Kaspersky Endpoint Security aplica la regla a la aplicación si la aplicación coincide con al menos una condición de inclusión.
- *Condiciones de exclusión*. Kaspersky Endpoint Security no aplica la regla a la aplicación si la aplicación coincide con al menos una de las condiciones de exclusión y no coincide con ninguna condición de inclusión.

Las condiciones de activación de regla se crean usando criterios. Se utilizan los siguientes criterios para crear reglas en Kaspersky Endpoint Security:

- Ruta de acceso de la carpeta que contiene el archivo ejecutable de la aplicación o ruta de acceso del archivo ejecutable de la aplicación.
- Metadatos: nombre del archivo ejecutable de la aplicación, versión del archivo ejecutable de la aplicación, nombre de la aplicación, versión de la aplicación, proveedor de la aplicación.
- Hash del archivo ejecutable de la aplicación
- Certificado: emisor, asunto, huella digital.
- Inclusión de la aplicación en una categoría KL.
- Ubicación del archivo ejecutable de la aplicación en un disco extraíble.

Se debe especificar el valor del criterio para cada criterio usado en la condición. Si los parámetros de la aplicación que se está iniciando coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, el Control de aplicaciones lleva a cabo la acción especificada en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, el Control de aplicaciones no controla el inicio de la aplicación.

## Decisiones que toma el componente Control de aplicaciones cuando se activa una regla

Cuando se activa una regla, el Control de aplicaciones permite que los usuarios (o grupos de usuarios) inicien aplicaciones o bloquea el inicio de acuerdo con la regla. Usted puede seleccionar un usuario o un grupo de usuarios a los que se les permita o no iniciar aplicaciones que activen una regla.

Si una regla no especifica los usuarios autorizados para iniciar aplicaciones que cumplan con la regla, se denomina regla de *bloqueo*.

Una regla que no especifica ningún usuario que no esté autorizado para iniciar aplicaciones que cumplan con la regla se denomina regla de *autorización*.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. Por ejemplo, si se ha especificado una regla de autorización del Control de aplicaciones para un grupo de usuarios y también se ha especificado una regla de bloqueo de este componente para un usuario de este grupo de usuarios, este usuario no podrá iniciar la aplicación.

### Estado operativo de una regla

Las reglas de control de aplicaciones pueden tener uno de los siguientes estados operativos:

- **Activado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en funcionamiento.
- **Desactivado**. Este estado significa que la regla se omite cuando el componente Control de aplicaciones está en funcionamiento.

**Prueba**. Este estado significa que Kaspersky Endpoint Security permite iniciar las aplicaciones a las cuales se aplican las reglas pero registra la información sobre el inicio de dichas aplicaciones en el informe.

## Recepción de información sobre las aplicaciones que se instalan en equipos de usuarios

Para crear reglas de Control de aplicaciones óptimas, se recomienda obtener primero un panorama general de las aplicaciones que se utilizan en los equipos de la red LAN corporativa. Para hacerlo, puede obtener la siguiente información:

- Proveedores, versiones y localizaciones de aplicaciones utilizadas en la red LAN.
- Frecuencia de actualización de las aplicaciones.
- Directivas de uso de las aplicaciones adoptadas en la empresa (pueden ser directivas de seguridad o directivas administrativas).
- Ubicación de almacenamiento de los paquetes de distribución de las aplicaciones.

La información sobre las aplicaciones que se utilizan en los equipos de la red LAN corporativa está disponible en la carpeta **Registro de aplicaciones** y en la carpeta **Archivos ejecutables**. Las carpetas **Registro de aplicaciones** y **Archivos ejecutables** están ubicadas en la carpeta **Administración de aplicaciones** en el 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 que está instalado en el equipo cliente.

La carpeta **Archivos ejecutables** contiene una lista de todos los archivos ejecutables que se han iniciado alguna vez en equipos cliente o que fueron detectados durante la tarea de inventario de Kaspersky Endpoint Security.

Para ver la información general acerca de la aplicación y los archivos ejecutables, y una lista de equipos donde se instaló la aplicación, abra la ventana de propiedades de una aplicación que esté seleccionada en la carpeta **Registro de aplicaciones** o en la carpeta **Archivos ejecutables**.

*Para abrir la ventana de propiedades de una aplicación desde 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 **Adicional** → **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 **Adicional** → **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 mayor comodidad al crear Regla de control de aplicaciones, puede crear categorías de aplicaciones.

Se recomienda crear la categoría "Aplicaciones de trabajo" que cubra el conjunto de aplicaciones estándar que se utilizan en la compañía. Si diferentes grupos de usuarios usan conjuntos de aplicaciones diferentes en su trabajo, se puede crear una categoría de aplicaciones separada para cada grupo de usuario.

*Para crear una categoría de aplicaciones:*

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 aplicaciones**.
3. Haga clic en el botón **Crear una categoría** en el espacio de trabajo.

   Se inicia el asistente de creación de categorías de usuarios.
4. Siga las instrucciones del asistente de creación de categorías de usuarios.

### Paso 1. Selección del tipo de categoría

En este paso, seleccione uno de los tipos siguientes de categorías de aplicaciones:

- **Categoría con contenido agregado manualmente**. Si selecciona este tipo de categoría, en los pasos "Configuración de las condiciones para la inclusión de aplicaciones en una categoría" y "Configuración de las condiciones para la exclusión de aplicaciones de una categoría", podrá definir los criterios que determinarán qué archivos ejecutables formarán parte de la categoría.
- **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**. Si selecciona este tipo de categoría, en el paso "Configuración" podrá seleccionar un equipo. Los archivos ejecutables del equipo que elija se incluirán automáticamente en la categoría.

- **Categoría que incluye archivos ejecutables desde la carpeta específica**. Si selecciona este tipo de categoría, en el paso "Carpeta de repositorio" podrá seleccionar una carpeta. Los archivos ejecutables de la carpeta que elija se incluirán automáticamente en la categoría.

Para crear una categoría con contenido agregado automáticamente, Kaspersky Security Center genera un inventario de los archivos que tienen los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR.

### Paso 2. Introducción de un nombre de categoría de usuario

En este paso, especifique un nombre para la categoría de aplicaciones.

### Paso 3. Configuración de las condiciones para la inclusión de aplicaciones en una categoría

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría con contenido agregado manualmente**.

En este paso, en la lista desplegable **Agregar**, seleccione las condiciones que determinarán qué aplicaciones se incluirán en la categoría:

- **Desde la lista de archivos ejecutables**. Agrega aplicaciones desde la lista de archivos ejecutables en el dispositivo cliente a la categoría personalizada.
- **Desde propiedades del archivo**. Especifica los datos detallados de archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.
- **Metadatos desde archivos en carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.
- **Sumas de comprobación de archivos en carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los hashes de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.
- **Certificados para archivos desde carpeta**. Seleccione una carpeta en el dispositivo cliente que contiene archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

  No se recomienda utilizar condiciones cuyas propiedades no tengan especificado el parámetro **Huella digital del certificado**.

- **Metadatos de los archivos del instalador de MSI**. Seleccione un paquete MSI. Kaspersky Security Center tomará los metadatos de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.
- **Sumas de comprobación de archivos desde el instalador MSI de la aplicación**. Seleccione un paquete MSI. Kaspersky Security Center tomará los hashes de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.

- **Categoría KL**. Especifique una categoría KL como una condición para agregar aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que comparten atributos de temas. Los expertos de Kaspersky son los encargados de mantener la lista. Por ejemplo: la categoría KL "Aplicaciones de ofimática" incluye todas las aplicaciones del conjunto de programas de Microsoft Office y Adobe Acrobat, entre otros.

  Puede seleccionar todas las categorías KL para generar una lista extendida de aplicaciones de confianza.

- **Ruta de la aplicación**. Selecciona una carpeta en el dispositivo cliente. Kaspersky Security Center agregará archivos ejecutables desde esta carpeta a la categoría personalizada.

- **Certificados desde repositorio de certificados**. Seleccione certificados que se hayan utilizado para firmar archivos ejecutables. Se los usará como condición para agregar aplicaciones a la categoría personalizada.

  No se recomienda utilizar condiciones cuyas propiedades no tengan especificado el parámetro **Huella digital del certificado**.

- **Tipo de unidad**. Seleccione el tipo de dispositivo de almacenamiento (todos los discos duros y unidades extraíbles o solo unidades extraíbles) como una condición para agregar aplicaciones a la categoría personalizada.

### Paso 4. Configuración de las condiciones para la exclusión de aplicaciones desde una categoría

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría con contenido agregado manualmente**.

Las aplicaciones especificadas en este paso se excluyen de la categoría incluso si estas aplicaciones se especificaron en el paso "Configuración de las condiciones para las aplicaciones incluidas en una categoría".

En este paso, en la lista desplegable **Agregar**, seleccione las condiciones que determinarán qué aplicaciones quedarán excluidas de la categoría:

- **Desde la lista de archivos ejecutables**. Agrega aplicaciones desde la lista de archivos ejecutables en el dispositivo cliente a la categoría personalizada.

- **Desde propiedades del archivo**. Especifica los datos detallados de archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Metadatos desde archivos en carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los metadatos de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Sumas de comprobación de archivos en carpeta**. Selecciona una carpeta en el dispositivo cliente que contiene archivos ejecutables. Kaspersky Security Center indicará los hashes de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Certificados para archivos desde carpeta**. Seleccione una carpeta en el dispositivo cliente que contiene archivos ejecutables firmados con certificados. Kaspersky Security Center indicará los certificados de estos archivos ejecutables como una condición para agregar aplicaciones a la categoría personalizada.

- **Metadatos de los archivos del instalador de MSI**. Seleccione un paquete MSI. Kaspersky Security Center tomará los metadatos de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.

- **Sumas de comprobación de archivos desde el instalador MSI de la aplicación**. Seleccione un paquete MSI. Kaspersky Security Center tomará los hashes de los archivos ejecutables que formen parte del paquete MSI como condición para agregar aplicaciones a la categoría personalizada.

- **Categoría KL**. Especifique una categoría KL como una condición para agregar aplicaciones a la categoría personalizada. Una *categoría KL* es una lista de aplicaciones que comparten atributos de temas. Los expertos de Kaspersky son los encargados de mantener la lista. Por ejemplo: la categoría KL "Aplicaciones de ofimática" incluye todas las aplicaciones del conjunto de programas de Microsoft Office y Adobe Acrobat, entre otros.

  Puede seleccionar todas las categorías KL para generar una lista extendida de aplicaciones de confianza.

- **Ruta de la aplicación**. Selecciona una carpeta en el dispositivo cliente. Kaspersky Security Center agregará archivos ejecutables desde esta carpeta a la categoría personalizada.

- **Certificados desde repositorio de certificados**. Seleccione certificados que se hayan utilizado para firmar archivos ejecutables. Se los usará como condición para agregar aplicaciones a la categoría personalizada.

- **Tipo de unidad**. Seleccione el tipo de dispositivo de almacenamiento (todos los discos duros y unidades extraíbles o solo unidades extraíbles) como una condición para agregar aplicaciones a la categoría personalizada.

## Paso 5. Configuración

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**.

En este paso, haga clic en el botón **Agregar** y especifique los equipos cuyos archivos ejecutables añadirá Kaspersky Security Center a la categoría de aplicaciones. Todos los archivos ejecutables que se encuentren en la carpeta **Archivos ejecutables** serán agregados por Kaspersky Security Center en la categoría de aplicaciones.

En este paso, puede realizar los siguientes ajustes:

- Algoritmo para el cálculo de la función hash por parte de Kaspersky Security Center. Para seleccionar un algoritmo, debe seleccionar al menos una de las siguientes casillas:

  - **Calcular SHA-256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.

  - **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.

- 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 la categoría de una aplicación después de que se haya creado.

- Campo**Período 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 carpeta **Sincronizar datos con el repositorio del Servidor de administración**.

### Paso 6. Carpeta de repositorio

Este paso está disponible si ha seleccionado el tipo de categoría **Categoría que incluye archivos ejecutables desde una carpeta seleccionada**.

En este paso, haga clic en el botón **Examinar** y especifique la carpeta en la cual Kaspersky Security Center buscará archivos ejecutables para agregar automáticamente aplicaciones a la categoría de aplicación.

En este paso, puede realizar los siguientes ajustes:

- Casilla de verificación **Incluir bibliotecas de vínculo dinámico (DLL) en esta categoría**. Seleccione esta casilla si desea que la categoría de aplicaciones incluya bibliotecas de vínculos dinámicos (archivos DLL).

  La categoría de aplicación Incluir archivos DLL puede reducir el rendimiento de Kaspersky Security Center.

- Casilla de verificación **Incluir datos de script en esta categoría**. Seleccione esta casilla si desea que la categoría de aplicaciones incluya también scripts.

  Incluir scripts en la categoría de aplicaciones puede afectar el rendimiento de Kaspersky Security Center.

- Algoritmo para el cálculo de la función hash por parte de Kaspersky Security Center. Para seleccionar un algoritmo, debe seleccionar al menos una de las siguientes casillas:

  - **Calcular SHA-256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)**.
  - **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**.

- Casilla **Forzar el análisis de carpeta en busca de cambios**. Seleccione esta casilla si desea que Kaspersky Security Center busque periódicamente archivos ejecutables en la carpeta usada para añadir automáticamente a la categoría de aplicación.

  Si desactiva la casilla **Forzar el análisis de 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**Período 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 utilizada para agregarlos automáticamente a la categoría de la aplicación.

  Este campo está disponible si se ha seleccionado la opción **Forzar el análisis de carpeta en busca de cambios**.

### Paso 7. Creación de una categoría personalizada

Para salir del Asistente de instalación de la aplicación, haga clic en el botón **Finalizar**.

## Agregar archivos ejecutables de la carpeta Archivos ejecutables a la categoría de la aplicación

En la carpeta **Archivos ejecutables**, se muestra la lista de archivos ejecutables detectados en los equipos. Kaspersky Endpoint Security genera una lista de archivos ejecutables como resultado de la tarea Inventario.

*Para agregar archivos ejecutables de la carpeta **Archivos ejecutables** a la categoría de la aplicación*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione **Adicional** → **Administración de aplicaciones** → carpeta **Archivos ejecutables**.
3. En el área de trabajo, seleccione los archivos ejecutables que desea agregar a la categoría de la aplicación.
4. Haga clic derecho para abrir el menú contextual de los archivos ejecutables seleccionados y seleccione **Añadir a la categoría**.

   Se abre la ventana **Seleccionar categoría de aplicaciones**.
5. En la ventana **Seleccionar categoría de aplicaciones**:
   - En la parte superior de la ventana, elija una de las siguientes acciones:
     - **Crear categoría de aplicaciones**. Seleccione esta opción si desea crear una nueva categoría de aplicación y añadirle archivos ejecutables.
     - **Añadir reglas a la categoría especificada**. Seleccione esta opción si desea seleccionar una categoría de aplicación existente y añadirle archivos ejecutables.
   - En la sección **Tipo de regla**, elija una de las siguientes opciones:
     - **Añadir a reglas de inclusión**. Seleccione esta opción si desea crear una condición que añada archivos ejecutables a la categoría de la aplicación.
     - **Añadir a reglas de exclusión**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de la aplicación.
   - En la sección **Tipo de Información de archivo**, elija una de las siguientes opciones:
     - **Datos de certificado (o SHA-256 para archivos sin certificado)**.
     - **Datos del certificado (se omitirán los archivos sin certificado)**.
     - **Solo SHA-256 (los archivos sin SHA-256 se omitirán)**.
     - **MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**.
6. Haga clic en **Aceptar**.

## Adición de archivos ejecutables relacionados con eventos a la categoría de la aplicación

*Para agregar archivos ejecutables relacionados con los eventos de Control de aplicaciones a la categoría de la aplicación:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.

3. Elija una selección de eventos relacionados con el funcionamiento del componente Control de aplicaciones (Visualización de eventos resultantes del funcionamiento del componente Control de aplicaciones, Visualización de eventos resultantes del funcionamiento de prueba del componente Control de aplicaciones) en la lista desplegable **Eventos de selección**.

4. Haga clic en el botón **Ejecutar selección**.

5. Seleccione los eventos cuyos archivos ejecutables asociados desea añadir a la categoría de la aplicación.

6. Haga clic derecho para abrir el menú contextual de los eventos seleccionados y seleccione **Añadir a la categoría**.

   Se abre la ventana **Seleccionar categoría de aplicaciones**.

7. En la ventana **Seleccionar categoría de aplicaciones**:

   - En la parte superior de la ventana, elija una de las siguientes acciones:

     - **Crear categoría de aplicaciones**. Seleccione esta opción si desea crear una nueva categoría de aplicación y añadirle archivos ejecutables.

     - **Añadir reglas a la categoría especificada**. Seleccione esta opción si desea seleccionar una categoría de aplicación existente y añadirle archivos ejecutables.

   - En la sección **Tipo de regla**, elija una de las siguientes opciones:

     - **Añadir a reglas de inclusión**. Seleccione esta opción si desea crear una condición que añada archivos ejecutables a la categoría de la aplicación.

     - **Añadir a reglas de exclusión**. Seleccione esta opción si desea crear una condición que excluya archivos ejecutables de la categoría de la aplicación.

   - En la sección **Tipo de Información de archivo**, elija una de las siguientes opciones:

     - **Datos de certificado (o SHA-256 para archivos sin certificado)**.

     - **Datos del certificado (se omitirán los archivos sin certificado)**.

     - **Solo SHA-256 (los archivos sin SHA-256 se omitirán)**.

     - **MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Haga clic en **Aceptar**.

## Crear y modificar una regla de Control de aplicaciones utilizando Kaspersky Security Center.

*Para crear una regla de Control de aplicaciones utilizando 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.

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

4. Seleccione la directiva correspondiente 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 agregar una regla, haga clic en el botón **Agregar**.
   - Si desea editar 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 inicia el asistente de creación de categorías de usuarios.

     b. Siga las instrucciones del asistente de creación de categorías de usuarios.

     c. En la lista desplegable **Categoría**, seleccione la categoría de aplicaciones que acaba de crear.

   - Si desea modificar una categoría existente:

     a. En la lista desplegable **Categoría**, seleccione la categoría de aplicaciones existente que desea modificar.

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

        Se abre la ventana **Propiedades: <Nombre de la categoría>**.

     c. Modifique la configuración de la categoría de aplicaciones seleccionada.

     d. Haga clic en **Aceptar**.

     e. En la lista desplegable **Categoría**, seleccione la categoría de aplicaciones creada en función de la cual quiera crear una regla.

8. En la tabla **Sujetos y sus derechos**, haga clic en el botón **Agregar**.

   Se abre la ventana **Seleccionar Usuarios o Grupos** estándar de Microsoft Windows.

9. En la ventana **Seleccionar usuarios o grupos**, especifique la lista de usuarios y/o grupos de usuarios para los que quiera configurar el permiso para iniciar aplicaciones que pertenezcan a la categoría seleccionada.

10. En la tabla **Sujetos y sus derechos**, haga lo siguiente:

    - Si quiere permitir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione la casilla **Permitir** en las filas correspondientes.

- Si quiere prohibir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione la casilla **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 aplicaciones seleccionada como actualizadores de confianza que permiten crear otros archivos ejecutables que posteriormente podrán ejecutarse, seleccione la casilla **Actualizadores de confianza**.

    Cuando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.

13. Guarde los cambios.

## Cambio del estado de una regla de Control de aplicaciones mediante Kaspersky Security Center

*Para cambiar el estado de una regla de Control de aplicaciones, realice lo siguiente:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 para mostrar el menú contextual y seleccionar una de las siguientes opciones:

   - **Activado**. Este estado significa que la regla se usa cuando el componente Control de aplicaciones está en funcionamiento.
   - **Desactivado**. Este estado significa que la regla se omite cuando el componente Control de aplicaciones está en funcionamiento.
   - **Prueba**. Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica la regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.

     Puede utilizar el estado **Prueba** para asignar la acción equivalente a la opción **Probar reglas** para una parte de las reglas cuando la opción **Aplicar reglas** está seleccionada en la lista desplegable **Acción**.
7. Guarde los cambios.

# Exportar e importar Reglas de control de aplicaciones

Puede exportar la lista de reglas de control de aplicaciones a un archivo XML. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas de Control de aplicaciones o para migrar la lista a otro servidor.

Al exportar e importar Reglas de control de aplicaciones, tenga en cuenta las siguientes consideraciones especiales:

- Kaspersky Endpoint Security exporta la lista de reglas solo con el modo de Control de aplicaciones activo. Esto quiere decir que, si el Control de aplicaciones funciona en modo de lista de rechazados, Kaspersky Endpoint Security solo exporta las reglas con este modo. Para exportar la lista de reglas con el modo de lista de admitidos, necesita cambiar el modo y volver a ejecutar la operación de exportación.

- Para operar, Kaspersky Endpoint Security utiliza categorías de aplicaciones para las reglas de Control de aplicaciones. Al migrar la lista de las reglas de Control de aplicaciones a un servidor diferente, también necesita migrar la lista de categorías de aplicaciones. Para obtener más información sobre las categorías de aplicaciones de exportación e importación, *consulte la Ayuda de Kaspersky Security Center*.

**Cómo exportar e importar una lista de reglas de Control de aplicaciones a la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 la regla de acceso que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
   b. Haga clic en el vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.
      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.
7. Para exportar una lista de reglas de Control de aplicaciones:
   a. Haga clic en el vínculo **Importar**.
      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.
      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
8. Guarde los cambios.

[Cómo exportar e importar una lista de reglas de control de aplicaciones a 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 correspondiente a los equipos en los que desee exportar o importar la lista de reglas.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Controles de seguridad** → **Control de aplicaciones**.
5. Haga clic en el vínculo **Configuración de listas de reglas**.
6. Seleccione una lista de reglas: lista de bloqueo o lista de autorización de aplicaciones.
7. Para exportar la lista de reglas de Control de aplicaciones:
   a. Seleccione la regla de acceso que desea exportar.
   b. Haga clic en el botón **Exportar**.
   c. Confirme que desea exportar solo las reglas seleccionadas, o bien exporte la lista completa.
   d. Haga clic en el botón **Exportar**.

      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 vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
9. Guarde los cambios.

## Prueba de las Reglas de Control de aplicaciones utilizando Kaspersky Security Center

Para garantizar que las reglas de control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas. Cuando se habilita la prueba de las Reglas de control de aplicaciones, Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio está prohibido por el Control de aplicaciones, sino que enviará notificaciones sobre su inicio al Servidor de administración.

El análisis del funcionamiento de las reglas de Control de aplicaciones en el modo de prueba incluye revisar los eventos de Control de aplicaciones resultantes comunicados a Kaspersky Security Center. Si el modo de prueba no bloquea los eventos de inicio de todas las aplicaciones necesarias para el trabajo del usuario del equipo, significa que se han creado las reglas correctas. De lo contrario, es aconsejable actualizar las parametrizaciones de las reglas creadas, crear reglas adicionales o borrar las reglas existentes.

De manera predeterminada, Kaspersky Endpoint Security permite ejecutar cualquier aplicación, excepto las que se han prohibido a través de una regla.

*Para habilitar o deshabilitar el modo de prueba para las reglas de Control de aplicaciones a través de 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 bloqueo**. Si se selecciona esta opción, el Control de aplicaciones permite que todos los usuarios inicien cualquier aplicación, excepto en casos en que las aplicaciones cumplan con las condiciones de las reglas de bloqueo de Control de aplicaciones.
   - **Lista de autorización**. Si se selecciona esta opción, el Control de aplicaciones bloquea a todos los usuarios de iniciar alguna aplicación, excepto en casos en que las aplicaciones cumplen con las condiciones de reglas de habilitación del Control de aplicaciones.
7. Realice una de las siguientes acciones:

   - Si desea habilitar el modo de prueba para las reglas de Control de aplicaciones, seleccione la opción **Probar reglas** en la lista desplegable **Acción**.
   - Si desea que Control de aplicaciones regule la ejecución de aplicaciones en los equipos de los usuarios, seleccione la opción **Aplicar reglas** en la lista desplegable **Acción**.
8. Guarde los cambios.

## Visualización de eventos resultantes de la operación de prueba del componente Control de aplicaciones

*Para ver los eventos que Kaspersky Security Center recibió mientras Control de aplicaciones funcionaba en modo de prueba:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.
3. Haga clic en el botón **Crear una selección**.

   Se abre la ventana **Propiedades: <Nombre de la selección>**.
4. Abra la sección **Eventos**.
5. Haga clic en el botón **Borrar todo**.
6. En la tabla **Eventos**, seleccione las casillas de verificación **Inicio de aplicación prohibido en el modo de prueba** y **Inicio de aplicación autorizado en el modo de prueba**.
7. Haga clic en **Aceptar**.
8. En la lista desplegable **Selección de eventos**, escoja la selección creada.
9. Haga clic en el botón **Ejecutar selección**.

## Acceso al informe sobre las aplicaciones bloqueadas en el modo de prueba

*Para ver el informe sobre las aplicaciones bloqueadas en el modo de prueba:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.

   Se inicia el Asistente de plantilla de informe.
4. Siga las instrucciones del Asistente de plantilla de informe. En el paso **Seleccionar el tipo de plantilla de informe**, seleccione **Otro → Informe sobre aplicaciones bloqueadas en el modo de prueba**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la ficha **Informes**.
5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

## Visualización de eventos resultantes de la operación del componente Control de aplicaciones

*Para ver los eventos resultantes de la operación del componente Control de aplicaciones recibidos por Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.

3. Haga clic en el botón **Crear una selección**.

   Se abre la ventana **Propiedades: <Nombre de la selección>**.

4. Abra la sección **Eventos**.

5. Haga clic en el botón **Borrar todo**.

6. En la tabla **Eventos**, seleccione la casilla **Inicio de aplicación prohibido**.

7. Haga clic en **Aceptar**.

8. En la lista desplegable **Selección de eventos**, escoja la selección creada.

9. Haga clic en el botón **Ejecutar selección**.

## Acceso al informe sobre las aplicaciones bloqueadas

*Para ver el informe sobre aplicaciones bloqueadas:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Informes**.

3. Haga clic en el botón **Nueva plantilla de informe**.

   Se inicia el Asistente de plantilla de informe.

4. Siga las instrucciones del Asistente de plantilla de informe. En el paso **Seleccionar el tipo de plantilla de informe**, seleccione **Otro → Informe sobre aplicaciones bloqueadas**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la ficha **Informes**.

5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

## Prueba de las reglas de Control de aplicaciones

Para garantizar que las reglas de control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas.

El análisis del funcionamiento de las reglas de Control de aplicaciones en el modo de prueba incluye revisar los eventos de Control de aplicaciones resultantes comunicados a Kaspersky Security Center. Si el modo de prueba no bloquea los eventos de inicio de todas las aplicaciones necesarias para el trabajo del usuario del equipo, significa que se han creado las reglas correctas. De lo contrario, es aconsejable actualizar las parametrizaciones de las reglas creadas, crear reglas adicionales o borrar las reglas existentes.

*Para habilitar la prueba de las Reglas de control de aplicaciones o para seleccionar una acción de bloqueo para el Control de aplicaciones:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Protección → Controles de seguridad → Control de aplicaciones**.

   Esto abre la lista de reglas de control de aplicaciones.
3. En la columna **Estado**, seleccione **Pruebas**.

   Este estado significa que Kaspersky Endpoint Security permite siempre iniciar las aplicaciones a las cuales se aplica esta regla, pero registra la información sobre el inicio de dichas aplicaciones en el informe.
4. Guarde los cambios.

Kaspersky Endpoint Security no bloqueará aplicaciones cuyo inicio no esté permitido por el componente Control de aplicaciones, pero enviará notificaciones sobre su inicio al Servidor de administración.

## Monitor de actividades de aplicaciones

El *Monitor de actividades de aplicaciones* es una herramienta diseñada para visualizar información en tiempo real sobre la actividad de las aplicaciones en el equipo de un usuario.

El uso de Monitor de actividades de aplicaciones requiere la instalación de los componentes Control de aplicaciones y Prevención de intrusiones en el host. Si estos componentes no están instalados, la sección Monitor de actividades de aplicaciones en la ventana principal de la aplicación está oculto.

*Para iniciar el Monitor de actividades de aplicaciones, realice lo siguiente:*

En la ventana principal de la aplicación, haga clic en **Más herramientas → Monitor de actividades de aplicaciones**.

Se abre la ventana **Actividad de las aplicaciones**. En esta ventana, se brinda información acerca de la actividad de las aplicaciones en el equipo del usuario en tres pestañas:

- En la pestaña **Todas las aplicaciones**, se muestra información acerca de todas las aplicaciones instaladas en el equipo.
- En la pestaña **En ejecución**, se muestra información en tiempo real acerca del consumo de los recursos del equipo que cada aplicación realiza. Desde esta pestaña, puede continuar para configurar los permisos de una sola aplicación.
- En la pestaña **Ejecutadas al inicio**, se muestra la lista de aplicaciones que se ejecutan cuando se inicia el sistema operativo.

## Reglas para crear máscaras de nombres para archivos o carpetas

La *máscara del nombre de un archivo o carpeta* es una representación del nombre y la extensión de un archivo o del nombre de una carpeta. Las máscaras se forman utilizando caracteres comunes.

Para crear la máscara del nombre de un archivo o de una carpeta, puede usar los siguientes caracteres comunes:

- El carácter `*` (asterisco), que toma el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío). Por ejemplo, la máscara `C:\*.txt` incluirá todas las rutas a archivos con la extensión `txt` ubicados en las carpetas y subcarpetas del disco C:.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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 las plantillas de mensajes de Control de aplicaciones

Cuando un usuario intenta iniciar una aplicación bloqueada por una regla de Control de aplicaciones, Kaspersky Endpoint Security muestra un mensaje en el que se indica que el inicio de la aplicación está bloqueado. Si el usuario cree que el inicio de la aplicación está bloqueado por error, puede usar el vínculo incluido en el texto del mensaje para enviar un mensaje al administrador de la red corporativa local.

Se dispone de plantillas especiales para el mensaje que aparece cuando el inicio de una aplicación está bloqueado y para el mensaje que se envía al administrador. Puede modificar las plantillas de mensajes.

*Para modificar una plantilla de mensaje:*

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

2. En la ventana de configuración de la aplicación, seleccione **Protección** → **Controles de seguridad** → **Control de aplicaciones**.

3. En el bloque **Plantillas**, configure las plantillas para los mensajes de Control de aplicaciones:

   - **Bloqueo**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.

   - **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error.

4. Guarde los cambios.

## Prácticas recomendadas para implementar una lista de aplicaciones permitidas

Al planificar la implementación de una lista de aplicaciones permitidas, se recomienda realizar las siguientes acciones:

1. Forme los siguientes tipos de grupos:

   - Grupos de usuario. Grupos de usuarios para quienes necesita permitir el uso de varios conjuntos de aplicaciones.

   - Grupos de administración. Uno o varios grupos de equipos a los cuales Kaspersky Security Center aplicará el modo de lista de aplicaciones permitidas. Es necesario crear varios grupos de equipos si se utilizan diferentes configuraciones de lista de autorización para esos grupos.

2. Crea una lista de aplicaciones cuyo inicio esté permitido.

   Antes de crear una lista, se le aconseja que haga lo siguiente:

   a. Ejecute la tarea de inventario.

      Encontrará información para crear, reconfigurar e iniciar una tarea de inventario en la sección Administración de tareas.

   b. Ver la lista de archivos ejecutables.

## Configuración del modo de lista de autorización para aplicaciones

Al configurar el modo de lista de autorización, se recomienda realizar las siguientes acciones:

1. Crear categorías de aplicaciones que incluyan las aplicaciones cuyo inicio estará permitido.

   Puede seleccionar uno de los métodos siguientes para crear categorías de aplicaciones:

   - **Categoría con contenido agregado manualmente**. Puede agregar manualmente a esta categoría usando las condiciones siguientes:
     - Metadatos de archivo. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables que tengan los metadatos especificados.
     - Código hash de archivo. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables que tengan el hash especificado.

       El uso de esta condición excluye la capacidad de instalar automáticamente actualizaciones porque las versiones diferentes de archivos tendrán un hash diferente.

     - Certificado de archivo. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables que tengan el certificado especificado.
     - Categoría KL Kaspersky Security Center agregará a la categoría de aplicaciones todas las aplicaciones que pertenezcan a la categoría KL especificada.
     - Ruta de la aplicación. Kaspersky Security Center agregará a la categoría de aplicaciones todos los archivos ejecutables almacenados en la carpeta seleccionada.

       El uso de la condición Carpeta de la aplicación puede no ser seguro porque se permitirá el inicio de cualquier aplicación desde la carpeta especificada. Se recomienda aplicar reglas que utilicen las categorías de aplicaciones con la condición Carpeta de la aplicación solo a aquellos usuarios para los que se debe permitir la instalación automática de actualizaciones.

   - **Categoría que incluye archivos ejecutables desde la carpeta específica**. Puede especificar una carpeta desde la cual los archivos ejecutables se asignen automáticamente a la categoría de aplicación creada.
   - **Categoría que incluye archivos ejecutables desde dispositivos seleccionados**. Puede especificar un equipo para el cual todos los archivos ejecutables se asignarán automáticamente a la categoría de aplicación creada.

Si elige este método para crear las categorías de aplicaciones, Kaspersky Security Center recurrirá a la **carpeta Archivos ejecutables** para obtener información sobre las aplicaciones que estén instaladas en el equipo.

2. Seleccione el modo lista de autorización para el componente Control de aplicaciones.

3. Cree Regla de control de aplicaciones usando las categorías de aplicaciones creadas.

La regla **Imagen de oro** y la regla **Actualizadores de confianza** se definen inicialmente para el modo Lista de autorización. Estas reglas de Control de aplicaciones corresponden a las categorías de KL. La categoría KL "Imagen de oro" incluye programas que aseguran el funcionamiento normal del sistema operativo. La categoría KL "Actualizadores de confianza" incluye actualizadores de los proveedores del software más respetables. No puede eliminar estas reglas. No se puede modificar la configuración de estas reglas. De forma predeterminada, la regla **Imagen de oro** está habilitada, y la regla **Actualizadores de confianza** está deshabilitada. A todos los usuarios se les permite iniciar aplicaciones que coincidan con las condiciones de activación de estas reglas.

**Imagen de oro**

4. Determine las aplicaciones para las que se debe permitir la instalación automática de actualizaciones.

   Puede permitir la instalación automática de actualizaciones utilizando uno de los métodos siguientes:

   - Especifique una lista ampliada de aplicaciones permitidas permitiendo el inicio de todas las aplicaciones que pertenezcan a cualquier categoría KL.

   - Especifique una lista ampliada de aplicaciones permitidas permitiendo el inicio de todas las aplicaciones firmadas con certificados.

     Para habilitar el inicio de todas las aplicaciones firmadas con certificados, puede crear una categoría con una condición basada en certificado que utilice solamente el parámetro **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.

     Cuando se migra la configuración de Kaspersky Endpoint Security, también se migra la lista de archivos ejecutables que crean los actualizadores de confianza.

   - Cree una carpeta y coloque en ella los archivos ejecutables de las aplicaciones que podrán actualizarse automáticamente. A continuación, cree una categoría de aplicaciones con la condición "Carpeta de la aplicación" y especifique la ruta de acceso a la carpeta. Por último, cree una regla de permiso y seleccione esta nueva categoría.

     El uso de la condición Carpeta de la aplicación puede no ser seguro porque se permitirá el inicio de cualquier aplicación desde la carpeta especificada. Se recomienda aplicar reglas que utilicen las categorías de aplicaciones con la condición Carpeta de la aplicación solo a aquellos usuarios para los que se debe permitir la instalación automática de actualizaciones.

## Prueba del modo de lista de autorización

Para garantizar que las reglas de control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas. Cuando está habilitado el modo de prueba, Kaspersky Endpoint Security no bloqueará aplicaciones cuyo inicio no esté permitido por las reglas de Control de aplicaciones, sino que enviará notificaciones sobre su inicio al Servidor de administración.

Al probar el modo de lista de autorización, se recomienda realizar las siguientes acciones:

1. Determinar el período de pruebas (pudiendo elegir entre varios días a dos meses).
2. Habilitar el modo de prueba para Reglas de control de aplicaciones.
3. Examinar, a fin de analizar los resultados de la prueba, los eventos que resulten de probar el funcionamiento de Control de aplicaciones y los informes sobre las aplicaciones bloqueadas en el modo de prueba.
4. Realice cambios en la configuración del modo de lista de autorización en función de los resultados de análisis.

   En particular, los resultados le permitirán agregar los archivos ejecutables vinculados a los eventos a una categoría de aplicaciones.

## Compatibilidad del modo de lista de autorización

Después de seleccionar una acción de bloqueo para Control de aplicaciones, se recomienda continuar con el modo de lista de autorización mediante las siguientes acciones:

- Examine los eventos resultantes de la operación del Control de aplicaciones y los informes sobre ejecuciones bloqueadas para analizar la eficacia del Control de aplicaciones.
- Analice las solicitudes que los usuarios le envíen cuando necesiten obtener acceso a alguna aplicación.
- Para analizar archivos ejecutables desconocidos, compruebe su reputación en Kaspersky Security Network.
- Antes de instalar actualizaciones para el sistema operativo o para el software, instale esas actualizaciones en un grupo de prueba de equipos para comprobar cómo serán procesadas por las Reglas de control de aplicaciones.
- Añada las aplicaciones necesarias a las categorías utilizadas en las Reglas de control de aplicaciones.

## Supervisión de puertos de red

Durante la operación de Kaspersky Endpoint Security, los componentes Control Web, Protección contra amenazas de correo y Protección contra amenazas web supervisan flujos de datos que se transmiten mediante protocolos específicos y que pasan por TCP abierto específico y puertos de UDP en el equipo del usuario. Por ejemplo, el componente Protección contra amenazas de correo analiza la información que se transmite mediante SMTP, mientras que el componente Protección contra amenazas web analiza la información que se transmite mediante HTTP y FTP.

Kaspersky Endpoint Security divide los puertos TCP y UDP del equipo en distintos grupos, tomando como criterio la probabilidad de que se vean vulnerados. Algunos puertos de red están reservados para servicios vulnerables. Se recomienda prestar especial atención a ellos: existe un riesgo mucho mayor de que se los utilice en un ataque de red. Si utiliza servicios que no son estándar que utilizan puertos de red no estándar, estos puertos también pueden convertirse en el blanco del ataque de otros equipos. Puede especificar una lista de los puertos de red y una de las aplicaciones que requieren acceso a la red. Luego, estos puertos y aplicaciones reciben atención especial de los componentes Protección contra amenazas de correo y Protección contra amenazas web durante la supervisión del tráfico de red.

## Habilitación de la supervisión de todos los puertos de red

*Para habilitar la supervisión de todos los puertos de red:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección **Puertos supervisados**, seleccione la opción **Supervisar 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 parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección **Puertos supervisados**, seleccione **Vigilar solo los puertos de red seleccionados**.
4. Haga clic en el botón **Seleccionar**.

   Esto abre una lista de puertos de red que se usan normalmente para la transmisión de mensajes de correo electrónico y tráfico de red. Esta lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
5. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la supervisión del puerto de red.
6. Si no se muestra un puerto de red en la lista de puertos de red, agréguelo haciendo lo siguiente:
   a. Haga clic en el botón **Agregar**.
   b. En la ventana que se abre, ingrese el número de puerto de red y una breve descripción.
   c. Configure el estado **Activo** o **Inactivo** para la supervisión del puerto de red.
7. Guarde los cambios.

Cuando se ejecuta el protocolo FTP en el modo pasivo, se puede establecer la conexión mediante un puerto de red aleatorio que no esté agregado a la lista de puertos de red supervisados. Para proteger tales conexiones, habilite el monitoreo de todos los puertos de red o configure el control de los puertos de red para aplicaciones que establecen conexiones FTP.

## Creación de una lista de aplicaciones para las que se supervisarán todos los puertos de red

Puede crear una lista de las aplicaciones para las que Kaspersky Endpoint Security deba supervisar todos los puertos de red.

Recomendamos que se incluyan las aplicaciones que envían o transmiten datos mediante el protocolo FTP en la lista de las aplicaciones para las que Kaspersky Endpoint Security deba supervisar todos los puertos de red.

*Para crear una lista de aplicaciones para las que se supervisarán todos los puertos de red, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Configuración de red**.
3. En la sección **Puertos supervisados**, seleccione **Vigilar solo los puertos de red seleccionados**.
4. Active la casilla **Supervisar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky**.

   Cuando esta casilla está activada, Kaspersky Endpoint Security supervisa todos los puertos de las siguientes aplicaciones:

   - Adobe Reader
   - Apple Application Support
   - Google Chrome
   - Microsoft Edge
   - Mozilla Firefox
   - Internet Explorer
   - Java
   - mIRC
   - Opera
   - Pidgin
   - Safari
   - Mail.ru Agent

- Yandex Browser

5. Seleccione la casilla **Supervisar todos los puertos de las aplicaciones especificadas**.
6. Haga clic en el botón **Seleccionar**.

   Esto abre una lista de las aplicaciones para las que Kaspersky Endpoint Security debe supervisar los puertos de red.
7. Use el interruptor en la columna **Estado** para habilitar o deshabilitar la supervisión del puerto de red.
8. Si una aplicación no está incluida en la lista de aplicaciones, agréguela del siguiente modo:

   a. Haga clic en el botón **Agregar**.

   b. En la ventana que se abre, ingrese la ruta al archivo ejecutable de la aplicación y una breve descripción.

   c. Configure el estado **Activo** o **Inactivo** para la supervisión del puerto de red.
9. Guarde los cambios.

## Exportar e importar listas de puertos supervisados

Kaspersky Endpoint Security utiliza las siguientes listas para supervisar los puertos de red: lista de puertos de red y lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security. Puede exportar listas de puertos supervisados a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de puertos con la misma descripción. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de las listas de puertos supervisados o para migrar las listas a otro servidor.

Cómo exportar e importar listas de puertos supervisados a la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 supervisados**, 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 de red que se usan normalmente para la transmisión de mensajes de correo y tráfico de red. Esta lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
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, escriba el nombre del archivo XML en el que se guardará la lista de puertos de red exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de puertos de red completa al archivo XML.
9. Para exportar la lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security:
   a. Seleccione la casilla **Supervisar 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, escriba el nombre del archivo XML en el que se guardará la lista de aplicaciones exportada. Seleccione también la carpeta en la que se guardará este archivo.
   e. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de aplicaciones completa 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 que se usará para importar la lista de puertos de red.

b. Haga clic en el botón **Abrir**.

Cuando ya exista una lista de puertos de red en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

11. Para importar una lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security:

a. En la lista de aplicaciones, haga clic en el botón **Importar**.

En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de aplicaciones.

b. Haga clic en el botón **Abrir**.

Cuando ya exista una lista de aplicaciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

12. Guarde los cambios.

Cómo exportar e importar listas de puertos supervisados 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 correspondiente a los equipos en los que desee exportar o importar listas de puertos supervisados.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a la sección **Configuración general** → **Configuración de red**.
5. Para exportar la lista de puertos de red:
   a. En la sección **Puertos supervisados**, seleccione **Vigilar solo los puertos de red seleccionados**.
   b. Haga clic en el vínculo **N puertos seleccionados**.

      Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos de red que se usan normalmente para la transmisión de mensajes de correo y tráfico de red. Esta lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.
   c. En la lista de puertos de red, seleccione los puertos que desea exportar.
   d. Haga clic en el botón **Exportar**.
   e. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de puertos de red exportada. Seleccione también la carpeta en la que se guardará este archivo.
   f. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de puertos de red completa al archivo XML.
6. Para exportar la lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security:
   a. En el bloque **Puertos supervisados**, seleccione la casilla **Supervisar todos los puertos para aplicaciones específicas**.
   b. Haga clic en el vínculo **N aplicaciones 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, escriba el nombre del archivo XML en el que se guardará la lista de aplicaciones exportada. Seleccione también la carpeta en la que se guardará este archivo.
   f. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de aplicaciones completa al archivo XML.
7. Para importar la lista de puertos de red:
   a. En la lista de puertos de red, haga clic en el botón **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de puertos de red.
   b. Haga clic en el botón **Abrir**.

Cuando ya exista una lista de puertos de red en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

8. Para importar una lista de aplicaciones cuyos puertos supervisa Kaspersky Endpoint Security:

   a. En la lista de aplicaciones, haga clic en el botón **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de aplicaciones.

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

      Cuando ya exista una lista de aplicaciones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

9. Guarde los cambios.

# Managed Detection and Response

El componente Managed Detection and Response se agregó a Kaspersky Endpoint Security en la versión 11.6.0. El componente facilita la interacción con la solución Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* opera continuamente para buscar, detectar y eliminar amenazas dirigidas a su organización. Para más detalles sobre el funcionamiento de la solución, *consulte la guía de ayuda de Kaspersky Managed Detection and Response*.

Al interactuar con Kaspersky Managed Detection and Response, la aplicación permite realizar las siguientes funciones:

- activar Managed Detection and Response con un archivo de configuración BLOB;
- ejecutar comandos de Kaspersky Managed Detection and Response;
- enviar datos de telemetría a Kaspersky Managed Detection and Response para facilitar la detección de amenazas.

## Integración con Kaspersky Managed Detection and Response

El proceso de integración con Kaspersky Managed Detection and Response se divide en los siguientes pasos:

1. **Configuración de Kaspersky Security Network Privada**

   Omita este paso si está usando 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 específicos de Kaspersky Security Network, pero KSN Global no.

   En las propiedades del Servidor de administración, cargue el archivo de configuración de Kaspersky Security Network. Encontrará el archivo de configuración de Kaspersky Security Network dentro del archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para obtener información sobre la configuración de KSN Privada, consulte la *Guía de ayuda de Kaspersky Security Center*. Si lo prefiere, puede cargar el archivo de configuración de Kaspersky Security Network al equipo utilizando la línea de comandos (consulte las instrucciones a continuación).

   **Cómo configurar KSN Privada mediante la línea de comandos**

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   `avp.com KSN /private <nombre de archivo>`

   `<nombre de archivo>` es el nombre del archivo de configuración que contenga la configuración de KSN Privada (formato de archivo PKCS7 o PEM).

   Ejemplo:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Como resultado, Kaspersky Endpoint Security utilizará KSN Privada para determinar la reputación de los archivos, las aplicaciones y los sitios web. La configuración de la directiva en la sección **Kaspersky Security Network** mostrará el siguiente estado operativo: *Red KSN: KSN Privada*.

Debe habilitar el modo KSN extendido para que Managed Detection and Response funcione.

2 **Activar Managed Detection and Response.**

Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (consulte las instrucciones más abajo). El archivo BLOB contiene el id. de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. Encontrará el archivo BLOB en el archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre el archivo BLOB, consulte la *guía de ayuda de Kaspersky Managed Detection and Response*.

**Cómo activar Managed Detection and Response 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la política.
5. En la ventana de la directiva, seleccione **Expansión de protección contra amenazas → Detection and Response**.
6. Active la casilla **Managed Detection and Response**.
7. En el bloque **Configuración**, haga clic en **Importar** y seleccione el archivo BLOB que obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tendrá la extensión P7.
8. Guarde los cambios.

**Cómo activar Managed Detection and Response 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. Seleccione **Expansión de protección contra amenazas** → **Detection and Response**.
5. Active el interruptor de **Managed Detection and Response**.
6. Haga clic en **Importar** y seleccione el archivo BLOB que obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tendrá la extensión P7.
7. Guarde los cambios.

**Cómo activar Managed Detection and Response mediante la línea de comandos**

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

   - Si la configuración de la aplicación no está protegida con contraseña:

     `avp.com MDRLICENSE /ADD <nombre de archivo>`

     Reemplace `<nombre de archivo>` con el nombre del archivo de configuración BLOB para activar Managed Detection and Response (un archivo de formato P7).

   - Si la configuración de la aplicación está protegida con contraseña:

     `avp.com MDRLICENSE /ADD <nombre de archivo> /login=<nombre de usuario> /password=<contraseña>`

Como resultado, Kaspersky Endpoint Security verificará el archivo BLOB. Durante la verificación, se controlarán la firma digital y el plazo de la licencia. De no ocurrir errores en este proceso, Kaspersky Endpoint Security cargará el archivo y lo enviará al equipo cuando se realice la siguiente sincronización con Kaspersky Security Center. El estado de funcionamiento del componente aparecerá en el *Informe sobre el estado de los componentes de la aplicación*. Para conocer el estado de funcionamiento de un componente, también puede consultar los informes disponibles en la interfaz de Kaspersky Endpoint Security. El componente **Managed Detection and Response** se agregará a la lista de componentes de Kaspersky Endpoint Security.

Debe habilitar los siguientes componentes para que Managed Detection and Response funcione:

- Kaspersky Security Network (modo ampliado).
- Detección de comportamientos.

La habilitación 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 habilitación de estos componentes es opcional. Los siguientes son algunos de los componentes que proporcionan datos adicionales:

- Protección contra amenazas web.
- Protección contra amenazas de correo.
- Firewall.

### Migración de Kaspersky Endpoint Agent a Kaspersky Endpoint Security para Windows

Kaspersky Endpoint Security es compatible, desde la versión 11, con la solución MDR. Kaspersky Endpoint Security versiones 11–11.5.0 solo envían datos de telemetría a Kaspersky Managed Detection and Response para habilitar la detección de amenazas. Kaspersky Endpoint Security versión 11.6.0 tiene todas las funcionalidades del agente integrado (Kaspersky Endpoint Agent).

Si utiliza Kaspersky Endpoint Security versiones 11–11.5.0, deberá actualizar las bases de datos a las más recientes para trabajar con la solución MDR. También deberá instalar Kaspersky Endpoint Agent.

Si utiliza Kaspersky Endpoint Security 11.6.0 o posterior, deberá 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. Deshabilite el componente Managed Detection and Response en la directiva de Kaspersky Endpoint Agent.

Si la directiva de Kaspersky Endpoint Security también aplica a los equipos que no tengan Kaspersky Endpoint Security 11–11.5.0 instalados, primero debe crear una directiva de Kaspersky Endpoint Agent independiente para esos equipos. En la directiva nueva, configure la integración con Kaspersky Managed Detection and Response.

## Kaspersky Endpoint Agent

*Kaspersky Endpoint Agent* permite que la aplicación interactúe con otras soluciones de Kaspersky para detectar amenazas avanzadas (p. ej., Kaspersky Sandbox). Cada solución de Kaspersky es compatible con una versión específica de Kaspersky Endpoint Agent.

Si necesita información más detallada sobre la versión de Kaspersky Endpoint Agent para Windows incluida en su solución de software, o para más detalles sobre la solución independiente, consulte la guía de ayuda del producto que corresponda:

- *Guía de ayuda de Kaspersky Anti Targeted Attack Platform*
- *Guía de ayuda de Kaspersky Sandbox*
- *Guía de ayuda de Kaspersky Endpoint Detection and Response Optimum*

- *Guía de ayuda de Kaspersky Managed Detection and Response*

Kaspersky Endpoint Agent está incluida en el kit de distribución de Kaspersky Endpoint Security. Puede instalar Kaspersky Endpoint Agent durante la instalación de Kaspersky Endpoint Security. Para ello, deberá seleccionar el componente Endpoint Agent cuando instale la aplicación (puede ocuparse de esto al momento de crear un paquete de instalación, por ejemplo). Una vez que instale la aplicación con la característica Endpoint Agent, se agregarán dos entradas a la lista de aplicaciones instaladas: una para Kaspersky Endpoint Security y otra para Kaspersky Endpoint Agent Cuando desinstale Kaspersky Endpoint Security, también se desinstalará Kaspersky Endpoint Agent.

# Eliminación de datos

Kaspersky Endpoint Security cuenta con una tarea para eliminar información a distancia de los equipos de los usuarios.

En Kaspersky Endpoint Security, la eliminación de datos opera:

- en forma silenciosa,
- en los discos duros y en las unidades extraíbles,
- en todas las cuentas de usuario del equipo.

Kaspersky Endpoint Security ejecutará la tarea *Eliminación de datos* sin importar el tipo de licencia que se esté utilizando y con independencia de que esta haya caducado.

## Modos de eliminación de datos

La tarea ofrece los siguientes modos de eliminación:

- Eliminación de datos inmediata.

  Utilice este modo para, por ejemplo, eliminar información antigua que esté ocupando espacio innecesariamente.

- Eliminación de datos pospuesta.

  Este modo está pensado para, por ejemplo, proteger los datos de un equipo portátil robado o extraviado. Es posible determinar que los datos de un equipo deberán eliminarse automáticamente si este abandona la red corporativa o no se sincroniza con Kaspersky Security Center por un tiempo prolongado.

No es posible configurar una eliminación de datos programada a través de las propiedades de la tarea. La eliminación solo puede suceder en forma inmediata (lo cual ocurre cuando la tarea se inicia manualmente) o en forma pospuesta (cuando no hay conexión con Kaspersky Security Center).

## Limitaciones

La característica de eliminación de datos tiene las siguientes limitaciones:

- Solo los administradores de Kaspersky Security Center pueden controlar la tarea *Eliminación de datos*. La tarea no puede iniciarse ni detenerse desde la interfaz local de Kaspersky Endpoint Security.
- Cuando el sistema de archivos de una unidad es NTFS, Kaspersky Endpoint Security solo puede eliminar los nombres de las secuencias de datos principales. Los nombres de las secuencias de datos alternativas no se pueden eliminar.
- Cuando Kaspersky Endpoint Security elimina un archivo de vínculo simbólico, elimina también los archivos que se encuentran en las rutas especificadas en dicho vínculo.

## Creación de una tarea de eliminación de datos

*Para eliminar información de los equipos de los usuarios:*

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

   Se abre la lista de tareas.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.

   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 **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

4. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Haga clic en **Siguiente**.

   Si se agregan nuevos equipos a un grupo de administración alcanzado por la tarea, la tarea de eliminación de datos inmediata se ejecutará en los nuevos equipos únicamente si la tarea se completa en los cinco minutos posteriores a la incorporación de dichos equipos.

5. Finalice el asistente haciendo clic en el botón **Finalizar**.

   La nueva tarea aparecerá en la lista de tareas.

6. Seleccione la tarea **Eliminación de datos** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

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

8. Seleccione el método de eliminación de datos:

   - **Eliminar a través del sistema operativo**. Kaspersky Endpoint Security utilizará los recursos del sistema operativo para eliminar los archivos. Los objetos eliminados no se enviarán a la Papelera de reciclaje.
   - **Eliminar por completo, sin posibilidad de recuperación**. Kaspersky Endpoint Security sobrescribirá los archivos con datos aleatorios. La información que se elimine será, a fines prácticos, imposible de recuperar.

9. Si desea posponer la eliminación de datos, active la casilla **Eliminar datos automáticamente si no ha habido conexión con Kaspersky Security Center en más de N días**. Defina el número de días.

   La tarea de eliminación pospuesta se ejecutará cada vez que no haya conexión con Kaspersky Security Center por el período definido.

   Al configurar la eliminación de datos pospuesta, recuerde que los empleados pueden apagar sus equipos cuando se van de vacaciones. La eliminación se llevará a cabo aun si este es el motivo por el que se excede 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 queda desactivada, la tarea se ejecutará en cuanto se realice la sincronización con Kaspersky Security Center.

10. Cree la lista de objetos que desee eliminar:

    - **Carpetas**. Kaspersky Endpoint Security eliminará todos los archivos y todas las subcarpetas de la carpeta. La ruta de acceso a la carpeta no puede contener máscaras ni variables de entorno.

    - **Archivos por extensión**. Kaspersky Endpoint Security buscará los archivos que tengan la extensión especificada en todas las unidades del equipo, incluidas las extraíbles. Para especificar más de una extensión, use los caracteres "`;`" o "`,`".

    - **Carpetas predefinidas**. Kaspersky Endpoint Security eliminará los archivos de las siguientes áreas:

        - **Documentos**. Archivos que se encuentren en la carpeta *Documentos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.

        - **Cookies**. Archivos en los que el navegador guarda información sobre los sitios web que el usuario ha visitado (por ejemplo, datos de autorización).

        - **Escritorio**. Archivos que se encuentren en la carpeta *Escritorio* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.

        - **Archivos temporales de Internet Explorer**. Archivos temporales vinculados al funcionamiento de Internet Explorer: copias de páginas web, imágenes, archivos multimedia, etc.

        - **Archivos temporales**. Archivos temporales vinculados al funcionamiento de las aplicaciones instaladas en el equipo. Aquí se incluyen, por ejemplo, las copias de seguridad temporales que se crean al trabajar con documentos en las aplicaciones de Microsoft Office.

        - **Archivos de Outlook**. Archivos vinculados al funcionamiento del cliente de correo electrónico Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de las libretas de direcciones sin conexión (OAB) y archivos de las libretas de direcciones personales (PAB).

        - **Perfil del usuario**. Grupo de archivos y carpetas en los que el sistema operativo almacena la configuración asociada a la cuenta local del usuario.

    Para crear la lista de objetos que se eliminarán, utilice las distintas pestañas. Kaspersky Endpoint Security generará una lista consolidada y eliminará todos los archivos que figuren en ella cuando se complete una tarea.

    > Los archivos que Kaspersky Endpoint Security necesita para funcionar no pueden eliminarse.

11. Haga clic en el botón **Guardar**.

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.

# Protección con contraseña

Un equipo puede ser utilizado por múltiples usuarios con diferentes niveles de conocimientos informáticos. Si los usuarios tienen acceso no restringido a Kaspersky Endpoint Security y a su configuración, es posible que se reduzca el nivel general de protección del equipo. La protección con contraseña permite restringir el acceso a Kaspersky Endpoint Security conforme a los permisos que los usuarios tienen asignados (por ejemplo, el permiso para cerrar la aplicación).

Si el usuario que ha iniciado sesión en Windows (el *usuario de la sesión*) tiene el permiso necesario para realizar una acción, Kaspersky Endpoint Security no le solicita un nombre de usuario y contraseña o una contraseña temporal. El usuario obtiene acceso a Kaspersky Endpoint Security de conformidad con los permisos que tiene asignados.

Si el usuario de la sesión no tiene permitido realizar una acción, tiene las siguientes alternativas para obtener acceso a la aplicación:

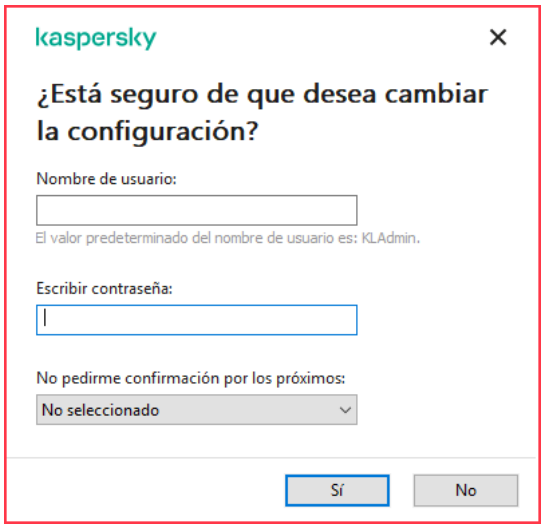
- Usar un nombre de usuario y contraseña.

  Este es el método más conveniente para las operaciones cotidianas. Para realizar una acción protegida con contraseña, se introducen las credenciales de una cuenta de dominio perteneciente a un usuario con el permiso necesario. Para usar esta opción, es necesario que el equipo esté conectado al dominio en cuestión. Si el equipo no está conectado al dominio, use la cuenta KLAdmin.

- Usar una contraseña temporal.

  Este método está pensado para que un usuario ajeno a la red corporativa pueda, en forma temporal, realizar una acción bloqueada (por ejemplo, cerrar la aplicación). Una vez que la contraseña temporal caduca o la sesión finaliza, Kaspersky Endpoint Security restablece su configuración anterior.

Como se ve en la siguiente imagen, cuando un usuario intenta realizar una acción protegida con contraseña, Kaspersky Endpoint Security le solicita su nombre de usuario y contraseña o una contraseña temporal.




Solicitud de contraseña de acceso en Kaspersky Endpoint Security

## Nombre de usuario y contraseña

Para acceder a Kaspersky Endpoint Security, introduzca las credenciales de su cuenta de dominio. La protección con contraseña admite las siguientes cuentas:

- **KLAdmin**. Cuenta de administración con acceso ilimitado a Kaspersky Endpoint Security. La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña. Los permisos de KLAdmin no pueden revocarse. Cuando habilite la protección con contraseña, Kaspersky Endpoint Security le pedirá que defina la contraseña de esta cuenta.

- **El grupo Everyone**. Grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa. Los usuarios del grupo Everyone tendrán acceso a la aplicación conforme a los permisos que se les asigne.

- **Usuarios o grupos individuales**. Cuentas de usuario a las que pueden asignarse permisos individuales. Es posible, por ejemplo, autorizar a un usuario o grupo en particular a realizar una acción que se encuentra bloqueada para el grupo Everyone.

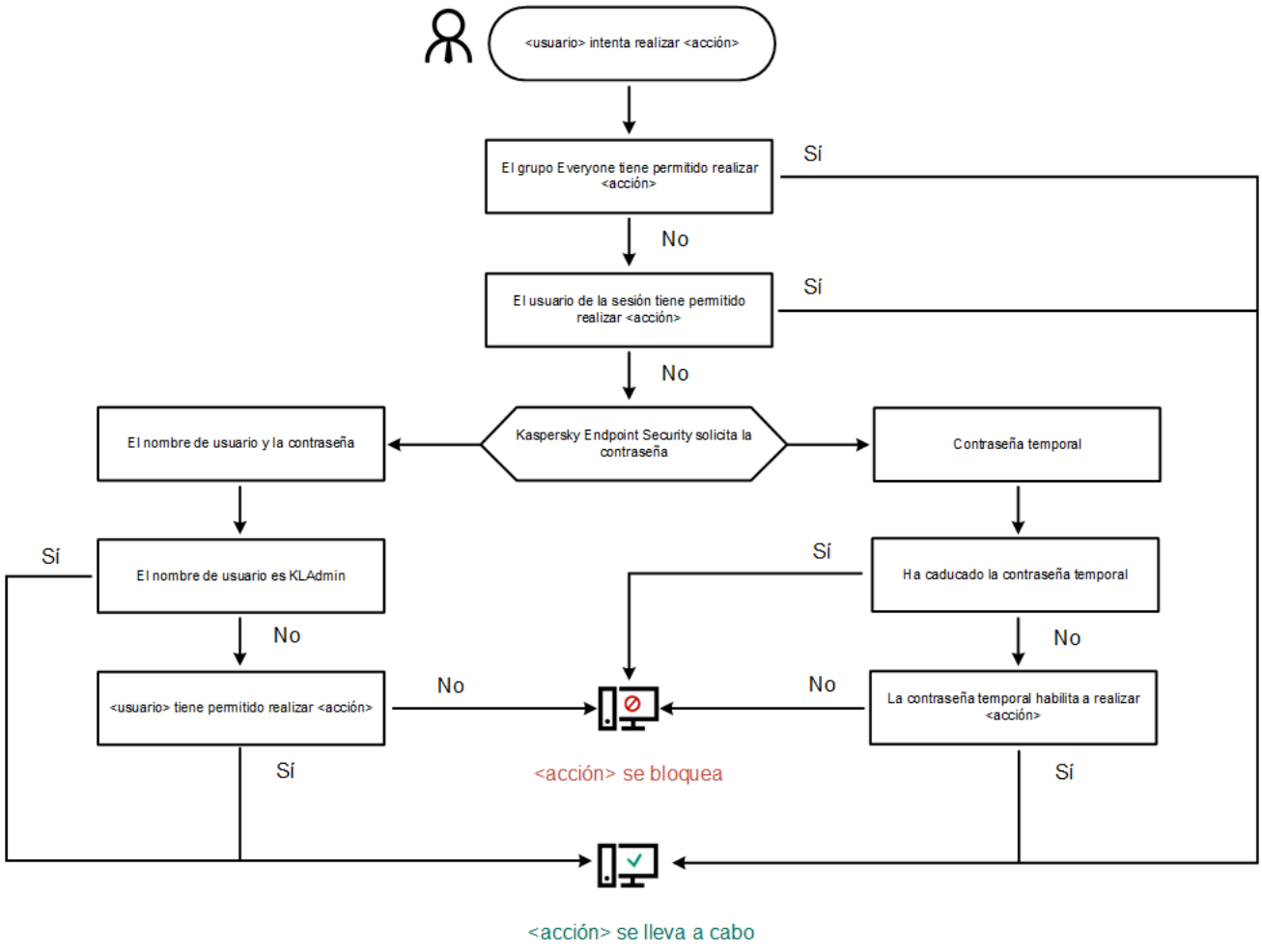
- **Usuario de la sesión**. Cuenta del usuario que inició sesión en Windows. Cuando la aplicación le solicite la contraseña, podrá cambiar a otro usuario de sesión (casilla **Save password for current session**). En tal caso, Kaspersky Endpoint Security considerará como usuario de la sesión al usuario a quien pertenezcan las credenciales de cuenta especificadas y no al que haya iniciado sesión en Windows.

## Contraseña temporal

Una contraseña temporal se utiliza para brindar acceso no permanente a Kaspersky Endpoint Security en un equipo ajeno a la red corporativa. El administrador genera la contraseña temporal para un equipo específico en Kaspersky Security Center, dentro de las propiedades del equipo. A continuación, especifica qué acciones estarán protegidas por dicha contraseña y cuál será su período de vigencia.

## Algoritmo de funcionamiento de la protección con contraseña

Para determinar si una acción protegida con contraseña debe permitirse o bloquearse, Kaspersky Endpoint Security usa el algoritmo de la siguiente imagen.




Algoritmo de funcionamiento de la protección con contraseña

# Habilitar la protección con contraseña

La protección con contraseña permite restringir el acceso a Kaspersky Endpoint Security conforme a los permisos que los usuarios tienen asignados (por ejemplo, el permiso para cerrar la aplicación).

*Para habilitar la protección con contraseña:*

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

   En la ventana Configuración de la aplicación, seleccione la sección **Interfaz**.

2. Utilice el interruptor **Protección con contraseña** para habilitar o deshabilitar el componente.

3. Defina la contraseña de la cuenta KLAdmin y confírmela.

   La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña.

   Si el equipo está sujeto a una directiva, el administrador puede restablecer la contraseña de la cuenta KLAdmin a través de las propiedades de la directiva. La contraseña no puede recuperarse si la olvida y el equipo no está conectado a Kaspersky Security Center.

4. Configure los permisos de los que dispondrán todos los usuarios de la red corporativa:

   a. En la tabla **Permisos**, haga clic en el botón **Editar** para abrir la lista de permisos del grupo Todos.

      El grupo *Everyone* es un grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa.

   b. Active las casillas adyacentes a las acciones que los usuarios podrán realizar sin que se les solicite la contraseña.

      Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

      Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.

   c. Haga clic en el botón **Aceptar**.

5. Guarde los cambios.

Una vez que la protección con contraseña esté habilitada, Kaspersky Endpoint Security restringirá el acceso de los usuarios sobre la base de los permisos otorgados al grupo Everyone. Cuando necesite realizar una acción que esté prohibida para el grupo Everyone, deberá usar la cuenta KLAdmin, una cuenta que disponga de los permisos necesarios o una contraseña temporal.

Para deshabilitar la protección con contraseña, deberá iniciar sesión con el usuario KLAdmin. La protección con contraseña no puede deshabilitarse cuando se está usando una contraseña temporal o cualquier otra cuenta.

Al momento de escribir la contraseña, puede activar la casilla **Guardar contraseña para esta sesión**. Con ello, en tanto la sesión de usuario continúe activa, podrá realizar otras acciones protegidas sin que Kaspersky Endpoint Security le solicite nuevamente la contraseña.

## Asignación de permisos a usuarios o grupos individuales

Existe la posibilidad de otorgar acceso a Kaspersky Endpoint Security a usuarios o grupos individuales. Por ejemplo, un usuario específico puede contar con el permiso **Salir de la aplicación** aun cuando los miembros del grupo Everyone tengan prohibido cerrar el programa. Con ello, la aplicación únicamente podrá cerrarse cuando se haya iniciado sesión como ese usuario específico o como KLAdmin.

Para acceder a la aplicación utilizando las credenciales de una cuenta de dominio, el equipo debe estar conectado al dominio en cuestión. Si el equipo no está conectado al dominio, use la cuenta KLAdmin o una contraseña temporal.

*Para conceder permisos a un usuario o grupo en particular:*

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

   En la ventana Configuración de la aplicación, seleccione la sección **Interfaz**.

2. En la tabla **Protección con contraseña**, haga clic en el botón **Agregar**.

3. En la ventana que se abre, haga clic en el botón **Seleccionar usuario**.

   Se abre el cuadro de diálogo Seleccionar Usuarios o Grupos estándar.

4. Seleccione un usuario o grupo de Active Directory y confirme su elección.

5. En la lista **Permisos**, seleccione las casillas adyacentes a las acciones que el usuario o grupo seleccionado podrá realizar sin que se le solicite una contraseña.

   Si deja alguna casilla desactivada, el usuario no podrá realizar la acción correspondiente. Por ejemplo, si no activa la casilla **Salir de la aplicación**, para cerrar la aplicación deberá iniciar sesión como KLAdmin, usar la cuenta de un usuario que disponga del permiso necesario o usar una contraseña temporal.

   Los permisos de protección con contraseña están sujetos a ciertas consideraciones especiales. No olvide verificar que se cumplan todas las condiciones para acceder a Kaspersky Endpoint Security.

6. Guarde los cambios.

Como resultado, si el grupo Everyone tiene acceso restringido a Kaspersky Endpoint Security, el acceso de los usuarios se regulará conforme a los permisos que se les haya asignado individualmente.

## Uso de una contraseña temporal para otorgar permisos

Una contraseña temporal se utiliza para brindar acceso no permanente a Kaspersky Endpoint Security en un equipo ajeno a la red corporativa. Permite que un usuario realice una acción bloqueada sin tener que conocer las credenciales de la cuenta KLAdmin. El equipo en el que va a usarse la contraseña temporal debe estar incluido en Kaspersky Security Center.

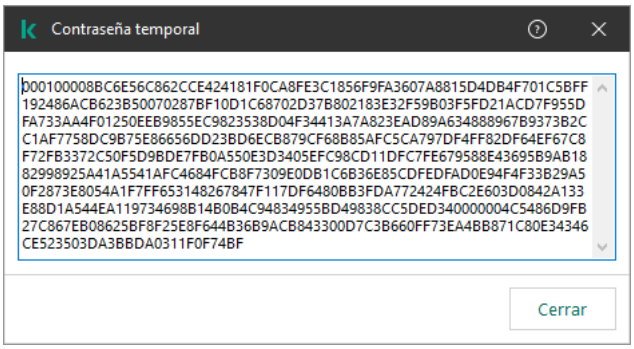
*Para que un usuario realice una acción bloqueada usando una contraseña temporal:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. Haga doble clic en un equipo para abrir su ventana de propiedades.
5. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
6. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Endpoint Security para Windows** y haga doble clic para abrir las propiedades de la aplicación.
7. En la ventana de configuración de la aplicación, vaya a **Configuración general** → **Interfaz**.
8. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección con contraseña**.
9. En la sección **Contraseña temporal**, haga clic en el botón **Configuración**.

   Se abre la ventana **Crear contraseña temporal**.
10. En el campo **Fecha de caducidad**, especifique cuándo caducará la contraseña temporal.
11. En la tabla **Alcance de la contraseña temporal**, active las casillas adyacentes a las acciones que el usuario podrá realizar una vez que introduzca la contraseña temporal.
12. Haga clic en el botón **Crear**.

    Se abre una ventana con la contraseña temporal (vea la siguiente imagen).
13. Copie la contraseña y envíesela al usuario.




Contraseña temporal

## Aspectos especiales de los permisos de la protección con contraseña

Los permisos de protección con contraseña están sujetos a ciertas consideraciones y limitaciones especiales.

### Configurar los parámetros de la aplicación

Cuando el equipo de un usuario esté sujeto a una directiva, asegúrese de verificar que todos los parámetros pertinentes de esta puedan editarse (es decir, que los atributos estén abiertos).

## Salir de la aplicación

No hay ninguna consideración o limitación que se deba tener en cuenta.

## Desactivar componentes de protección.

- No es posible autorizar al grupo Everyone a deshabilitar los componentes de protección. Para que KLAdmin no sea el único usuario autorizado a deshabilitar los componentes de protección, agregue un usuario o grupo que tenga el permiso **Deshabilitar componentes de protección** en la configuración de la protección con contraseña.
- Cuando el equipo de un usuario esté sujeto a una directiva, asegúrese de verificar que todos los parámetros pertinentes de esta puedan editarse (es decir, que los atributos estén abiertos).
- Para deshabilitar los componentes de protección en la configuración de la aplicación, el usuario debe contar con el permiso **Configurar los parámetros de la aplicación**.
- Para deshabilitar los componentes de protección a través del menú contextual (a través del elemento **Pausar protección**), el usuario debe contar tanto con el permiso **Deshabilitar componentes de protección** como con el permiso **Deshabilitar componentes de control**.

## Desactivar componentes de control

- No es posible autorizar al grupo Everyone a deshabilitar los componentes de control. Para que KLAdmin no sea el único usuario autorizado a deshabilitar los componentes de control, agregue un usuario o grupo que tenga el permiso **Deshabilitar componentes de control** en la configuración de la protección con contraseña.
- Cuando el equipo de un usuario esté sujeto a una directiva, asegúrese de verificar que todos los parámetros pertinentes de esta puedan editarse (es decir, que los atributos estén abiertos).
- Para deshabilitar los componentes de control en la configuración de la aplicación, el usuario debe contar con el permiso **Configurar los parámetros de la aplicación**.
- Para deshabilitar los componentes de control a través del menú contextual (usando el elemento **Pausar protección**), el usuario debe contar tanto con el permiso **Deshabilitar componentes de control** como con el permiso **Deshabilitar componentes de protección**.

## Deshabilitar la directiva de Kaspersky Security Center

No es posible asignar al grupo "Everyone" el permiso para deshabilitar la directiva de Kaspersky Security Center. Para que KLAdmin no sea el único usuario autorizado a deshabilitar la directiva, agregue un usuario o grupo que tenga el permiso **Deshabilitar la directiva de Kaspersky Security Center** en la configuración de la protección con contraseña.

## Eliminar una clave

No hay ninguna consideración o limitación que se deba tener en cuenta.

## Eliminar, modificar o restaurar la aplicación

Si permitió eliminar, modificar y restaurar la aplicación para el grupo "Todos", Kaspersky Endpoint Security no solicitará una contraseña cuando el usuario intente llevar a cabo estas operaciones. Por lo tanto, todos los usuarios, incluidos aquellos que estén fuera del dominio, podrán instalar, modificar o restaurar la aplicación.

## Restaurar el acceso a los datos de unidades cifradas

Para restaurar el acceso a los datos de unidades cifradas, deberá iniciar sesión con el usuario KLAdmin. El permiso para realizar esta acción no puede otorgarse a ningún otro usuario.

## Ver informes

No hay ninguna consideración o limitación que se deba tener en cuenta.

## Restaurar objetos de Copias de seguridad

No hay ninguna consideración o limitación que se deba tener en cuenta.

# Zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza independientemente, teniendo en cuenta las características de los objetos manejados y las aplicaciones instaladas en el equipo. Puede ser necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a un objeto o una aplicación determinados, si está seguro de que dicho objeto o aplicación no suponen peligro alguno. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza además de la zona de confianza general en una directiva.

# Cómo crear una exclusión de análisis

Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas.

A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre el software legal que los delincuentes pueden utilizar para dañar el equipo o los datos personales están disponibles en la Enciclopedia de Kaspersky.

Kaspersky Endpoint Security puede bloquear estas aplicaciones. Para prevenir que se bloqueen, puede configurar la exclusión del análisis para las aplicaciones en uso. Busque para ello el nombre (o la máscara de nombre) pertinente en la Enciclopedia de Kaspersky y agréguelo a la zona de confianza. Por ejemplo, a menudo utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security considera esta actividad como sospechosa y puede bloquearla. Para evitar que la aplicación se bloquee, cree una exclusión de análisis con el nombre o la máscara de nombre que se indiquen en la Enciclopedia de Kaspersky.

Si una aplicación que recopila información y la envía para su proceso se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis si configura Kaspersky Endpoint Security tal como se describe en este documento.

Las exclusiones de escaneo pueden ser utilizadas por los siguientes componentes de aplicaciones y tareas configuradas por el administrador del sistema:

- Detección de comportamientos.
- Prevención de exploits.
- Prevención contra intrusos
- Protección contra amenazas de archivos.
- Protección contra amenazas web.
- Protección contra amenazas de correo.
- Tareas de análisis.

Kaspersky Endpoint Security no analiza un objeto si la unidad o la carpeta que lo contiene está incluida en el alcance del análisis al inicio de una de las tareas de análisis. Sin embargo, la exclusión de análisis no se aplica cuando se inicia una tarea de análisis personalizado para este objeto en particular.

Cómo crear una exclusión de 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 **Zona de confianza**, seleccione la pestaña **Exclusiones de análisis**.

   Esto abre una ventana que contiene una lista de exclusiones.
8. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
9. Seleccione la casilla **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de deshabilitar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
10. Haga clic en el botón **Agregar**.
11. Para excluir un archivo o una carpeta del análisis:

    a. En la sección **Propiedades**, seleccione la casilla **Archivo o carpeta**.

    b. Haga clic en el vínculo al **archivo o carpeta** en la sección **Descripción de la exclusión de análisis** 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) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\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.

- `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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. En la ventana **Nombre de archivo o carpeta**, haga clic en **Aceptar**.

Aparece un vínculo al archivo o la carpeta agregados en la sección **Descripción de la exclusión de escaneo** de la ventana **Exclusión de análisis**.

12. Para excluir objetos con un nombre específico del análisis:

a. En la sección **Propiedades**, seleccione la casilla **Nombre de objeto**.

b. Haga clic en el vínculo para **ingresar nombre de objeto** de la sección **Descripción de la exclusión de análisis** para abrir la ventana **Nombre de objeto**.

c. Escriba el nombre que se le da al tipo de objeto en la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Cliente*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

d. Haga clic en **Aceptar** en la ventana **Nombre de objeto**.

Aparece un vínculo al nombre del objeto agregado en la sección **Descripción de la exclusión de escaneo** de la ventana **Exclusión de análisis**.

13. Si desea excluir un archivo individual de los análisis:

a. En la sección **Propiedades**, seleccione la casilla **Hash del objeto**.

b. Haga clic en el vínculo de entrada de hash del objeto para abrir la ventana **Hash del objeto**.

c. Ingrese el hash del archivo o seleccione el archivo haciendo clic en el botón **Examinar**.

Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se agregará a las exclusiones.

d. Haga clic en **Aceptar** en la ventana **Hash del objeto**.

Aparece un vínculo al objeto agregado en el bloque **Descripción de la exclusión de análisis** de la ventana **Exclusión de análisis**.

14. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

15. Especifique los componentes de Kaspersky Endpoint Security que deben utilizar la exclusión de análisis:

a. Haga clic en **cualquier** vínculo en la sección **Descripción de la exclusión de análisis** para activar el vínculo para **seleccionar componentes**.

b. Haga clic en el vínculo para **seleccionar componentes** para abrir la ventana **Componentes de protección**.

c. Seleccione las casillas que se encuentran frente a los componentes a los cuales se debe aplicar la exclusión de análisis.

d. En la ventana **Componentes de protección**, haga clic en **Aceptar**.

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 para detener una exclusión en cualquier momento.

17. Guarde los cambios.

Cómo crear una exclusión de análisis con 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 correspondiente a los equipos en los que desee agregar una exclusión.

   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 vínculo **Exclusiones de análisis**.
6. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
7. Seleccione la casilla **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Si se generó una lista local, después de deshabilitar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los archivos enumerados de los análisis.
8. Haga clic en el botón **Agregar**.
9. Seleccione cómo desea agregar la exclusión: **Archivo o carpeta**, **Nombre de objeto** o **Suma de comprobación de objeto**.
10. Si desea excluir un archivo o una carpeta de los análisis, para seleccionar el archivo o la carpeta haga clic en el botón **Examinar**.

    También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite los caracteres * y ? al ingresar una máscara:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\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.
    - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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** debe ingresar el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `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, ingrese 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 agregará a las exclusiones.

13. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

14. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

15. Puede usar el interruptor para detener una exclusión en cualquier momento.

16. Guarde los cambios.

Cómo crear una exclusión de análisis en la interfaz de la aplicación

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el vínculo **Administrar exclusiones**.
4. Haga clic en el botón **Agregar**.
5. Si desea excluir un archivo o una carpeta de los análisis, para seleccionar el archivo o la carpeta haga clic en el botón **Examinar**.

   También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite los caracteres * y ? al ingresar una máscara:

   - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\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.
   - `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. 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** debe ingresar el nombre del tipo de objeto de acuerdo con la clasificación de la Enciclopedia Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `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, ingrese 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 agregará a las exclusiones.
8. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.
9. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.
10. Seleccione el estado **Activo** para la exclusión.

    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:

- Si utiliza la máscara `*.exe`, se excluirán del análisis las rutas a todos los archivos de extensión EXE.
- Si utiliza la máscara `ejemplo*`, se excluirán del análisis 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 los archivos almacenados en la carpeta C:\dir\, pero no a los almacenados en las subcarpetas de C:\dir\.
- La máscara `C:\dir\*` comprende las rutas a todos los archivos de la carpeta C:\dir\, 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\prueba` 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\*\prueba` 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 `dir\*.*` comprende las rutas a los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*.exe` comprende las rutas a todos los archivos de extensión EXE almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\prueba` 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.

## Activar y desactivar una exclusión de análisis

*Para habilitar o deshabilitar una exclusión de análisis:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.

3. En el bloque **Exclusiones**, haga clic en el vínculo **Administrar exclusiones**.

4. Seleccione la exclusión que necesite en la lista de exclusiones de escaneo.

5. Utilice el interruptor ubicado junto a un objeto para incluir este objeto en el alcance del análisis o excluirlo.

6. Guarde los cambios.

## Modificación de la lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de archivos y de red (incluida la actividad maliciosa) y el acceso al registro del sistema no son supervisados por Kaspersky Endpoint Security. De manera predeterminada, Kaspersky Endpoint Security controla las acciones y el tráfico de red de todas las aplicaciones y analiza los objetos que abren, ejecutan o guardan los procesos asociados a las mismas. Sin embargo, Kaspersky Endpoint Security excluye de los análisis a una aplicación que se haya agregado a la lista de aplicaciones de confianza.

Por ejemplo, si considera que los objetos utilizados por la aplicación estándar Bloc de notas de Microsoft Windows son seguros sin análisis, es decir, que confía en esta aplicación, puede agregar el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza. De este modo, el análisis ignora objetos utilizados por esta aplicación.

Además, ciertas acciones clasificadas por Kaspersky Endpoint Security como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de una cantidad de aplicaciones. Por ejemplo, la intercepción del texto escrito con el teclado es un proceso de rutina para los conmutadores de disposición del teclado automática (como Punto Switcher). Para tener en cuenta las características de estas aplicaciones y no supervisarlas, se recomienda agregarlas a la lista de aplicaciones de confianza.

Al excluir del análisis las aplicaciones de confianza, se evitan problemas de compatibilidad de Kaspersky Endpoint Security con otros programas (por ejemplo, el doble análisis del tráfico de red en el equipo de un tercero realizado por Kaspersky Endpoint Security y otra aplicación antivirus) y además se mejora el rendimiento del equipo, lo que resulta crítico cuando se ejecutan aplicaciones del servidor.

Al mismo tiempo, el archivo ejecutable y los procesos de la aplicación de confianza seguirán siendo analizados en busca de virus y otras clases de malware. Una aplicación se puede excluir completamente del análisis de Kaspersky Endpoint Security mediante exclusiones de escaneo.

[Cómo agregar 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 **Zona de confianza**, seleccione la ficha **Aplicaciones de confianza**.

   Esto abre una ventana que contiene una lista de las aplicaciones de confianza.
8. Active la casilla **Combinar valores al heredar** si desea crear una lista de aplicaciones de confianza unificada para todos los equipos de la empresa. La lista de aplicaciones de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las aplicaciones de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
9. Seleccione la casilla **Permitir el uso de aplicaciones de confianza locales** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Si se generó una lista local, Kaspersky Endpoint Security continúa excluyendo de los análisis las aplicaciones de confianza enumeradas después de deshabilitar esta funcionalidad.
10. Haga clic en el botón **Agregar**.
11. En la ventana que se abre, ingrese la ruta al archivo ejecutable de la aplicación de confianza.

    Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

    > Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Usuarios\*\Documentos\Archivo.exe`).

    > Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.
12. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).
13. Puede utilizar la casilla para excluir una aplicación de la zona de confianza en cualquier momento.
14. Guarde los cambios.

[Cómo agregar una aplicación a la lista 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 correspondiente a los equipos en los que desea agregar la aplicación a la lista de confianza.

   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 vínculo **Aplicaciones de confianza**.

   Esto abre una ventana que contiene una lista de las aplicaciones de confianza.
6. Active la casilla **Combinar valores al heredar** si desea crear una lista de aplicaciones de confianza unificada para todos los equipos de la empresa. La lista de aplicaciones de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las aplicaciones de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
7. Seleccione la casilla **Permitir el uso de aplicaciones de confianza locales** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Si se generó una lista local, Kaspersky Endpoint Security continúa excluyendo de los análisis las aplicaciones de confianza enumeradas después de deshabilitar esta funcionalidad.
8. Haga clic en el botón **Agregar**.
9. En la ventana que se abre, ingrese la ruta al archivo ejecutable de la aplicación de confianza.

   Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

   > Kaspersky Endpoint Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Usuarios\*\Documentos\Archivo.exe`).

   > Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.
10. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).
11. Puede utilizar la casilla para excluir una aplicación de la zona de confianza en cualquier momento.
12. Guarde los cambios.

[Cómo agregar una aplicación a la lista de confianza en la interfaz de la aplicación]

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el vínculo **Especificar aplicaciones de confianza**.
4. En la ventana, haga clic en el botón **Agregar**.
5. Seleccione el archivo ejecutable de la aplicación de confianza.

   También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.

   > Kaspersky Endpoint Security es compatible con variables de entorno y convierte la ruta en la interfaz local de la aplicación. Es decir, si ingresa la ruta de archivo `%userprofile%\Documentos\Archivo.exe`, se agregará un registro `C:\Usuarios\Fernando123\Documentos\Archivo.exe` en la interfaz local de la aplicación para el usuario Fernando123. De forma similar, Kaspersky Endpoint Security omite el programa de confianza `File.exe` para otros usuarios. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Usuarios\*\Documentos\Archivo.exe`).

   > Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, defina la configuración avanzada (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 |
|---|---|
| **No analizar archivos abiertos** | Kaspersky Endpoint Security no analizará ningún archivo que la aplicación abra. Por ejemplo, si utiliza aplicaciones para realizar copias de seguridad de archivos, esta función ayuda a reducir el consumo de recursos de Kaspersky Endpoint Security. |
| **No supervisar la actividad de la aplicación** | Kaspersky Endpoint Security no supervisará la actividad de la red y los archivos de la aplicación en el sistema operativo. La actividad de la aplicación se supervisa través de los siguientes componentes: Detección de comportamiento, Prevención de exploits, Prevención de intrusiones en el host, Motor de reparación y Firewall. |
| **No heredar restricciones del proceso principal (aplicación)** | Kaspersky Endpoint Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal lo inicia una aplicación para la que se configuran los derechos de aplicaciones (Prevención de intrusiones en el host) y las reglas de red de aplicaciones (Firewall). |
| **No se supervisa la actividad de aplicaciones secundarias** | Kaspersky Endpoint Security no supervisará las actividades de red ni las operaciones de archivo que realicen las aplicaciones iniciadas por la aplicación. |

| | |
|---|---|
| **Permitir la interacción con la interfaz de Kaspersky Endpoint Security** | La Autoprotección de Kaspersky Endpoint Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona esta casilla, se permite que la aplicación de acceso remoto administre la configuración de Kaspersky Endpoint Security a través de la interfaz de Kaspersky Endpoint Security. |
| **No bloquear la interacción con el componente de protección vía AMSI**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Kaspersky Endpoint Security no supervisará las solicitudes de la aplicación de confianza para que el componente de protección vía AMSI analice objetos. |
| **No analizar el tráfico cifrado / No analizar todo el tráfico** | Kaspersky Endpoint Security no analizará el tráfico de red que tenga origen en la aplicación. Puede excluir de los análisis todo el tráfico o solo el tráfico cifrado. También puede excluir direcciones IP y números de puerto individuales de los análisis. |
| **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:<br>• Un estado **Activo** significa que la aplicación está en la zona de confianza.<br>• Un estado **Inactivo** significa que la aplicación fue excluida de la zona de confianza. |

## Activación y desactivación de reglas de la zona de confianza para una aplicación en la lista de aplicaciones de confianza

*Para habilitar o deshabilitar la acción de las reglas de la zona de confianza aplicadas a una aplicación de la lista de aplicaciones de confianza:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el vínculo **Especificar aplicaciones de confianza**.
4. En la lista de aplicaciones de confianza, seleccione la aplicación de confianza necesaria.
5. Use el interruptor en la columna **Estado** para incluir una aplicación de confianza en el alcance del análisis o excluirla.
6. Guarde los cambios.

# Uso de almacenamiento de certificados de sistema de confianza

Utilizar el almacenamiento de certificados de sistema le permite excluir aplicaciones firmadas con una firma digital de confianza del análisis antivirus. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al grupo *De confianza*.

*Para comenzar a utilizar el almacenamiento de certificados de sistema de confianza:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En la lista desplegable **Almacén de confianza de certificados del sistema**, seleccione qué almacén del sistema debe ser considerado como de confianza por Kaspersky Endpoint Security.
4. Guarde los cambios.

# Administración del Depósito de copias de seguridad

El depósito *Copia de seguridad* contiene copias de respaldo de los archivos que se modifican o eliminan cuando se realiza una desinfección. Una *copia de seguridad* es una copia del archivo creada antes de desinfectar o eliminar el archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. Se conceden accesos limitados a esta carpeta al usuario cuya cuenta se utilizó para instalar Kaspersky Endpoint Security.

Kaspersky Endpoint Security no brinda la capacidad de configurar permisos de acceso de usuario a copias de seguridad de archivos.

A veces no es posible mantener la integridad de los archivos durante la desinfección. Si después de la desinfección pierde acceso total o parcial a información importante del archivo desinfectado, puede intentar restaurar el archivo desde su copia de seguridad a su carpeta original.

Si Kaspersky Endpoint Security se está ejecutando bajo la administración de Kaspersky Security Center, las copias de seguridad de los archivos se pueden transmitir al Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la administración de las copias de seguridad en Kaspersky Security Center, consulte la sección de ayuda de Kaspersky Security Center.

# Configuración del período de almacenamiento máximo de los archivos en Copias de seguridad

De manera predeterminada, el plazo máximo de almacenamiento de las copias de archivos en Copias de seguridad es de 30 días. Al caducar el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos de Copia de seguridad.

*Para configurar el período de almacenamiento máximo de los archivos en Copias de seguridad, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **Informes y repositorios**.
3. Si desea limitar el período de almacenamiento para las copias de archivos en Copia de seguridad, seleccione la casilla **Conservar objetos durante un máximo de N días** en el bloque **Copia de seguridad**. En el campo ubicado a la derecha de la casilla **Conservar objetos como máximo N días**, especifique el plazo máximo de almacenamiento para las copias de los archivos en Copia de seguridad.
4. Guarde los cambios.

# Configuración del tamaño máximo de Copias de seguridad

Puede especificar el tamaño máximo de Copia de seguridad. El tamaño de Copias de seguridad es ilimitado de forma predeterminada. Después de que alcanza el tamaño máximo, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos de Copias de seguridad para que no se supere el tamaño máximo.

*Para configurar el tamaño máximo de Copias de seguridad, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **Informes y repositorios**.
3. Si desea limitar el tamaño de Copia de seguridad, seleccione la casilla **Limitar el tamaño de 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 desde el Depósito de copias de seguridad

Si se detecta código malintencionado en el archivo, Kaspersky Endpoint Security bloquea el archivo, le asigna el estado de *Infectado*, coloca una copia en el Depósito de copias de seguridad e intenta desinfectarlo. Si se lleva a cabo una desinfección de un archivo, el estado de la copia de seguridad del archivo cambia a *Desinfectado*. El archivo queda disponible en su carpeta original. Si no se puede desinfectar un archivo, Kaspersky Endpoint Security lo elimina de su carpeta original. Puede restaurar el archivo de su copia de seguridad a su carpeta original.

Los archivos de estado *Se desinfectará al reiniciar el equipo* no se pueden restaurar. Reinicie el equipo para que el estado cambie a *Desinfectado* o *Eliminado*. Si tiene una copia de seguridad del archivo, puede restaurarla a su carpeta original.

Después de detectar código malintencionado en un archivo que es parte de la aplicación Tienda Windows, Kaspersky Endpoint Security inmediatamente elimina el archivo sin pasar una copia a Copia de seguridad. Puede restaurar la integridad de la aplicación de la Tienda Windows con las herramientas adecuadas del sistema operativo Microsoft Windows 8 (para obtener información sobre la restauración de aplicaciones de la Tienda Windows, consulte los *archivos de ayuda de Microsoft Windows 8*).

El conjunto de copias de seguridad de los archivos se presenta en forma de tabla. Para una copia de seguridad de un archivo, se muestra la ruta a la carpeta original del archivo. La ruta a la carpeta original del archivo puede contener datos personales.

Si varios archivos con nombres idénticos y contenido diferente localizados en la misma carpeta se mueven a Copias de seguridad, solamente se podrá restaurar el archivo que se movió en último lugar a Copias de seguridad.

*Para restaurar los archivos desde el Depósito de copias de seguridad:*

1. En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Almacenamiento**.

   Se abre la ventana **Copias de seguridad**.
2. En la tabla de la ventana **Depósito de copias de seguridad**, seleccione uno o más archivos de Copias de seguridad.
3. Haga clic en el botón **Restaurar**.

   Kaspersky Endpoint Security restaura archivos desde las copias de seguridad seleccionadas a sus carpetas originales.

# Eliminar copias de seguridad de archivos de Copias de seguridad

Una vez transcurrido el plazo de almacenamiento definido en la configuración de la aplicación, Kaspersky Endpoint Security elimina automáticamente las copias de seguridad de los archivos con cualquier estado. También puede eliminar manualmente de Copias de seguridad cualquier copia de un archivo.

*Para eliminar copias de seguridad de archivos desde el Depósito de copias de seguridad:*

1. En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Almacenamiento**.

   Se abre la ventana **Copias de seguridad**.

2. Seleccione las copias de seguridad de los archivos que desea eliminar de Copia de seguridad y haga clic en el botón **Eliminar**. También puede eliminar todos los archivos de Copia de seguridad; para eso, debe hacer clic en el botón **Eliminar todo**.

Kaspersky Endpoint Security elimina todas las copias de seguridad de archivos seleccionadas del Depósito de copias de seguridad.

# Servicio de notificación

Se producen todo tipo de eventos durante el funcionamiento de Kaspersky Endpoint Security. Las notificaciones de estos eventos pueden ser puramente informativas o contener información crítica. Por ejemplo, una notificación puede sencillamente informar que las bases de datos y los módulos se han actualizado correctamente, o puede dar aviso de un problema en un componente que deba resolverse.

Kaspersky Endpoint Security admite el registro de información sobre eventos en la operación del registro de aplicación de Microsoft Windows o el registro de eventos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security proporciona notificaciones de las siguientes maneras:

- usando notificaciones emergentes en el área de notificaciones de la barra de tareas de Microsoft Windows;
- por correo electrónico.

Puede configurar la entrega de notificaciones de eventos. El método de entrega de notificación se configura para cada tipo de evento.

Cuando usa la tabla de eventos para configurar el servicio de notificaciones, puede realizar las siguientes acciones:

- Filtrar eventos de servicio de notificación mediante el valor de columna o con condiciones de filtros personalizadas.
- Usar la función de búsqueda para eventos de servicio de notificación.
- Ordenar eventos de servicios de notificación.
- Cambiar el orden y el conjunto de columnas que se muestran en la lista de eventos de servicio de notificación.

# Configuración de los parámetros del registro de eventos

*Para configurar los parámetros del registro de eventos:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana Configuración de la aplicación, seleccione la sección **Interfaz**.
3. En la sección **Notificaciones**, haga clic en el botón **Configurar notificaciones**.

   Los componentes y las tareas de Kaspersky Endpoint Security se muestran en la parte izquierda de la ventana. En la parte derecha de la ventana se enumeran los eventos generados para la tarea o el componente seleccionado.

   Los Eventos pueden contener los siguientes datos del usuario:

   - Rutas a archivos analizados por Kaspersky Endpoint Security.
   - Rutas a claves del Registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
   - Nombre de usuario de Microsoft Windows.
   - Las direcciones de páginas web abiertas por el usuario.

4. En la parte izquierda de la ventana, seleccione el componente o la tarea para el cual desea configurar los parámetros del registro de eventos.

5. En las columnas **Guardar en informe local** y **Guardar en registro de eventos de Windows**, seleccione las casillas ubicadas junto a los eventos que le resulten pertinentes.

   Los eventos cuyas casillas estén seleccionadas en la columna **Guardar en informe local** se mostrarán en el nodo **Registros de aplicaciones y servicios**, sección **Registro de eventos de Kaspersky**. Los eventos cuyas casillas estén seleccionadas en la columna **Guardar en registro de eventos de Windows** se muestran en el área de **Registros de Windows** de la sección **Aplicación**. Para abrir los registros de eventos, seleccione **Inicio** → **Panel de control** → **Administración** → **Visor de eventos**.

6. Guarde los cambios.

## Configuración de la visualización y el envío de notificaciones

*Para configurar la visualización y el envío de notificaciones:*

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

2. En la ventana Configuración de la aplicación, seleccione la sección **Interfaz**.

3. En la sección **Notificaciones**, haga clic en el botón **Configurar notificaciones**.

   Los componentes y las tareas de Kaspersky Endpoint Security se muestran en la parte izquierda de la ventana. En la parte derecha de la ventana se enumeran los eventos generados para el componente o la tarea seleccionado.

   Los Eventos pueden contener los siguientes datos del usuario:

   - Rutas a archivos analizados por Kaspersky Endpoint Security.
   - Rutas a claves del Registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
   - Nombre de usuario de Microsoft Windows.
   - Las direcciones de páginas web abiertas por el usuario.

4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los cuales desea configurar el envío de notificaciones.

5. En la columna **Notificar en la pantalla**, seleccione las casillas junto a los eventos requeridos.

   La información acerca de los eventos seleccionados se muestra en la pantalla como mensajes emergentes en el área de notificación de la barra de tareas de Microsoft Windows.

6. En la columna **Notificar por correo electrónico**, seleccione las casillas junto a los eventos requeridos.

   La información sobre los eventos seleccionados se entrega por correo electrónico si se configuraron los parámetros de entrega de notificaciones por correo.

7. Haga clic en **Aceptar**.

8. Si habilitó las notificaciones por correo electrónico, defina la configuración para la entrega de correo electrónico:

   a. Haga clic en el botón **Parámetros de notificaciones por correo electrónico**.

b. Seleccione la casilla **Notificar sobre eventos** para habilitar el envío de notificaciones sobre los eventos de Kaspersky Endpoint Security seleccionados en la columna **Notificar por correo electrónico**.

c. Especifique los parámetros de envío de notificaciones por correo electrónico.

d. Haga clic en **Aceptar**.

9. Guarde los cambios.

## Configuración de la visualización de advertencias acerca del estado de la aplicación en el área de notificación

*Para configurar la visualización de advertencias acerca del estado de la aplicación en el área de notificación:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana Configuración de la aplicación, seleccione la sección **Interfaz**.
3. En la sección **Mostrar el estado de la aplicación en el área de notificaciones**, seleccione las casillas que se encuentran frente a las categorías de eventos sobre las cuales quiera ver notificaciones en el área de notificación de Microsoft Windows.
4. Guarde los cambios.

Cuando se registren eventos asociados con las categorías seleccionadas, el icono de la aplicación en el área de notificación pasará a o a , en función de la gravedad de la advertencia.

# Administración de informes

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la ejecución de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se registra en informes.

Los Informes se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES\Report`.

Los Informes pueden contener los siguientes datos del usuario:

- Rutas a archivos analizados por Kaspersky Endpoint Security.
- Rutas a claves del Registro modificadas cuando Kaspersky Endpoint Security está en funcionamiento.
- Nombre de usuario de Microsoft Windows.
- Las direcciones de páginas web abiertas por el usuario.

Los datos de un informe se presentan en forma de tabla. Cada fila de la tabla contiene información sobre un evento individual. Los atributos del evento se ubican en las columnas de la tabla. Ciertas columnas son compuestas y contienen columnas anidadas con atributos adicionales. Para ver los atributos adicionales, haga clic en el botón ⊞ que verá junto al nombre de la columna. Los eventos registrados mientras los distintos componentes o las distintas tareas están en ejecución poseen diferentes conjuntos de atributos.

Están disponibles los siguientes informes:

- Informe de **Auditoría del sistema**. Contiene información sobre eventos que ocurren durante la interacción entre el usuario y la aplicación y en el transcurso del funcionamiento de la aplicación en general, que no están relacionados con ningún componente ni tarea en particular de Kaspersky Endpoint Security.
- Informes sobre el funcionamiento de los componentes de Kaspersky Endpoint Security.
- Informes de las tareas de Kaspersky Endpoint Security.
- Informe de **cifrado de datos**. Contiene información sobre eventos que ocurren durante el cifrado y descifrado de datos.

En los informes se usan los siguientes niveles de importancia de eventos:

ⓘ **Mensajes informativos**. Eventos de referencia que normalmente no contienen información importante.

⚠ **Advertencias**. Eventos que requieren atención dado que reflejan situaciones importantes relacionadas con el funcionamiento de Kaspersky Endpoint Security.

⚠ **Eventos críticos**. Eventos de importancia crítica que indican problemas en el funcionamiento de Kaspersky Endpoint Security o vulnerabilidades en la protección del equipo del usuario.

Para el procesamiento conveniente de los informes, es posible modificar la presentación de los datos en la pantalla de las siguientes formas:

- Filtrar la lista de eventos según distintos criterios.
- Usar la función de búsqueda para encontrar un evento específico.
- Ver el evento seleccionado en una sección separada.

- Ordenar la lista de eventos por cada columna del informe.
- Usar el botón ⊞ para mostrar y ocultar eventos que se hayan agrupado con el filtro de eventos.
- Cambiar el orden y la organización de las columnas que se muestran en el informe.

Puede guardar el informe generado en un archivo de texto, si es necesario. También puede eliminar la información del informe sobre los componentes y las tareas de Kaspersky Endpoint Security que están combinados en grupos.

Cuando Kaspersky Endpoint Security se ejecuta bajo la órbita administrativa de Kaspersky Security Center, puede transmitir información sobre los eventos al Servidor de administración de Kaspersky Security Center (para más detalles, consulte la *Guía de ayuda de Kaspersky Security Center*).

## Ver informes

Si un usuario puede ver informes, el usuario también puede ver todos los eventos reflejados en los informes.

*Para visualizar informes:*

1. En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Informes**.
2. A la izquierda de la ventana **Informes**, en la lista de componentes y tareas, seleccione un componente o una tarea.

   La parte derecha de la ventana muestra un informe que contiene una lista de eventos resultantes de la operación del componente o tarea seleccionado de Kaspersky Endpoint Security. Puede clasificar los eventos en el informe utilizando los valores en las celdas de una de las columnas. Por defecto, los eventos del informe se disponen en orden ascendente según los valores en las celdas de la columna **Fecha de evento**.
3. Para ver los detalles de un evento en particular, seleccione el evento que le interese en el informe.

   Se presenta una sección con el resumen del evento en la parte inferior de la ventana.

## Configuración de la duración máxima del almacenamiento de informes

El plazo de almacenamiento máximo de los informes sobre eventos registrados en Kaspersky Endpoint Security es de 30 días. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.

*Para modificar la duración máxima del almacenamiento de informes:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **Informes y repositorios**.
3. Si desea limitar el período de almacenamiento de informes, seleccione la casilla **Conservar informes como máximo N días** en el bloque **Informes**. Defina la duración máxima del almacenamiento de informes.
4. Guarde los cambios.

## Configuración del tamaño máximo del archivo del informe

Puede especificar el tamaño máximo del archivo que contiene el informe. El tamaño máximo predeterminado del archivo del informe es de 1024 MB. Para evitar que se exceda el tamaño máximo del archivo del informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas de este archivo cuando alcanza el tamaño máximo.

*Para configurar el tamaño máximo del archivo del informe:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **Informes y repositorios**.
3. En el bloque **Informes**, seleccione la casilla **Limitar el tamaño del archivo de los informes a N MB** si desea limitar el tamaño de un archivo de informe. Defina el tamaño máximo del archivo del informe.
4. Guarde los cambios.

## Almacenamiento de informes en archivos

El usuario es responsable personalmente de asegurar la seguridad de la información desde un informe guardado al archivo, y en particular de controlar y restringir el acceso a esta información.

Puede guardar el informe generado en un archivo en formato de texto (TXT) o en un archivo CSV.

Kaspersky Endpoint Security registra los eventos en el informe de la misma manera en la que aparecen en pantalla: en otras palabras, con el mismo conjunto y la misma secuencia de atributos del evento.

*Para guardar un informe en un archivo:*

1. En la ventana principal de la aplicación, haga clic en **Más herramientas** → **Informes**.
2. En la ventana que se abre, seleccione el componente o la tarea.

   Se muestra un informe a la derecha de la ventana, el cual contiene una lista de los eventos que tuvieron lugar durante el funcionamiento del componente o la tarea de Kaspersky Endpoint Security que se hayan seleccionado.
3. Si es necesario, puede modificar la presentación de datos en el informe mediante las siguientes acciones:
   - Filtrar eventos
   - Ejecutar una búsqueda de eventos
   - Reorganizar las columnas
   - Ordenar los eventos
4. Haga clic en el botón **Guardar informe** en la parte derecha de la ventana.

5. En la ventana que se abre, especifique la carpeta de destino para el archivo de informe.
6. En el campo **Nombre de archivo**, escriba el nombre del archivo de informe.
7. En el campo **Tipo de archivo**, seleccione el formato de archivo de informe necesario: TXT o CSV.
8. Guarde los cambios.

## Borrado de informes

*Para eliminar información de los informes:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **Informes y repositorios**.
3. En el bloque **Informes**, haga clic en el botón **Borrar**.
4. Si la Protección con contraseña está habilitada, Kaspersky Endpoint Security puede solicitarle las credenciales de la cuenta de usuario. La aplicación solicita las credenciales de la cuenta si el usuario no tiene los permisos necesarios.

Kaspersky Endpoint Security eliminará todos los informes de todos los componentes y las tareas de la aplicación.

# Autoprotección de Kaspersky Endpoint Security

Kaspersky Endpoint Security protege el equipo contra aplicaciones maliciosas de distintos tipos, que buscan inhabilitar o incluso 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 |
|---|---|---|---|
| **El mecanismo de Autoprotección** | La tecnología bloquea el acceso a los siguientes componentes de la aplicación:<br>• Archivos de la carpeta de instalación de Kaspersky Endpoint Security<br>• Claves de registro con informes pertenecientes a la aplicación<br>• Procesos que la aplicación ejecuta | ✓ | ✓ |
| **AM-PPL (Antimalware Protected Process Light)** | La tecnología evita que los procesos de Kaspersky Endpoint Security se vean afectados por acciones maliciosas. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft.<br>La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019. | ✓ | – |
| **Mecanismo de protección de administración externa** | La tecnología restringe la gestión de Kaspersky Endpoint Security mediante aplicaciones de administración remota especiales (como TeamViewer o RemotelyAnywhere). | ✓ | – (excepto para Windows 7) |

# Habilitar y deshabilitar el componente Autoprotección

El mecanismo de Autoprotección de Kaspersky Endpoint Security está habilitado por defecto.

*Para habilitar o deshabilitar la Autoprotección:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **General**.
3. Utilice la casilla **Habilitar Autoprotección** para habilitar o deshabilitar el mecanismo de autoprotección.
4. Guarde los cambios.

# Habilitar y deshabilitar la compatibilidad con AM-PPL

Kaspersky Endpoint Security es compatible con una tecnología de Microsoft denominada Antimalware Protected Process Light (en adelante, "AM-PPL"). AM-PPL evita que los procesos de Kaspersky Endpoint Security se vean afectados por acciones malintencionadas; puede impedir, por ejemplo, el cierre de la aplicación. AM-PPL no permite que un proceso se ejecute si no es de confianza. Los procesos de Kaspersky Endpoint Security, al estar firmados como lo exigen los requisitos de seguridad de Windows, se consideran de confianza. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está habilitada por defecto.

Kaspersky Endpoint Security también cuenta con mecanismos propios para proteger sus procesos. Si opta por utilizar AM-PPL, la protección de los procesos quedará en manos del sistema operativo. Con ello, se reducirá el uso de recursos del equipo y aumentará la velocidad de la aplicación.

El servicio AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019.

*Para habilitar o deshabilitar la tecnología AM-PPL:*

1. Desactive el mecanismo de Autoprotección de la aplicación.

   El mecanismo de Autoprotección evita que los procesos de la aplicación se modifiquen o se eliminen de la memoria del equipo. Una de las acciones contra las que protege es la modificación del estado de AM-PPL.

2. Abra el símbolo del sistema (cmd.exe) como administrador.

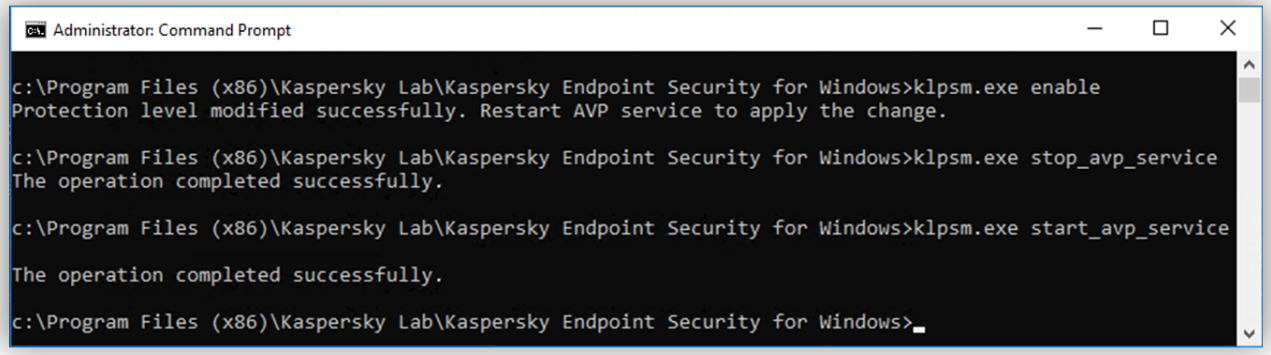
3. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.

4. En la línea de comandos, escriba lo siguiente:

   - `klpsm.exe enable`: habilitar la compatibilidad con la tecnología AM-PPL (vea la siguiente imagen).
   - `klpsm.exe disable`: deshabilitar la compatibilidad con la tecnología AM-PPL.

5. Reinicie Kaspersky Endpoint Security.

6. Reactive el mecanismo de Autoprotección de la aplicación.




Habilitar la compatibilidad con la tecnología AM-PPL

## Habilitar y deshabilitar protección de administración externa

La protección contra la administración externa permite prohibir la administración de Kaspersky Endpoint Security mediante aplicaciones de administración remota (como TeamViewer o RemotelyAnywhere). La tecnología tiene las siguientes finalidades:

- Protección contra modificaciones de la configuración de Kaspersky Endpoint Security.
- Protección contra la administración de los servicios de Kaspersky Endpoint Security (como el servicio `AVP`).
- Protección contra la detención de los procesos de la aplicación.

La protección contra la administración externa solo está disponible para equipos que ejecuten sistemas operativos de 32 bits. La tecnología no está disponible para equipos que ejecuten sistemas operativos de 64 bits.

*Para habilitar o deshabilitar la protección contra la administración externa:*

1. En la ventana principal de la aplicación haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, vaya a **Configuración avanzada** → **General**.
3. Utilice la casilla **Permitir que la configuración de Kaspersky Endpoint Security se administre a través de aplicaciones de control remoto** para habilitar o deshabilitar la protección contra modificaciones de la configuración de Kaspersky Endpoint Security. Si usa aplicaciones de administración remota, debe permitir la administración de la configuración de Kaspersky Endpoint Security y agregar las aplicaciones a la lista de confianza. No se permite que las aplicaciones de administración remota no confiables modifiquen la configuración de Kaspersky Endpoint Security ni siquiera cuando la casilla **Permitir que la configuración de Kaspersky Endpoint Security se administre a través de aplicaciones de control remoto** está seleccionada. Esta casilla no está disponible si se selecciona la casilla **Habilitar Autoprotección**.
4. Utilice la casilla **Habilitar el control externo de servicios** para habilitar o deshabilitar la protección de los servicios de Kaspersky Endpoint Security contra la administración externa.

   Para salir de la aplicación desde la línea de comandos, deshabilítela protección de los servicios de Kaspersky Endpoint Security contra la administración externa.

5. Guarde los cambios.

De esta manera, cuando los mecanismos de protección contra administración externa están habilitados, Kaspersky Endpoint Security evita que el puntero del mouse apunte al ícono de la aplicación. Cuando un usuario remoto intenta cerrar un servicio de aplicación, aparece una ventana del sistema con un mensaje de error.

## Compatibilidad con aplicaciones de administración remota

Ocasionalmente, puede necesitar usar una aplicación de administración remota mientras está habilitada la protección de administración externa.

*Para habilitar el funcionamiento de aplicaciones de administración remota:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En el bloque **Exclusiones**, haga clic en el vínculo **Especificar aplicaciones de confianza**.
4. En la ventana, haga clic en el botón **Agregar**.
5. Seleccione el archivo ejecutable de la aplicación de administración remota.

   También puede ingresar manualmente la ruta. Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara.
6. Seleccione la casilla **No supervisar la actividad de la aplicación**.
7. Guarde los cambios.

# Rendimiento de Kaspersky Endpoint Security y su compatibilidad con otras aplicaciones

## Rendimiento de Kaspersky Endpoint Security

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

## Selección de tipos de objetos detectables

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

## Uso del modo de ahorro de energía

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

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

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

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

## Dispensación de recursos del equipo a otras aplicaciones

El uso de recursos del equipo que realiza Kaspersky Endpoint Security puede afectar el rendimiento de otras aplicaciones. Para resolver el problema del funcionamiento simultáneo durante períodos de mayor carga en la CPU y en los subsistemas del disco duro, Kaspersky Endpoint Security puede suspender tareas programadas y conceder recursos a otras aplicaciones.

Sin embargo, varias aplicaciones se inician inmediatamente en cuanto se liberan recursos de la CPU y funcionan en segundo plano. Para evitar que el análisis dependa del rendimiento de otras aplicaciones, conviene no dispensarles recursos del sistema operativo.

Puede iniciar manualmente esas tareas, si es necesario.

### Uso de tecnología de desinfección avanzada

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

Una vez completado el proceso de desinfección avanzada en un equipo con Microsoft Windows para estaciones de trabajo, Kaspersky Endpoint Security solicita el permiso del usuario para reiniciar el equipo. Después del reinicio del sistema, Kaspersky Endpoint Security elimina los archivos de malware e inicia una análisis completo "ligero" del equipo.

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

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

## Selección de tipos de objetos detectables

*Para seleccionar los tipos de objetos detectables:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En la sección **Tipos de objetos detectados**, seleccione las casillas ubicadas junto a 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 virus y gusanos tradicionales realizan acciones no autorizadas por el usuario. Pueden crear copias de sí mismos capaces de replicarse.

**Virus habitual**

Cuando un virus tradicional ingresa a un equipo, lo que hace es infectar un archivo, activarse, realizar acciones malintencionadas y agregar copias de sí mismo a otros archivos.

Los virus tradicionales solo se multiplican en los recursos locales del equipo; no pueden penetrar otros equipos por sí mismos. Solo pueden pasar a otro equipo si agregan una copia de sí mismos a un archivo almacenado en una carpeta compartida o en un CD dentro del equipo, o si el usuario reenvía un mensaje de correo con un archivo adjunto infectado.

El código de los virus tradicionales puede penetrar diversas áreas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de scripts* y *virus de macros*.

Los virus pueden infectar archivos mediante una variedad de técnicas. *Los virus de sobreescritura* escriben su código sobre el código del archivo infectado y borran el contenido de este. El archivo infectado deja de funcionar y no se puede restaurar. *Los virus parasitarios* modifican archivos y los dejan total o parcialmente funcionales. *Los virus de acompañamiento* no modifican archivos, sino que crean duplicados de ellos. Cuando se abre un archivo infectado, se inicia un duplicado de este (que, en realidad, es un virus). También es posible encontrarse con los siguientes tipos de virus: *virus de 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. Los gusanos reciben este nombre debido a su capacidad para "arrastrarse" de un equipo a otro y propagar copias de sí mismos sin el permiso del usuario mediante numerosos canales de datos.

La principal función que permite diferenciar los distintos tipos de gusanos es la forma de propagarse. La siguiente tabla proporciona un resumen de distintos tipos de gusanos, clasificados según la forma en que se propagan.

Formas de propagación

| Tipo | Nombre | Descripción |
|---|---|---|
| **Gusano de correo** | Gusano de correo | Se propagan mediante el correo.<br>Un mensaje de correo infectado contiene un documento adjunto con una copia de un gusano o un vínculo a un archivo cargado en un sitio web que puede haber sufrido un ataque o haber sido creado exclusivamente con ese fin. Cuando se abre el documento adjunto, se activa el gusano. Cuando se hace clic en el vínculo, se descarga y se abre el archivo, y el gusano empieza a realizar acciones malintencionadas. Después de esto, empieza a distribuir copias de sí mismo. Para ello, busca otras direcciones de correo y les envía mensajes infectados. |
| **IM-Worm** | Clientes de MI | Se propagan a través de clientes de MI. |

| | | |
|---|---|---|
| | | Por lo general, estos gusanos envían mensajes que incluyen un vínculo a un archivo con una copia del gusano ubicado en un sitio web y utilizan las listas de contactos del usuario. Cuando el usuario descarga el archivo y lo abre, se activa el gusano. |
| **IRC-Worm** | Gusanos de chat de Internet | Se propagan mediante Internet Relay Chats, sistemas de servicio que permiten comunicarse con otras personas a través de Internet en tiempo real.<br>Estos gusanos publican un archivo con una copia de sí mismos o un vínculo al archivo en un chat de Internet. Cuando el usuario descarga el archivo y lo abre, se activa el gusano. |
| **Gusano de red** | Gusanos de red | Estos gusanos se propagan a través de redes de equipos.<br>A diferencia de otros tipos de gusanos, un gusano de red típico se propaga sin la participación del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red (punto vulnerable) especialmente formado que contiene el código del gusano o una parte de él. Si en la red hay algún equipo "vulnerable", recibe este paquete de red. El gusano se activa una vez que penetra completamente en el equipo. |
| **P2P-Worm** | Gusanos de redes de uso compartido de archivos | Se propagan mediante redes punto a punto de uso compartido de archivos.<br>Para infiltrar una red P2P, el gusano se copia en una carpeta de uso compartido de archivos que, por lo general, está situada en el equipo del usuario. La red P2P muestra información sobre este archivo, de modo que el usuario pueda "encontrar" el archivo infectado en la red como a cualquier otro archivo, descargarlo y abrirlo.<br>Gusanos más sofisticados emulan el protocolo de red de una red P2P específica: devuelven respuestas positivas a solicitudes de búsqueda y ofrecen copias de sí mismo para su descarga. |
| **Gusano** | Otros tipos de gusanos | Otros tipos de gusanos incluyen los siguientes:<br>• Gusanos que distribuyen copias de sí mismos por los recursos de red. Al utilizar las funciones del sistema operativo, buscan carpetas disponibles de red, se conectan a equipos conectados a Internet e intentan obtener acceso total a sus unidades de disco. A diferencia de los tipos de gusanos descritos anteriormente, otras clases de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano.<br>• Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono móvil a otro). |

- Troyanos

**Subcategoría**: Troyanos

**Nivel de amenaza**: alto

A diferencia de los gusanos y los virus, los troyanos no se autorreplican. Por ejemplo, penetran un equipo a través del correo o un navegador cuando el usuario visita una página web infectada. Los troyanos requieren la participación del usuario para iniciarse. Comienzan a realizar acciones malintencionadas inmediatamente después de iniciarse.

Los distintos troyanos se comportan de manera diferente en los equipos infectados. Las principales funciones de los troyanos consisten en bloquear, modificar o destruir información y en deshabilitar equipos o redes. Los troyanos también reciben o envían archivos, los ejecutan, muestran mensajes en pantalla, solicitan páginas web, descargan e instalan programas y reinician equipos.

Con frecuencia, los piratas usan "conjuntos" de varios troyanos.

Los tipos de comportamiento de los caballos de troya se describen en la siguiente tabla.

Tipos de comportamiento de caballos de troya en equipos infectados

| Tipo | Nombre | Descripción |
|---|---|---|
| **Trojan-ArcBomb** | Troyanos: "bombas en archivos de almacenamiento" | Cuando se descomprimen, estos archivos de almacenamiento aumentan de tamaño en una medida tal que afecta el funcionamiento del equipo.<br>Cuando el usuario intenta descomprimir un archivo de almacenamiento de esta clase, es posible que el equipo se ralentice o se bloquee, y el disco duro puede llenarse de datos "vacíos". Las "bombas en archivo de almacenamiento" son especialmente peligrosas para los servidores de correo y de archivos. Si el servidor utiliza un sistema automático para procesar la información entrante, una "bomba en archivo de almacenamiento" puede detener el servidor. |
| **Backdoor** | Troyanos de administración remota | Se considera que son los troyanos más peligrosos. Funcionan de manera bastante similar a las aplicaciones de administración remota instaladas en los equipos.<br>Estos programas se instalan en el equipo sin que el usuario los detecte, lo que permite al intruso administrarlo de forma remota. |
| **Caballo de troya** | Troyanos | En esta categoría se incluyen las siguientes aplicaciones malintencionadas:<br>• **Troyanos tradicionales**. Estos programas solo realizan las funciones principales de los troyanos: bloquear, modificar o destruir información y deshabilitar equipos o redes. A diferencia de los otros tipos de troyano descritos en la tabla, estos no tienen funciones avanzadas.<br>• **Troyanos versátiles**. Estos programas tienen funciones avanzadas típicas de diversos tipos de troyanos. |
| **Trojan-Ransom** | Ransom troyanos | Toman la información del usuario como "rehén", modificándola o bloqueándola, o afectan el funcionamiento del equipo, de modo que el usuario pierde la capacidad de utilizar la información. El intruso le exige al usuario un rescate a cambio de una aplicación que permita restaurar la información y la operatividad del equipo. |

| | | |
|---|---|---|
| **Trojan-Clicker** | Trojan-Clicker | Acceden a páginas web desde el equipo del usuario, ya sea mediante el envío de comandos a un navegador por su cuenta o por medio de la modificación de las direcciones web especificadas en los archivos del sistema operativo.<br>Al utilizar estos programas, los intrusos realizan ataques de red e incrementan las visitas a sitios web, lo que aumenta la cantidad de anuncios publicitarios que se muestran. |
| **Trojan-Downloader** | Descargadores troyanos | Acceden a la página web del intruso para descargar de allí otra aplicación malintencionada e instalarla en el equipo del usuario. El nombre del archivo que se debe descargar puede venir establecido de antemano dentro del troyano o puede determinarse al acceder a la página del atacante. |
| **Trojan-Dropper** | Caballos de troya instaladores de software malintencionado | Contienen otros troyanos que descargan en el disco duro y luego instalan.<br>Los intrusos pueden utilizar programas de este tipo para cumplir los siguientes objetivos:<br>• Instalar una aplicación malintencionada sin que el usuario lo advierta: Los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (por ejemplo, pueden advertir sobre la existencia de un archivo dañado o sobre incompatibilidades en el sistema operativo).<br>• Impedir la detección de una aplicación malintencionada conocida. No todos los antivirus son capaces de detectar aplicaciones malintencionadas cuando vienen ocultas en troyanos de este tipo. |
| **Trojan-Notifier** | Caballos de troya notificadores | Le informan al atacante que puede introducirse en el sistema infectado y le envían información sobre el equipo: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso por medio de correo, FTP, ingreso a la página web del intruso o de otra manera.<br>Los troyanos notificadores suelen utilizarse en conjuntos conformados por varios troyanos. Informan al intruso que se han instalado correctamente otros troyanos en el equipo del usuario. |
| **Trojan-Proxy** | Caballos de troya proxy | Permiten al intruso acceder de forma anónima a páginas web mediante el equipo del usuario. Con frecuencia, se utilizan para enviar correo no deseado. |
| **Trojan-PSW** | Programas que roban contraseñas | Los programas que roban contraseñas son una clase de caballo de troya que roba cuentas de usuarios, tales como datos de registro de software. Estos troyanos encuentran datos confidenciales en archivos del sistema y en el Registro y se los envían a su "maestro" mediante correo, FTP, acceso a la página web del intruso o de otro modo.<br>Algunos de estos troyanos se categorizan en los distintos tipos descritos en esta tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan por Internet (Trojan-GameThief). |
| **Trojan-Spy** | Caballos de troya espías | Espían al usuario y reúnen información acerca de las acciones que este realiza cuando trabaja en el equipo. Pueden interceptar los datos introducidos por el usuario |

| | | |
|---|---|---|
| | | mediante el teclado, realizar capturas de pantalla o compilar listas de aplicaciones activas. Después de recibir la información, se la transfieren al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. |
| **Trojan-DDoS** | Caballos de troya atacantes de red | Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). Los piratas suelen infectar muchos equipos con estos programas de manera de utilizar los equipos para atacar a un único servidor simultáneamente.<br>Los programas DoS llevan a cabo un ataque desde un único equipo con el conocimiento del usuario. Los programas DDoS (DoS distribuida) llevan a cabo ataques distribuidos desde distintos equipos sin que lo advierta el usuario del equipo infectado. |
| **Trojan-IM** | Troyanos que roban información de usuarios de clientes de mensajería instantánea | Roban los números de cuenta y contraseñas de quienes usan clientes de mensajería instantánea. Transfieren los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. |
| **Rootkit** | RootKits | Enmascaran la existencia y las acciones de otras aplicaciones malintencionadas para ayudarlas a perdurar en el sistema operativo. También pueden ocultar archivos, claves del registro que se utilicen para ejecutar aplicaciones malintencionadas o procesos que se encuentren cargados en la memoria del equipo infectado. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones en el equipo del usuario y en otros equipos de la red. |
| **Trojan-SMS** | Troyanos en la forma de mensajes SMS | Infectan teléfonos móviles y envían mensajes SMS a números de teléfono con tarifas elevadas. |
| **Trojan-GameThief** | Troyanos que roban información de usuarios de juegos en línea | Roban credenciales de las cuentas de usuarios de juegos en línea, tras lo cual envían los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. |
| **Trojan-Banker** | Troyanos que roban cuentas bancarias | Roban datos de cuentas bancarias o de sistemas de dinero electrónico y luego envían la información al hacker por correo electrónico, por FTP, a través de una página creada por el atacante o usando otros medios. |
| **Trojan-Mailfinder** | Troyanos que reúnen direcciones de correo | Recopilan direcciones de correo almacenadas en un equipo y se las envían al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado. |

- Herramientas maliciosas

**Subcategoría**: Herramientas maliciosas

**Nivel de peligrosidad**: medio

A diferencia de otros tipos de software malware, las herramientas maliciosas no realizan acciones inmediatamente después de iniciarse. Pueden almacenarse de manera segura e iniciarse en el equipo del usuario. A menudo, los intrusos utilizan las funciones de estos programas para crear virus, gusanos y troyanos, perpetrar ataques de red en servidores remotos, atacar equipos o llevar a cabo otras acciones malintencionadas.

Varias funciones de las herramientas maliciosas se agrupan en los tipos descritos en la siguiente tabla.

Funciones de herramientas maliciosas

| Tipo | Nombre | Descripción |
|---|---|---|
| **Constructor** | Constructores | Permiten crear nuevos virus, gusanos y troyanos. Algunos constructores ofrecen una interfaz estándar, con ventanas para elegir el tipo de aplicación malintencionada que se va a crear, los métodos que se usarán para contrarrestar los depuradores y otras características. |
| **Dos** | Ataque de red | Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). |
| **Exploit** | Exploits | Los puntos vulnerables son conjuntos de datos o un código de programa que se sirve de las vulnerabilidades de la aplicación en la que se procesa para realizar una acción malintencionada en un equipo. Por ejemplo, un punto vulnerable puede escribir o leer archivos o solicitar páginas web "infectadas".<br>Distintos puntos vulnerables se sirven de las vulnerabilidades de diversos servicios de red o aplicaciones. Disfrazados como paquete de red, los puntos vulnerables se transfieren a través de la red a numerosos equipos y buscan equipos con servicios de red vulnerables. Un punto vulnerable en un archivo DOC se sirve de las vulnerabilidades de un editor de texto. Puede comenzar a realizar las acciones preprogramadas por el pirata cuando el usuario abre el archivo infectado. Un punto vulnerable incrustado en un mensaje de correo busca vulnerabilidades en cualquier cliente de correo. Puede empezar a realizar una acción malintencionada apenas el usuario abre el mensaje infectado en dicho cliente.<br>Los gusanos de red se propagan por las redes mediante los puntos vulnerables. Los puntos vulnerables *Nuker* son paquetes de red que deshabilitan equipos. |
| **FileCryptor** | Cifradores | Se utilizan para cifrar otras aplicaciones malintencionadas y evitar, con ello, que las aplicaciones antivirus las detecten. |
| **Flooder** | Programas para "contaminar" redes | Envían numerosos mensajes a través de canales de red. Este tipo de herramienta incluye, por ejemplo, programas que contaminan Internet Relay Chats. |

| | | |
|---|---|---|
| | | Las herramientas de tipo "flooder" no incluyen programas que "contaminan" los canales usados por el correo, los clientes de mensajería instantánea y los sistemas de comunicaciones móviles. Estos programas se describen de manera individual en la tabla (flooder de correo, IM-Flooder y flooder de SMS). |
| **HackTool** | Herramientas de piratería | Permiten los ataques a los equipos en los que están instalados o atacan otro equipo (por ejemplo, mediante la adición de nuevas cuentas de sistema sin el permiso del usuario o la eliminación de registros del sistema para ocultar rastros de su presencia en el sistema operativo). Este tipo de herramienta incluye algunos analizadores de protocolos que ofrecen funciones malintencionadas, como la interceptación de contraseñas. Los analizadores de protocolos son programas que permiten ver el tráfico de red. |
| **Hoax** | Hoax | Alarman al usuario con mensajes similares a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario de que se dio formato a un disco, cuando esto no sucedió en realidad. |
| **Spoofer** | Herramientas de falsificación | Envían mensajes y solicitudes de red con una dirección falsa del remitente. Los intrusos utilizan herramientas de falsificación para hacerse pasar por los verdaderos remitentes de los mensajes, por ejemplo. |
| **VirTool** | Herramientas que pueden ingresar modificaciones en las aplicaciones malintencionadas | Permiten la modificación de otros programas de software malware y los ocultan de las aplicaciones antivirus. |
| **Email-Flooder** | Programas que "contaminan" las direcciones de correo | Envían numerosos mensajes a varias direcciones de correo electrónico y, de este modo, las contaminan. Un gran volumen de mensajes entrantes impide que los usuarios vean mensajes deseados en sus buzones. |
| **IM-Flooder** | Programas que "contaminan" el tráfico de los clientes de MI | "Inundan" a los usuarios de clientes de MI con mensajes. Un gran volumen de mensajes impide a los usuarios visualizar mensajes entrantes deseados. |
| **SMS-Flooder** | Programas que "contaminan" el tráfico con mensajes SMS | Envían numerosos mensajes de SMS a teléfonos móviles. |

- Adware

**Subcategoría**: software de publicidad (Adware);

**Nivel de amenaza**: medio

El adware muestra información publicitaria al usuario. Los programas de adware muestran anuncios publicitarios en las interfaces de otros programas y redireccionan las solicitudes de búsqueda a páginas web publicitarias. Algunos reúnen información de marketing acerca del usuario y la envían a su desarrollador. Esta información puede incluir los nombres de los sitios web visitados por el usuario o el contenido de sus solicitudes de búsqueda. A diferencia de los caballos de troya espías, el adware envía esta información al desarrollador con el permiso del usuario.

- Marcadores automáticos

**Subcategoría**: software legal que los delincuentes pueden usar para dañar el equipo o sus datos personales

**Nivel de peligrosidad**: medio

La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP, y Telnet.

Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

| Tipo | Nombre | Descripción |
|---|---|---|
| **Client-IRC** | Clientes de chat de Internet | Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware. |
| **Dialer** | Marcadores automáticos | Pueden establecer conexiones telefónicas a través de un módem en modo oculto. |
| **Downloader** | Programas para realizar descargas | Pueden descargar archivos de páginas web en modo oculto. |
| **Monitor** | Programas para supervisar | Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos). |
| **PSWTool** | Restauradores de contraseñas | Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito. |
| **RemoteAdmin** | Programas de administración remota | Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos.<br>Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo. |
| **Server-FTP** | Servidores FTP | Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP. |
| **Server-Proxy** | Servidores proxy | Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **Server-Telnet** | Servidores Telnet | Funcionan como servidores Telnet. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de Telnet. |

| | | |
|---|---|---|
| **Server-Web** | Servidores web | Funcionan como servidores web. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP. |
| **RiskTool** | Herramientas para trabajar en un equipo local | Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos. |
| **NetTool** | Herramientas de red | Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos. |
| **Client-P2P** | Clientes de red P2P | Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware. |
| **Client-SMTP** | Clientes SMTP | Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **WebToolbar** | Barras de herramientas web | Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda. |
| **FraudTool** | Pseudoprogramas | Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada. |

- Otro software que los delincuentes pueden usar para dañar el equipo o sus datos personales

**Subcategoría**: software legal que los delincuentes pueden usar para dañar el equipo o sus datos personales

**Nivel de peligrosidad**: medio

La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP, y Telnet.

Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

| Tipo | Nombre | Descripción |
|---|---|---|
| **Client-IRC** | Clientes de chat de Internet | Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware. |
| **Dialer** | Marcadores automáticos | Pueden establecer conexiones telefónicas a través de un módem en modo oculto. |
| **Downloader** | Programas para realizar descargas | Pueden descargar archivos de páginas web en modo oculto. |
| **Monitor** | Programas para supervisar | Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos). |
| **PSWTool** | Restauradores de contraseñas | Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito. |
| **RemoteAdmin** | Programas de administración remota | Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos.<br>Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo. |
| **Server-FTP** | Servidores FTP | Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP. |
| **Server-Proxy** | Servidores proxy | Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **Server-Telnet** | Servidores Telnet | Funcionan como servidores Telnet. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de Telnet. |

| | | |
|---|---|---|
| **Server-Web** | Servidores web | Funcionan como servidores web. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP. |
| **RiskTool** | Herramientas para trabajar en un equipo local | Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos. |
| **NetTool** | Herramientas de red | Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos. |
| **Client-P2P** | Clientes de red P2P | Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware. |
| **Client-SMTP** | Clientes SMTP | Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **WebToolbar** | Barras de herramientas web | Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda. |
| **FraudTool** | Pseudoprogramas | Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada. |

- **Ejecutables comprimidos que puedan tener código malicioso oculto**

  Kaspersky Internet Security analiza objetos comprimidos y el módulo descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

  Para ocultar los programas peligrosos de las aplicaciones antivirus, los intrusos los comprimen mediante compresores especiales o crean archivos de empaquetado múltiple.

  Los analistas de virus de Kaspersky han identificado los compresores más utilizados por los piratas.

  Cuando Kaspersky Endpoint Security detecta uno de estos compresores en un archivo, puede darse casi por seguro que el archivo contiene una aplicación malintencionada o una aplicación que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario.

  Kaspersky Endpoint Security distingue los siguientes tipos de programas:

  - *Archivos comprimidos potencialmente peligrosos*: se usan para comprimir software malware, como virus, gusanos y troyanos.
  - *Archivos comprimidos varias veces* (nivel de amenaza medio): el objeto se comprimió tres veces con un compresor o varios.

- **Archivos de empaquetado múltiple**

Kaspersky Internet Security analiza objetos comprimidos y el módulo descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

Para ocultar los programas peligrosos de las aplicaciones antivirus, los intrusos los comprimen mediante compresores especiales o crean archivos de empaquetado múltiple.

Los analistas de virus de Kaspersky han identificado los compresores más utilizados por los piratas.

Cuando Kaspersky Endpoint Security detecta uno de estos compresores en un archivo, puede darse casi por seguro que el archivo contiene una aplicación malintencionada o una aplicación que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario.

Kaspersky Endpoint Security distingue los siguientes tipos de programas:

- *Archivos comprimidos potencialmente peligrosos*: se usan para comprimir software malware, como virus, gusanos y troyanos.
- *Archivos comprimidos varias veces* (nivel de amenaza medio): el objeto se comprimió tres veces con un compresor o varios.

4. Guarde los cambios.

## Activación o desactivación de la tecnología de desinfección avanzada

Si Kaspersky Endpoint Security no puede detener la ejecución de un software malicioso, puede usar la tecnología de desinfección avanzada. De manera predeterminada, la Desinfección avanzada está deshabilitada, ya que esta tecnología utiliza una cantidad considerable de recursos del equipo. Por lo tanto, puede habilitar la Desinfección avanzada solo al trabajar con amenazas activas.

La desinfección avanzada funciona de manera diferente para estaciones de trabajo y servidores. Para utilizar la tecnología en servidores, debe habilitar la Desinfección avanzada inmediata en las propiedades de la tarea *Análisis antivirus*. Este requisito previo no es necesario para utilizar la tecnología en estaciones de trabajo.

*Para habilitar o deshabilitar la tecnología de Desinfección avanzada, realice lo siguiente:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **General**.
3. En la sección **Modo de protección**, seleccione la casilla **Habilitar la tecnología de Desinfección avanzada** o anule su selección para habilitar o deshabilitar la tecnología de Desinfección avanzada.
4. Guarde los cambios.

De esta manera, el usuario no podrá usar la mayoría de las funciones del sistema operativo mientras se ejecuta la Desinfección avanzada. Cuando finalice la desinfección, se reiniciará el equipo.

## Activación o desactivación del modo de ahorro de energía

*Para habilitar o deshabilitar el modo de ahorro de energía:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione **Amenazas y exclusiones**.
3. En la sección **Rendimiento**, use la casilla **Posponer las tareas programadas cuando el equipo funciona con carga de batería** para habilitar o deshabilitar el modo de ahorro de energía.

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

   - 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 dispensación de recursos para otras aplicaciones

*Para habilitar o deshabilitar la dispensación de recursos para otras aplicaciones:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **General**.
3. En la sección **Rendimiento**, use la casilla **Conceder recursos a otras aplicaciones** para habilitar o deshabilitar la concesión de recursos a otras aplicaciones.

   Cuando está configurado para dispensar recursos para otras aplicaciones, Kaspersky Endpoint Security pospone las tareas programadas que ralentizan otras aplicaciones:

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

   Por defecto, la aplicación está configurada para dispensar recursos para otras aplicaciones.
4. Guarde los cambios.

# Crear y utilizar un archivo de configuración

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

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

  Para hacerlo, debe guardar el archivo de configuración en la misma carpeta del kit de distribución.

- Realizar la instalación remota de Kaspersky Endpoint Security mediante Kaspersky Security Center con la configuración predefinida.

- Migrar los parámetros de Kaspersky Endpoint Security de un equipo a otro.

*Para crear un archivo de configuración:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Administrar configuración**.
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 ingrese su nombre.

   Para usar el archivo de configuración para la instalación local o remota de Kaspersky Endpoint Security, debe llamarlo install.cfg.

5. Haga clic en el botón **Guardar**.

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

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Administrar configuración**.
3. Haga clic en el botón **Importar**.
4. En la ventana que se abre, escriba la ruta de acceso al archivo de configuración.
5. Haga clic en el botón **Abrir**.

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

# Restauración de la configuración predeterminada de la aplicación

Puede restaurar la configuración recomendada por Kaspersky for Endpoint Security en cualquier momento. Después de restaurar la configuración, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección.

*Para restaurar la configuración predeterminada de la aplicación:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón .
2. En la ventana de configuración de la aplicación, seleccione **Administrar configuración**.
3. Haga clic en el botón **Restaurar**.
4. Haga clic en el botón **Guardar**.

# Comunicación entre el administrador y los usuarios

Los componentes de Control de aplicaciones, Control de dispositivos, Control Web y Control de anomalías adaptativo permiten que los usuarios de una red LAN con equipos que tienen Kaspersky Endpoint Security instalado envíen mensajes al administrador.

Es posible que un usuario tenga que enviar un mensaje al administrador de la red corporativa local en los siguientes casos:

- El Control de dispositivos bloqueó el acceso al dispositivo.

  La plantilla del mensaje para una solicitud de acceso a un dispositivo bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección Control de dispositivos.

- Control de aplicaciones bloqueó el inicio de una aplicación.

  La plantilla del mensaje para una solicitud de permiso para iniciar una aplicación bloqueada está disponible en la interfaz de Kaspersky Endpoint Security, en la sección Control de aplicaciones.

- El Control Web bloqueó el acceso a un recurso web.

  La plantilla del mensaje para una solicitud de acceso a un recurso web bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección Control Web.

El método usado para enviar mensajes y la plantilla utilizada dependen de si se está ejecutando una directiva Kaspersky Security Center activa en el equipo que tiene Kaspersky Endpoint Security instalado, y de si hay una conexión con el Servidor de administración de Kaspersky Security Center. Pueden darse las siguientes situaciones:

- Cuando el equipo con Kaspersky Endpoint Security no se encuentra sujeto a una directiva de Kaspersky Security Center, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

  Los campos del mensaje se completan con los valores de los campos de la plantilla definida en la interfaz local de Kaspersky Endpoint Security.

- Cuando el equipo con Kaspersky Endpoint Security se encuentra sujeto a una directiva de Kaspersky Security Center, se envía un mensaje estándar al Servidor de administración de Kaspersky Security Center.

  En este caso, el administrador encontrará los mensajes de los usuarios en el repositorio de eventos de Kaspersky Security Center (vea las instrucciones para acceder a estos mensajes más abajo). Los campos del mensaje se completan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

- Si se está ejecutando una directiva por ausencia de la oficina de Kaspersky Security Center en el equipo con Kaspersky Endpoint Security instalado, el método usado para enviar mensajes depende de si hay una conexión con Kaspersky Security Center.

  - Si se establece una conexión con Kaspersky Security Center, Kaspersky Endpoint Security envía el mensaje estándar al Servidor de administración de Kaspersky Security Center.

  - Si no hay ninguna conexión con Kaspersky Security Center, el mensaje de un usuario se envía al administrador de la red de área local por correo electrónico.

  En ambos casos, los campos del mensaje se completan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

*Para visualizar el mensaje de un usuario en el almacenamiento de eventos de Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Eventos**.

   En el espacio de trabajo de Kaspersky Security Center se muestran todos los eventos que ocurren durante el funcionamiento de Kaspersky Endpoint Security, incluidos los mensajes al administrador que se reciben de usuarios de la red LAN.

3. Para configurar el filtro de eventos, en la lista desplegable **Selección de eventos**, seleccione **Solicitudes del usuario**.

4. Seleccione el mensaje enviado al administrador.

5. Haga clic en el botón **Abrir ventana de propiedades del evento** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

# Cifrado de datos

Kaspersky Endpoint Security le permite cifrar archivos y carpetas que están almacenados en unidades locales o extraíbles, o unidades extraíbles y discos duros en su totalidad. El cifrado de datos minimiza el riesgo de fugas de información que pueden ocurrir como consecuencia del robo o la pérdida de un equipo portátil, un disco extraíble o un disco duro, o cuando acceden a los datos usuarios o aplicaciones no autorizados. Kaspersky Endpoint Security utiliza el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard").

Si caducó la licencia, la aplicación no cifra nuevos datos, y los datos cifrados anteriores permanecen cifrados y disponibles para su uso. En este caso, el cifrado de datos nuevos requiere que la aplicación se active con una licencia nueva que permita el uso de cifrado.

No se garantiza que los archivos que cifre se mantengan cifrados si su licencia caduca, si infringe el Contrato de licencia de usuario final, si desinstala Kaspersky Endpoint Security o si elimina la clave de licencia o los componentes de cifrado. Esto se debe a que algunas aplicaciones, como Microsoft Office Word, crean una copia temporal de los archivos durante la modificación. Cuando se guarda el archivo original, la copia temporal reemplaza el archivo original. Por lo tanto, en un equipo que no tiene funcionalidad de cifrado o en el que esta es inaccesible, el archivo permanece no cifrado.

Kaspersky Endpoint Security ofrece los siguientes aspectos de protección de datos:

- **Cifrado de archivos en discos de equipos locales**. Puede compilar listas de archivos por extensión o grupo de extensiones y listas de carpetas almacenadas en discos locales del equipo, además de crear reglas para cifrar archivos que son creados por aplicaciones específicas. Luego de que se aplique una directiva, Kaspersky Endpoint Security cifrará y descifrará los siguientes archivos:
  - archivos agregados individualmente a listas para cifrado y descifrado;
  - archivos almacenados en carpetas agregadas a listas para cifrado y descifrado;
  - Archivos creados por aplicaciones por separado.
- **Cifrado de unidades extraíbles**. Se puede especificar una regla de cifrado predeterminada según la cual la aplicación realiza la misma acción en todos los discos extraíbles, o especificar reglas de cifrado para discos extraíbles individuales.

  La regla de cifrado predeterminada tiene menos prioridad que las reglas de cifrado creadas para discos extraíbles individuales. Las reglas de cifrado creadas para discos extraíbles del modelo de dispositivo especificado tienen menos prioridad que las reglas de cifrado creadas para discos extraíbles con el identificador del dispositivo especificado.

  Para seleccionar una regla de cifrado para archivos de un disco extraíble, Kaspersky Endpoint Security comprueba si el modelo y el identificador del dispositivo son conocidos. Luego, la aplicación realiza una de las siguientes operaciones:
  - Si se conoce el modelo del dispositivo, la aplicación usa la regla de cifrado (si la hubiera) creada para discos extraíbles del modelo de dispositivo específico.
  - Si solo se conoce el identificador del dispositivo, la aplicación usa la regla de cifrado (si la hubiera) creada para discos extraíbles con el identificador de dispositivo específico.
  - Si se conocen el modelo y el identificador del dispositivo, la aplicación usa la regla de cifrado (si la hubiera) creada para discos extraíbles con el identificador de dispositivo específico. Si no hay ninguna de esas reglas, pero sí una regla de cifrado creada para discos extraíbles con el modelo del dispositivo específico, la aplicación aplica esta regla. Si no se especifica ninguna regla de cifrado para el identificador del dispositivo ni para el modelo del dispositivo específico, la aplicación aplica la regla de cifrado predeterminada.

- Si no se conoce ni el modelo ni el id. del dispositivo, la aplicación utiliza la regla de cifrado predeterminada.

La aplicación permite preparar un disco extraíble para utilizar datos cifrados almacenados en el disco en modo portátil. Después de habilitar el modo portátil, se puede acceder a los archivos cifrados en los discos extraíbles conectados a un equipo sin funcionalidad de cifrado.

- **Administración de reglas de acceso de aplicaciones a archivos cifrados**. Para cualquier aplicación, puede crear una regla de acceso a archivos cifrados que bloquee el acceso a archivos cifrados o que permita el acceso a archivos cifrados solo como texto cifrado, que es una secuencia de caracteres obtenidos cuando se aplica el cifrado.

- **Creación de paquetes cifrados**. Puede crear archivos de almacenamiento cifrados y proteger el acceso a ellos con una contraseña. Solo se puede acceder al contenido de los archivos de almacenamiento cifrados si se ingresan las contraseñas con las que protegió el acceso a esos archivos de almacenamiento. Estos archivos de almacenamiento se pueden transmitir de manera segura a través de redes o por medio de unidades extraíbles.

- **Cifrado de disco completo**. Puede seleccionar una tecnología de cifrado: Cifrado de disco de Kaspersky o Cifrado disco de BitLocker (en adelante también llamado simplemente "BitLocker").

  *BitLocker* es una tecnología que forma parte del sistema operativo Windows. Si un equipo tiene un Módulo de plataforma segura (TPM), BitLocker lo usa para almacenar claves de recuperación que proporcionan acceso a un disco duro cifrado. Cuando se inicia el equipo, BitLocker solicita las claves de recuperación del disco duro al Módulo de plataforma segura y desbloquea la unidad. Puede configurar el uso de una contraseña y/o de un código PIN para acceder a claves de recuperación.

  Puede especificar la regla predeterminada de cifrado de disco completo y crear una lista de los discos duros que se excluirán del cifrado. Kaspersky Endpoint Security lleva a cabo el cifrado de disco completo sector por sector una vez aplicada la directiva de Kaspersky Security Center. La aplicación cifra simultáneamente todas las particiones lógicas de los discos duros.

  Una vez cifrados los discos duros del sistema, la próxima vez que se inicie el equipo, el usuario deberá superar la autenticación por medio del Agente de autenticación para poder acceder a los discos duros y cargar el sistema operativo. Para tal fin, podrá introducir la contraseña de un token o de una tarjeta inteligente que conecte al equipo, o el nombre de usuario y la contraseña de su cuenta del Agente de autenticación (cuenta que el administrador de la red de área local habrá creado con la tarea *Administrar cuentas del Agente de autenticación*). Estas cuentas se basan en las cuentas de Microsoft Windows con las que el usuario inicia sesión en el sistema operativo. Existe también la posibilidad de usar la tecnología de inicio de sesión único (SSO), que permite iniciar sesión en el sistema operativo automáticamente con el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

  > Si realiza una copia de seguridad de un equipo y, posteriormente, cifra los datos del equipo, después de lo cual restaura la copia de seguridad del equipo y vuelve a cifrar los datos del equipo, Kaspersky Endpoint Security crea duplicados de las cuentas del Agente de autenticación. Para eliminar las cuentas duplicadas, emplee la utilidad klmover con la clave `dupfix`. La utilidad klmover se incluye en la compilación de Kaspersky Security Center. Puede leer más sobre su funcionamiento en la ayuda de Kaspersky Security Center.

  Para acceder a un disco duro cifrado, es necesario utilizar un equipo en el que se haya instalado Kaspersky Endpoint Security con la característica de cifrado de disco completo. Esta precaución minimiza el riesgo de fugas de datos desde un disco duro cifrado cuando se intenta acceder al disco desde fuera de la red de área local de la empresa.

Para cifrar discos duros y discos extraíbles, puede usar la función **Solo cifrar el espacio de disco usado**. Se recomienda usar esta función solo para dispositivos nuevos que no se han usado anteriormente. Si está aplicando el cifrado a un dispositivo que ya está en uso, le recomendamos que cifre todo el dispositivo. De esta manera, se asegurará de que toda la información —incluida la información eliminada, que podría contener datos recuperables— esté protegida.

Antes de que comience el cifrado, Kaspersky Endpoint Security obtiene el mapa de sectores del sistema de archivos. La primera tanda de cifrado incluye los sectores que están ocupados por archivos al momento de iniciarse el cifrado. La segunda tanda de cifrado incluye los sectores que se escribieron después de iniciado el cifrado. Una vez finalizado el cifrado, todos los sectores que contienen datos estarán cifrados.

Una vez finalizado el cifrado, si un usuario elimina un archivo, los sectores que almacenaban el archivo eliminado se vuelven disponibles para almacenar información nueva a nivel del sistema de archivos, pero permanecen cifrados. Esto quiere decir que, después de un tiempo, todos los sectores de un dispositivo nuevo terminan por cifrarse, según se van guardando archivos en él, si este se cifra regularmente con la función **Solo cifrar el espacio de disco usado**.

El Servidor de administración de Kaspersky Security Center que controló el equipo cuando se realizó el cifrado brinda los datos necesarios para descifrar los archivos. Si el equipo que contiene los objetos cifrados estuvo, por algún motivo, controlado por un Servidor de administración diferente, existen distintos métodos para obtener acceso a la información cifrada:

- Cuando los Servidores de administración pertenecen a la misma jerarquía:
  - No es necesario realizar ninguna acción. El usuario seguirá teniendo acceso a los objetos cifrados. Las claves de cifrado se distribuyen a todos los Servidores de administración.
- Cuando los Servidores de administración son independientes:
  - Solicítele al administrador de la LAN que le brinde acceso a los objetos cifrados.
  - Restaure de datos de dispositivos cifrados con la Utilidad de restauración.
  - Restaure la configuración del Servidor de administración de Kaspersky Security Center que controló al equipo durante el cifrado desde una copia de seguridad y utilice esta configuración en el Servidor de administración que ahora controla al equipo con objetos cifrados.

Si no puede acceder a la información que se ha cifrado, siga las instrucciones especiales para el caso (Procedimiento para recuperar el acceso a archivos cifrados, Trabajar con dispositivos cifrados cuando no tenemos acceso a ellos).

## Limitaciones de la función de cifrado

La característica de cifrado de datos tiene las siguientes limitaciones:

- La aplicación crea archivos de servicio durante el cifrado. Para almacenarlos, se requiere aproximadamente un 0,5 % de espacio libro sin fragmentar en el disco duro. Si no hay suficiente espacio libre sin fragmentar en el disco duro, el cifrado no iniciará hasta que libere suficiente espacio.
- Las funciones para administrar los componentes de cifrado están disponibles en la Consola de administración de Kaspersky Security Center y en Kaspersky Security Center 12 Web Console. Kaspersky Security Center Cloud Console solo puede utilizarse para administrar BitLocker.
- Para que las funciones de cifrado estén disponibles, Kaspersky Endpoint Security debe utilizarse en conjunto con los sistemas de administración Kaspersky Security Center o Kaspersky Security Center Cloud Console (en este último caso, únicamente tendrá acceso a las funciones de BitLocker). Utilizar la característica de cifrado de datos cuando Kaspersky Endpoint Security opera en modo sin conexión no es posible porque la aplicación almacena las claves de cifrado en Kaspersky Security Center.
- Si Kaspersky Endpoint Security se ha instalado en un equipo con Microsoft Windows para servidores, la única tecnología disponible para el cifrado de discos completos será Cifrado de unidad BitLocker. Si Kaspersky

Endpoint Security se ha instalado en un equipo con Microsoft Windows para estaciones de trabajo, podrán utilizarse todas las características de cifrado de datos.

El cifrado de disco completo usando la tecnología de Cifrado de disco de Kaspersky no está disponible para discos duros que no cumplen con los requisitos de hardware y software.

No está soportada la compatibilidad entre la funcionalidad de cifrado de disco completo de Kaspersky Endpoint Security y Kaspersky Anti-Virus para UEFI. Kaspersky Anti-Virus para UEFI se inicia antes de que se cargue el sistema operativo. Cuando se usa la característica de cifrado de disco completo, la aplicación detecta que no hay un sistema operativo instalado en el equipo. Esto conduce a que Kaspersky Anti-Virus para UEFI se cierre con un error. La característica de cifrado de archivos (FLE) no afecta el funcionamiento de Kaspersky Anti-Virus para UEFI.

Kaspersky Endpoint Security admite las siguientes configuraciones:

- Unidades de disco duro, SSD y USB.

  La tecnología Cifrado de disco de Kaspersky (FDE) permite trabajar con SSD y preserva el rendimiento y la vida útil de las unidades SSD.

- Unidades conectadas por bus: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.
- Unidades no extraíbles conectadas por bus SD o MMC.
- Unidades con sectores de 512 bytes.
- Unidades con sectores de 4096 bytes que emulan 512 bytes.
- Unidades con el siguiente tipo de particiones: GPT, MBR y VBR (unidades extraíbles).
- Software integrado del estándar UEFI 64 y Legacy BIOS.
- Software integrado del estándar UEFI con arranque seguro.

  *Arranque seguro* es una tecnología diseñada para verificar firmas digitales para aplicaciones y controladores de cargadores UEFI. El arranque seguro bloquea el inicio de aplicaciones y controladores UEFI que no están firmados o firmados por editores desconocidos. Cifrado de disco de Kaspersky (FDE) es totalmente compatible con el arranque seguro. El agente de autenticación está firmado por un certificado de editor de controladores UEFI de Microsoft Windows.

  En algunos dispositivos (por ejemplo, Microsoft Surface Pro y Microsoft Surface Pro 2), se puede instalar una lista desactualizada de certificados de verificación de firma digital de forma predeterminada. Antes de cifrar la unidad, debe actualizar la lista de certificados.

- Software integrado del estándar UEFI compatible con Fast Boot.

  *Fast Boot* es una tecnología que ayuda a que el equipo se inicie más rápido. Cuando la tecnología Fast Boot está habilitada, normalmente el equipo carga solo el conjunto mínimo de controladores UEFI necesarios para iniciar el sistema operativo. Cuando la tecnología Fast Boot está habilitada, es posible que los teclados, ratones, tokens USB, paneles táctiles y pantallas táctiles USB no funcionen mientras el Agente de autenticación se está ejecutando.

  Para utilizar Cifrado de disco de Kaspersky (FDE), se recomienda deshabilitar la tecnología Fast Boot. Puede usar la Utilidad de prueba FDE para poner a prueba el funcionamiento de Cifrado de disco de Kaspersky (FDE).

Kaspersky Endpoint Security no admite las siguientes configuraciones:

- El cargador del inicio está ubicado en una unidad mientras que el sistema operativo está en otra.
- El sistema contiene software integrado del estándar UEFI 32.
- El sistema tiene tecnología Intel® Rapid Start y unidades que tienen una partición de hibernación, incluso cuando la tecnología Intel® Rapid Start está deshabilitada.
- Unidades en formato MBR con más de 10 particiones extendidas.
- El sistema tiene un archivo de intercambio ubicado en una unidad que no es del sistema.
- Sistema multiarranque con varios sistemas operativos instalados a la vez.
- Particiones dinámicas (solo se admiten particiones primarias).
- Unidades con menos del 0,5 % de espacio de disco no fragmentado libre.
- Unidades con un tamaño de sector diferente de 512 bytes o 4096 bytes que emulan 512 bytes.
- Unidades híbridas.
- El sistema tiene cargadores de terceros.
- Unidades con directorios NTFS comprimidos.
- La tecnología Cifrado de disco de Kaspersky (FDE) no es compatible con otras tecnologías de cifrado de disco completo (como BitLocker, McAfee Drive Encryption y WinMagic SecureDoc).
- La tecnología Cifrado de disco de Kaspersky (FDE) no es compatible con la tecnología ExpressCache.
- No se admite la creación, eliminación y modificación de particiones en una unidad cifrada. Podría perder datos.
- No se permite formatear el sistema de archivos. Podría perder datos.

  Si necesita formatear una unidad que se cifró con la tecnología Cifrado de disco de Kaspersky (FDE), formatee la unidad en un equipo que no tenga Kaspersky Endpoint Security para Windows y use solo el cifrado de disco completo.

  Una unidad cifrada formateada con la opción de formato rápido puede identificarse erróneamente como cifrada la próxima vez que se conecte a un equipo que tenga instalado Kaspersky Endpoint Security para Windows. Los datos del usuario no estarán disponibles.
- El Agente de autenticación no admite más de 100 cuentas.
- La tecnología de inicio de sesión único no es compatible con otras tecnologías de desarrolladores externos.
- La tecnología Cifrado de disco de Kaspersky (FDE) no es compatible con los siguientes modelos de dispositivos:
  - Dell Latitude E6410 (modo UEFI)
  - HP Compaq nc8430 (modo Legacy BIOS)
  - Lenovo Think Center 8811 (modo Legacy BIOS)

- El Agente de autenticación no admite trabajar con tokens USB cuando Legacy USB Support está habilitado. Solo se podrá utilizar la autenticación basada en contraseña en el equipo.
- Al cifrar una unidad en modo Legacy BIOS, se recomienda habilitar Legacy USB Support en los siguientes modelos de dispositivos:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - PC microtorre de HP Compaq dx2450
  - Lenovo G550
  - Lenovo ThinkPad L530
  - Lenovo ThinkPad T510
  - Lenovo ThinkPad W540
  - Lenovo ThinkPad X121e
  - Lenovo ThinkPad X200s (74665YG)

- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (placa madre)

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

Kaspersky Endpoint Security utiliza el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard"). En Kaspersky Endpoint Security, la longitud de clave efectiva de este algoritmo puede ser de 256 bits o de 56 bits. El algoritmo de cifrado depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución. Están disponibles tanto una variante de cifrado "fuerte" *(AES256)* como una de cifrado "ligero" *(AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

La longitud de la clave de cifrado solo puede cambiarse en Kaspersky Endpoint Security 11.2.0 y versiones posteriores.

Para cambiar la longitud de la clave de cifrado, complete estos pasos:

1. Antes de cambiar la longitud de la clave de cifrado, descifre los objetos que Kaspersky Endpoint Security ya haya cifrado:
   a. Descifrar discos duros.
   b. Descifre los archivos almacenados en los discos locales.
   c. Descifre las unidades extraíbles.

   Una vez que cambie la longitud de la clave de cifrado, los objetos que permanezcan cifrados dejarán de estar disponibles.
2. Elimine Kaspersky Endpoint Security.
3. Instale Kaspersky Endpoint Security con un paquete de distribución de Kaspersky Endpoint Security que contenga una biblioteca de cifrado diferente.

Otra alternativa para realizar el cambio de longitud consiste en actualizar la aplicación. Para que el cambio pueda hacerse de este modo, se deben cumplir las siguientes condiciones:

- La versión de Kaspersky Endpoint Security instalada en el equipo debe ser la 10 Service Pack 2 o posterior.
- Los componentes de cifrado de datos (Cifrado de archivos, Cifrado de disco completo) no deben estar instalados en el equipo.

  De manera predeterminada, Kaspersky Endpoint Security no incluye los componentes de cifrado de datos. El componente Administración de BitLocker no afecta la capacidad de cambiar la longitud de la clave de cifrado.

Para cambiar la longitud de la clave de cifrado, ejecute los archivos kes_win.msi o setup_kes.exe del paquete de distribución que contenga la biblioteca de cifrado necesaria. Si necesita actualizar la aplicación en forma remota, utilice el paquete de instalación.

Para cambiar la longitud de la clave de cifrado utilizando un paquete de distribución correspondiente a la versión que ya está instalada en el equipo, primero deberá desinstalar la aplicación.

## Cifrado de Disco de Kaspersky

La tecnología Cifrado de disco de Kaspersky puede usarse únicamente en equipos con ediciones de Windows para estaciones de trabajo. En equipos que tengan una edición de Windows para servidores, deberá utilizar la tecnología Cifrado de unidad BitLocker.

La característica de cifrado de disco completo de Kaspersky Endpoint Security es compatible con los sistemas de archivos FAT32, NTFS y exFAT.

Antes de comenzar el cifrado de disco completo, la aplicación ejecuta una serie de verificaciones para determinar si el dispositivo puede cifrarse, lo que incluye la verificación del disco duro del sistema para detectar la compatibilidad con el Agente de autenticación o con los componentes de cifrado de BitLocker. Es necesario reiniciar el equipo para verificar la compatibilidad. Una vez reiniciado el equipo, la aplicación realiza todas las verificaciones necesarias de forma automática. Si el control de compatibilidad se realiza correctamente, el cifrado de disco completo se inicia después de que el sistema operativo y la aplicación se inician. Si se descubre que el disco duro del sistema es incompatible con el Agente de autenticación o con los componentes de cifrado de BitLocker, se deberá reiniciar el equipo presionando el botón físico para Restablecer. Kaspersky Endpoint Security lleva un registro de la información sobre la incompatibilidad. Sobre la base de esta información, la aplicación no inicia la tarea de cifrado de disco completo al inicio del sistema operativo. La información sobre este evento se mantiene en los informes de Kaspersky Security Center.

Si se cambia la configuración de hardware del equipo, se debe eliminar la información sobre incompatibilidad registrada por la aplicación durante la verificación anterior, a fin de verificar la compatibilidad del disco duro del sistema con el Agente de autenticación y con los componentes de cifrado de BitLocker. Para hacerlo, antes del cifrado de disco completo, ingrese `avp pbatestreset` en la línea de comandos. Si el sistema operativo no logra cargarse luego de verificar la compatibilidad del disco duro del sistema con el Agente de autenticación, deberá eliminar los objetos y los datos restantes luego de la operación de prueba del Agente de autenticación; para ello, emplee la Utilidad de Restauración y, luego, inicie Kaspersky Endpoint Security y vuelva a ejecutar el comando `avp pbatestreset`.

Una vez iniciado el cifrado de disco completo, Kaspersky Endpoint Security cifra todos los datos que se escriben en los discos duros.

Si el usuario apaga o reinicia el equipo durante la tarea de cifrado de disco completo, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo.

Si el sistema operativo cambia al modo de hibernación durante el cifrado de disco completo, el Agente de autenticación se carga cuando el sistema operativo sale del modo de hibernación. Kaspersky Endpoint Security reanuda el cifrado de disco completo después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el cifrado de disco completo, Kaspersky Endpoint Security reanuda el cifrado de disco completo cuando el sistema operativo sale del modo de suspensión sin cargar el Agente de autenticación.

La autenticación de usuarios en el Agente de autenticación se puede realizar de dos formas:

- Ingrese el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red LAN que está utilizando las herramientas de Kaspersky Security Center.
- Ingrese la contraseña de un token o tarjeta inteligente conectados al equipo.

  El uso de un token o de una tarjeta inteligente está disponible solo si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, se rechazará la adición del archivo de certificado electrónico al comando.

El agente de autenticación es compatible con la disposición de teclado para los siguientes idiomas:

- Inglés (Reino Unido)
- Inglés (Estados Unidos)
- Árabe (Argelia, Marruecos, Túnez; disposición AZERTY)
- Español (América Latina)
- Italiano
- Alemán (Alemania y Austria)
- Alemán (Suiza)
- Portugués (Brasil, disposición ABNT2)
- Ruso (para teclados IBM/Windows de 105 teclas con disposición QWERTY)
- Turco (disposición QWERTY)
- Francés (Francia)
- Francés (Suiza)
- Francés (Bélgica; disposición AZERTY)
- Japonés (para teclados de 106 teclas con disposición QWERTY)

Una disposición de teclado se vuelve disponible en el Agente de autenticación si se la ha agregado en la configuración de idioma y regional del sistema operativo y se ha vuelto disponible en la pantalla de bienvenida de Microsoft Windows.

Si el nombre de la cuenta del Agente de autenticación contiene símbolos que no se pueden introducir con las distribuciones de teclado disponibles en el Agente de autenticación, deberá realizar uno de dos procedimientos para poder acceder a los discos duros cifrados: realizar una restauración con la Utilidad de restauración, o restablecer el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

## Características especiales del cifrado de unidades SSD

La aplicación admite el cifrado de unidades SSD, unidades SSHD híbridas y unidades con la función Intel Smart Response. La aplicación no admite el cifrado de unidades con la función Intel Rapid Start. Desactive la función Intel Rapid Start antes de cifrar dicha unidad.

El cifrado de unidades SSD tiene las siguientes características especiales:

- Si una unidad SSD es nueva y no contiene datos confidenciales, habilite el cifrado solo del espacio ocupado. Esto le permite sobrescribir los sectores de la unidad correspondiente.
- Si una unidad SSD está en uso y tiene datos confidenciales, seleccione una de las siguientes opciones:
  - Limpie completamente la unidad SSD (Borrado seguro), instale el sistema operativo y ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado habilitada.
  - Ejecute el cifrado de la unidad SSD con la opción de cifrar solo el espacio ocupado deshabilitada.

El cifrado de una unidad SSD requiere entre 5 y 10 GB de espacio libre. Los requisitos de espacio libre para almacenar datos de administración de cifrado se proporcionan en la siguiente tabla.

Requisitos de espacio libre para almacenar datos de administración de cifrado

| Tamaño de la unidad SSD (GB) | Espacio libre en la partición principal de la unidad SSD (MB) | Espacio libre en la partición secundaria de la unidad SSD (MB) |
|---|---|---|
| 128 | 250 | 64 |
| 256 | 250 | 640 |
| 512 | 300 | 128 |

## Cifrado de disco completo con tecnología de Cifrado de Disco de Kaspersky

Antes de cifrar un disco completo, recomendamos verificar que el equipo no esté infectado. Para hacerlo, inicie la tarea de Análisis completo o la de Análisis de áreas críticas. La realización del cifrado de disco completo en un equipo que está infectado con un rootkit puede hacer que el equipo se vuelva inoperable.

*Para realizar el cifrado de disco completo con tecnología de Cifrado de Disco de Kaspersky, realice lo siguiente:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 de Cifrado de disco de Kaspersky no se puede utilizar si el equipo tiene discos duros que fueron cifrados con 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 dichos discos duros.

8. Configure reglas que permitan agregar cuentas del Agente de autenticación como parte del cifrado de disco. Los usuarios emplean el Agente de autenticación para identificarse, obtener acceso a las unidades cifradas de sus equipos y cargar el sistema operativo. Para que las cuentas del Agente de autenticación se agreguen automáticamente, configure los siguientes ajustes:

   - **Durante el cifrado, crear cuentas del Agente de autenticación automáticamente para los usuarios de Windows**. Cuando esta casilla está activada, la aplicación crea cuentas del Agente de autenticación para las cuentas de usuario de Windows disponibles en el equipo. De manera predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario haya iniciado sesión en el sistema operativo en los treinta días anteriores.

   - **Crear cuentas del Agente de autenticación automáticamente para todos los usuarios de este equipo cuando inicien sesión**. Cuando se activa esta casilla, antes de que el Agente de autenticación se inicie, la aplicación analiza las cuentas de Windows que se han creado en el equipo. Si detecta que una cuenta de Windows no tiene su correspondiente cuenta para el Agente de autenticación, crea esa cuenta para que el usuario pueda acceder a las unidades cifradas de su equipo. La nueva cuenta del Agente de autenticación tendrá las siguientes opciones por defecto: inicio de sesión con contraseña únicamente y cambio de contraseña obligatorio tras el primer inicio de sesión. Gracias a esta función, ya no necesitará agregar cuentas del Agente de autenticación manualmente con la tarea *Administrar cuentas del Agente de autenticación* para los equipos que ya tengan sus unidades cifradas.

   Si deshabilitó la creación automática de cuentas del Agente de autenticación, puede agregarlas manualmente con la tarea *Administrar cuentas*. Use también esta tarea para realizar cambios de configuración en alguna cuenta del Agente de autenticación que se haya creado automáticamente.

9. Cuando alguien se identifica por primera vez, el Agente de autenticación puede recordar su nombre de usuario para que, cuando esa persona quiera iniciar sesión nuevamente, solamente necesite escribir su contraseña. Si desea habilitar esta característica, active la casilla **Guardar el nombre de usuario utilizado en el Agente de autenticación**.

10. Seleccione uno de los siguientes métodos de cifrado:

    - Si quiere aplicar el cifrado solo a los sectores de los discos duros que estén ocupados por archivos, seleccione la casilla **Solo cifrar el espacio de disco usado**.

      Si está aplicando el cifrado a un disco que ya está en uso, le recomendamos que cifre todo el disco. De esta manera, se asegurará de que toda la información —incluida la información eliminada, que podría contener datos recuperables— esté protegida. Se recomienda usar la función **Solo cifrar el espacio de disco usado** en el caso de discos nuevos sin uso previo.

    - Si quiere aplicar el cifrado al disco duro completo, desmarque la casilla **Solo cifrar el espacio de disco usado**.

Si un dispositivo ya se cifró con la función **Solo cifrar el espacio de disco usado**, después de aplicar una directiva en el modo **Cifrar todos los discos duros**, no se cifrarán los sectores no ocupados por archivos.

11. Si se presentan problemas de compatibilidad con el hardware al cifrar el equipo, puede seleccionar la casilla **Usar Legacy USB Support**.

    *Legacy USB Support* es una función de la BIOS o UEFI que permite utilizar dispositivos USB (por ejemplo, tokens de seguridad) durante el arranque del equipo, en la etapa anterior al inicio del sistema operativo (modo BIOS). La función Legacy USB Support no afecta la capacidad de usar dispositivos USB una vez que el sistema operativo se ha iniciado.

    Si habilita la función Legacy USB Support y el Agente de autenticación se ha instalado en modo BIOS, no podrá usar tokens USB. Se recomienda usar esta opción solo cuando hay un problema de compatibilidad del hardware y solo para esos equipos en los cuales el problema ocurrió.

12. Guarde los cambios.

Si desea monitorear el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.

Si los discos duros del sistema están cifrados, se carga el Agente de autenticación antes del inicio del sistema operativo. Utilice el Agente de autenticación para completar el proceso de autenticación a fin de obtener acceso a los discos duros cifrados del sistema y cargar el sistema operativo. Después de la finalización correcta del procedimiento de autenticación, se carga el sistema operativo. El proceso de autenticación se repite cada vez que se reinicia el sistema operativo.

## Creación de una lista de discos duros excluidos del cifrado

Puede crear una lista de exclusiones del cifrado solo para la tecnología de Cifrado de disco de Kaspersky.

*Para elaborar una lista de discos duros excluidos del cifrado:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 disco de Kaspersky**.

   Las entradas correspondientes a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**. Esta tabla está vacía si no elaboró previamente una lista de discos duros excluidos del cifrado.
7. Para agregar discos duros a la lista de discos duros excluidos del cifrado:

a. Haga clic en el botón **Agregar**.

Se abre la ventana **Agregar dispositivos de la lista de Kaspersky Security Center**.

b. En la ventana **Agregar dispositivos de la lista de Kaspersky Security Center**, especifique los valores de los siguientes parámetros: **Nombre**, **Equipo**, **Tipo de disco** o **Cifrado de disco de Kaspersky**.

c. Haga clic en el botón **Actualizar**.

d. En la columna **Nombre**, seleccione las casillas de las filas de la tabla que correspondan a los discos duros que quiera agregar a la lista de discos duros excluidos del cifrado.

e. Haga clic en **Aceptar**.

Los discos duros seleccionados aparecen en la tabla **No cifrar los siguientes discos duros**.

8. Si desea quitar uno o varios de los discos incluidos en la tabla de exclusiones, seleccione la o las filas correspondientes en la tabla **No cifrar los siguientes discos duros** y haga clic en el botón **Eliminar**.

Para seleccionar más de una fila a la vez, mantenga presionada la tecla **CTRL** mientras indica su selección.

9. Guarde los cambios.

## Exportar e importar una lista de discos duros excluidos del cifrado

Puede exportar la lista de exclusiones de cifrado del disco duro a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de exclusiones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar las exclusiones a otro servidor.

Cómo exportar e importar una lista de exclusiones de cifrado de disco duro a la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 disco de Kaspersky**.

   Las entradas correspondientes 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 vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
9. Guarde los cambios.

[Cómo exportar e importar una lista de exclusiones de cifrado de disco duro a Web Console]

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desea importar o exportar una lista de exclusiones.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Cifrado de datos** → **Cifrado de disco completo**.
5. Seleccione la tecnología **Cifrado de disco de Kaspersky** y haga clic en el vínculo para configurar los ajustes.

   Se muestran los ajustes de cifrado.
6. Haga clic en el vínculo **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 bien exporte la lista completa de exclusiones.
   d. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   e. Haga clic en el botón **Guardar**.

      Kaspersky Endpoint Security exportará la lista de exclusiones completa 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 que se usará para importar la lista de exclusiones.
   c. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
9. Guarde los cambios.

## Habilitación de la tecnología de inicio de sesión único (SSO)

La tecnología de inicio de sesión único (SSO) permite iniciar sesión en el sistema operativo automáticamente utilizando las credenciales del Agente de autenticación.

Si opta por usar la tecnología SSO, el Agente de autenticación no tendrá en cuenta los requisitos que puedan haberse definido en Kaspersky Security Center para controlar la seguridad de las contraseñas. Para controlar la seguridad de las contraseñas, utilice las opciones del sistema operativo.

La tecnología de inicio de sesión único no es compatible con proveedores externos de credenciales de cuentas.

Cómo habilitar el uso de la tecnología SSO en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 contraseñas**, haga clic en el botón **Configuración**.
7. En la ventana que se abre, en la ficha **Agente de autenticación**, active la casilla **Usar tecnología de inicio de sesión único (SSO)**.
8. Guarde los cambios.

Como resultado, el usuario necesitará autenticarse una sola vez, a través del Agente. No será necesario que complete el procedimiento de autenticación para que el sistema operativo se cargue. El sistema operativo se cargará automáticamente.

Cómo habilitar el uso de la tecnología SSO 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 correspondiente a los equipos en los que desee habilitar el inicio de sesión único.

   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 haga clic en el vínculo para configurar los ajustes.

   Se muestran los ajustes de cifrado.
6. En la sección **Configuración de contraseñas**, active la casilla **Usar tecnología de inicio de sesión único (SSO)**.
7. Haga clic en **Aceptar**.

Como resultado, el usuario necesitará autenticarse una sola vez, a través del Agente. No será necesario que complete el procedimiento de autenticación para que el sistema operativo se cargue. El sistema operativo se cargará automáticamente.

Para poder utilizar la tecnología SSO, la contraseña de la cuenta de Windows debe ser la misma que la contraseña de la cuenta del Agente de autenticación. Si las contraseñas no son las mismas, el usuario deberá autenticarse dos veces: una vez en la interfaz del Agente de autenticación, y una segunda vez antes de que se cargue el sistema operativo. Tras ello, Kaspersky Endpoint Security reemplazará la contraseña de la cuenta del Agente de autenticación por la contraseña de la cuenta de Windows.

## Administración de cuentas del Agente de autenticación

El Agente de autenticación es un componente necesario para operar con unidades que se han protegido con la tecnología Cifrado de disco de Kaspersky (FDE). El usuario debe autenticarse con el Agente antes de que se cargue el sistema operativo. Para configurar los ajustes de autenticación de los usuarios, utilice la tarea *Administrar cuentas del Agente de autenticación*. Puede optar por usar tareas locales para equipos específicos o tareas de grupo para selecciones de equipos o equipos que pertenezcan a diferentes grupos de administración.

La ejecución de la tarea *Administrar cuentas del Agente de autenticación* no puede programarse. Tampoco es posible detener esta tarea a la fuerza.

Cómo crear la tarea Administrar cuentas del Agente de autenticación en la Consola de administración (MMC)

1. En 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**.

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

### Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Endpoint Security para Windows (11.6.0)** → **Administrar cuentas del Agente de autenticación**.

### Paso 2. Selección del comando para administrar las cuentas del Agente de autenticación

Genere una lista de comandos para administrar las cuentas del Agente de autenticación. Los comandos de administración le permitirán agregar, modificar y eliminar cuentas (consulte las instrucciones más abajo). Solo los usuarios que tengan una cuenta del Agente de autenticación podrán completar el procedimiento de autenticación, cargar el sistema operativo y acceder a la unidad cifrada.

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

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

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

### Paso 4. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo `Cuentas de administrador`.

### Paso 5. Completar creación de la tarea

Salga del Asistente. De ser necesario, active la casilla **Ejecutar la tarea al finalizar el Asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Como resultado, la tarea se completará cuando el equipo vuelva a iniciarse y el nuevo usuario podrá autenticarse, cargar el sistema operativo y acceder a la unidad cifrada.

[Cómo crear la tarea Administrar cuentas del Agente de autenticación en Web Console]

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

   Se abre la lista de tareas.

2. Haga clic en el botón **Agregar**.

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

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

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security para Windows (11.6.0)**.
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 **Seleccione los dispositivos a los que se asignará la tarea**, elija el alcance de la tarea.

### Paso 2. Administración de cuentas del Agente de autenticación

Genere una lista de comandos para administrar las cuentas del Agente de autenticación. Los comandos de administración le permitirán agregar, modificar y eliminar cuentas (consulte las instrucciones más abajo). Solo los usuarios que tengan una cuenta del Agente de autenticación podrán completar el procedimiento de autenticación, cargar el sistema operativo y acceder a la unidad cifrada.

### Paso 3. Completar creación de la tarea

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, la tarea se completará cuando el equipo vuelva a iniciarse y el nuevo usuario podrá autenticarse, cargar el sistema operativo y acceder a la unidad cifrada.

Para agregar una cuenta del Agente de autenticación, deberá agregar un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Recomendamos utilizar una tarea de grupo si, por ejemplo, desea agregar una cuenta de administración en todos los equipos.

Kaspersky Endpoint Security permite crear las cuentas del Agente de autenticación automáticamente antes de que se cifre una unidad. La opción para que las cuentas del Agente de autenticación se creen de forma automática puede habilitarse en la configuración de la directiva de cifrado de disco completo. También es posible usar la tecnología de inicio de sesión único (SSO).

**Cómo agregar una cuenta del Agente de autenticación mediante la Consola de administración (MMC)**

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de la tarea, vaya a la sección **Opciones**.
3. Haga clic en **Agregar** → **Comando de adición de cuenta**.
4. En la ventana que se abre, en el campo **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows que se usará para crear la cuenta del Agente de autenticación.
5. Si escribió el nombre de la cuenta de Windows manualmente, haga clic en el botón **Permitir** para que se determine el identificador de seguridad (SID) de la cuenta.

   Si opta por no determinar el identificador de seguridad (SID) haciendo clic en el botón **Permitir**, el SID será determinado al momento de ejecutar la tarea en el equipo.

   > Determinar el identificador de seguridad de una cuenta de Windows tiene la finalidad de verificar que el nombre de la cuenta se haya escrito correctamente. Si la cuenta de Windows no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con un error.

6. Seleccione la casilla **Reemplazar cuenta existente** para que la cuenta que se cree tenga un nombre idéntico al nombre de cuenta del Agente de autenticación previamente creada que se reemplaza.

   > Este paso está disponible cuando se agrega un comando de creación de cuenta del Agente de autenticación en las propiedades de una tarea de grupo para administrar cuentas del Agente de autenticación. Este paso no está disponible si agrega un comando para crear la cuenta del Agente de autenticación en las propiedades de la tarea local **Cifrado de disco completo, administración de cuentas**.

7. En el campo **Nombre de usuario**, escriba el nombre de la cuenta del Agente de autenticación que se debe ingresar durante la autenticación para poder acceder a discos duros cifrados.
8. Seleccione la casilla **Permitir autenticación basada en contraseña** si desea que la aplicación le solicite al usuario ingresar la contraseña de la cuenta del Agente de autenticación durante la autenticación para poder acceder a discos duros cifrados. Defina una contraseña para la cuenta del Agente de autenticación. Si lo considera necesario, puede exigir que el usuario cambie la contraseña la primera vez que se autentique.
9. Seleccione la casilla **Permitir la autenticación basada en certificado** si desea que la aplicación le solicite al usuario que conecte un token o una tarjeta inteligente al equipo durante la autenticación para poder acceder a discos duros cifrados. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token.
10. Si es necesario, en el campo **Descripción de comando**, ingrese los detalles de la cuenta del Agente de autenticación que necesita para administrar el comando.
11. Realice una de las siguientes acciones:

    - Seleccione la opción **Permitir autenticación** si desea que la aplicación permita que el usuario trabaje con la cuenta especificada en el comando para acceder al cuadro de diálogo de autenticación en el Agente de autenticación.

- Seleccione la opción **Bloquear autenticación** si desea que la aplicación no permita que el usuario trabaje con la cuenta especificada en el comando para acceder al cuadro de diálogo de autenticación en el Agente de autenticación.

12. Guarde los cambios.

[Cómo agregar 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 de propiedades de la tarea.

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

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Agregar**.

   Se abre un asistente para administrar las cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Agregar cuenta**.

6. Seleccione una cuenta de usuario. Puede escribir el nombre de la cuenta manualmente o elegir una de las disponibles en la lista de cuentas de dominio. Haga clic en **Siguiente**.

   Kaspersky Endpoint Security determinará el identificador de seguridad (SID) de la cuenta. Esto se hace para verificar que la cuenta se haya especificado correctamente. Si se cometió un error al escribir el nombre de usuario, Kaspersky Endpoint Security finalizará la tarea con un error.

7. Configure los ajustes de la cuenta del Agente de autenticación.

   - **Crear una nueva cuenta del Agente de autenticación para reemplazar la existente**. Kaspersky Endpoint Security hará un relevamiento de las cuentas del equipo. Si el id. de seguridad del usuario en el equipo coincide con el de la tarea, Kaspersky Endpoint Security modificará la configuración de la cuenta de usuario como lo indique la tarea.

   - **Nombre de usuario**. En una cuenta del Agente de autenticación, el nombre de usuario predeterminado se corresponde con el nombre del usuario en el dominio.

   - **Permitir la autenticación por contraseña**. Defina una contraseña para la cuenta del Agente de autenticación. Si lo considera necesario, puede exigir que el usuario cambie la contraseña la primera vez que se autentique. De este modo, cada usuario tendrá su propia contraseña. Si desea definir requisitos de seguridad para la contraseña de la cuenta del Agente de autenticación, puede hacerlo en la directiva.

   - **Permitir la autenticación por certificado**. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token. De este modo, el usuario no necesitará introducir la contraseña para usar su tarjeta inteligente o token.

   - **Acceso de la cuenta a los datos cifrados**. Configure las opciones que regularán el acceso del usuario a la unidad cifrada. Puede, por ejemplo, impedir temporalmente que un usuario se autentique en lugar de eliminar su cuenta del Agente de autenticación.

   - **Comentario**. Escriba una descripción para la cuenta, de ser necesario.

8. Guarde los cambios.

9. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Como resultado, la tarea se completará cuando el equipo vuelva a iniciarse y el nuevo usuario podrá autenticarse, cargar el sistema operativo y acceder a la unidad cifrada.

Para modificar la contraseña u otros datos de configuración de una cuenta del Agente de autenticación, deberá agregar un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Recomendamos utilizar una tarea de grupo si, por ejemplo, necesita reemplazar el certificado del token del administrador en todos los equipos.

**Cómo modificar una cuenta del Agente de autenticación mediante la Consola de administración (MMC)**

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de la tarea, vaya a la sección **Opciones**.
3. Haga clic en **Agregar** → **Comando de modificación de cuenta**.
4. En el campo **Cuenta de Windows** de la ventana que se abre, especifique el nombre de la cuenta de Microsoft Windows que desee modificar.
5. Si escribió el nombre de la cuenta de Windows manualmente, haga clic en el botón **Permitir** para que se determine el identificador de seguridad (SID) de la cuenta.

   Si opta por no determinar el identificador de seguridad (SID) haciendo clic en el botón **Permitir**, el SID será determinado al momento de ejecutar la tarea en el equipo.

   > Determinar el identificador de seguridad de una cuenta de Windows tiene la finalidad de verificar que el nombre de la cuenta se haya escrito correctamente. Si la cuenta de Windows no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con un error.

6. Seleccione la casilla **Cambiar nombre de usuario** e ingrese un nuevo nombre para la cuenta del Agente de autenticación si desea que Kaspersky Endpoint Security cambie el nombre de usuario para todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo nombre figura en el campo **Cuenta de Windows** por el nombre que se ingrese en el campo a continuación.
7. Seleccione la casilla **Modificar la configuración de la autenticación por contraseña** para hacer modificables las configuraciones de autenticación basada en contraseña.
8. Seleccione la casilla **Permitir autenticación basada en contraseña** si desea que la aplicación le solicite al usuario ingresar la contraseña de la cuenta del Agente de autenticación durante la autenticación para poder acceder a discos duros cifrados. Defina una contraseña para la cuenta del Agente de autenticación.
9. Seleccione la casilla **Modificar la regla de cambio de contraseña al autenticarse en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie el valor de la configuración de cambio de contraseña correspondiente a todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo el nombre se indica en el campo **Cuenta de Windows** por el valor de configuración que se especifica a continuación.
10. Especifique el valor de la configuración de cambio de contraseña al autenticarse en el Agente de autenticación.
11. Seleccione la casilla **Modificar la configuración de la autenticación por certificado** para hacer modificables las configuraciones de autenticación basadas en un certificado electrónico de un dispositivo o tarjeta inteligente.
12. Seleccione la casilla **Permitir la autenticación basada en certificado** si desea que la aplicación le solicite al usuario ingresar la contraseña del token o la tarjeta inteligente conectados al equipo durante el proceso de autenticación a fin de obtener acceso a discos duros cifrados. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token.
13. Seleccione la casilla **Modificar descripción de comando** y modifique la descripción del comando si desea que Kaspersky Endpoint Security cambie la descripción del comando correspondiente a todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo nombre se indica en el campo **Cuenta de Windows**.

14. Seleccione la casilla **Modificar la regla de acceso a la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie la regla de acceso de usuarios al cuadro de diálogo de autenticación en el Agente de autenticación por el valor especificado a continuación para todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows cuyo nombre se indica en el campo **Cuenta de Windows**.

15. Especifique la regla para acceder al cuadro de diálogo de autenticación en el Agente de autenticación.

16. Guarde los cambios.

Cómo modificar una cuenta del Agente de autenticación mediante Web Console

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

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

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Agregar**.

   Se abre un asistente para administrar las cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Modificar cuenta**.

6. Seleccione una cuenta de usuario. Puede escribir el nombre de la cuenta manualmente o elegir una de las disponibles en la lista de cuentas de dominio. Haga clic en **Siguiente**.

   Kaspersky Endpoint Security determinará el identificador de seguridad (SID) de la cuenta. Esto se hace para verificar que la cuenta se haya especificado correctamente. Si se cometió un error al escribir el nombre de usuario, Kaspersky Endpoint Security finalizará la tarea con un error.

7. Active las casillas ubicadas junto a los parámetros que desee modificar.

8. Configure los ajustes de la cuenta del Agente de autenticación.

   - **Crear una nueva cuenta del Agente de autenticación para reemplazar la existente**. Kaspersky Endpoint Security hará un relevamiento de las cuentas del equipo. Si el id. de seguridad del usuario en el equipo coincide con el de la tarea, Kaspersky Endpoint Security modificará la configuración de la cuenta de usuario como lo indique la tarea.

   - **Nombre de usuario**. En una cuenta del Agente de autenticación, el nombre de usuario predeterminado se corresponde con el nombre del usuario en el dominio.

   - **Permitir la autenticación por contraseña**. Defina una contraseña para la cuenta del Agente de autenticación. Si lo considera necesario, puede exigir que el usuario cambie la contraseña la primera vez que se autentique. De este modo, cada usuario tendrá su propia contraseña. Si desea definir requisitos de seguridad para la contraseña de la cuenta del Agente de autenticación, puede hacerlo en la directiva.

   - **Permitir la autenticación por certificado**. Seleccione el archivo del certificado que se usará para la autenticación con la tarjeta inteligente o el token. De este modo, el usuario no necesitará introducir la contraseña para usar su tarjeta inteligente o token.

   - **Acceso de la cuenta a los datos cifrados**. Configure las opciones que regularán el acceso del usuario a la unidad cifrada. Puede, por ejemplo, impedir temporalmente que un usuario se autentique en lugar de eliminar su cuenta del Agente de autenticación.

   - **Comentario**. Escriba una descripción para la cuenta, de ser necesario.

9. Guarde los cambios.

10. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Para eliminar una cuenta del Agente de autenticación, deberá agregar un comando especial a la tarea *Administrar cuentas del Agente de autenticación*. Recomendamos utilizar una tarea de grupo si, por ejemplo, necesita eliminar la cuenta de un empleado que ha renunciado.

**Cómo eliminar una cuenta del Agente de autenticación mediante la Consola de administración (MMC)**

1. Abra las propiedades de la tarea *Administrar cuentas del Agente de autenticación*.
2. En las propiedades de la tarea, vaya a la sección **Opciones**.
3. Haga clic en **Agregar** → **Comando de eliminación de cuenta**.
4. En el campo **Cuenta de Windows** de la ventana que se abre, especifique el nombre de la cuenta de usuario de Microsoft Windows que se haya utilizado para crear la cuenta del Agente de autenticación que va a eliminar.
5. Si escribió el nombre de la cuenta de Windows manualmente, haga clic en el botón **Permitir** para que se determine el identificador de seguridad (SID) de la cuenta.

   Si opta por no determinar el identificador de seguridad (SID) haciendo clic en el botón **Permitir**, el SID será determinado al momento de ejecutar la tarea en el equipo.

   > Determinar el identificador de seguridad de una cuenta de Windows tiene la finalidad de verificar que el nombre de la cuenta se haya escrito correctamente. Si la cuenta de Windows no existe en el equipo o en el dominio de confianza, la tarea *Administrar cuentas del Agente de autenticación* finalizará con un error.

6. Guarde los cambios.

**Cómo eliminar una cuenta del Agente de autenticación mediante Web Console**

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

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

4. En la lista de cuentas del Agente de autenticación, haga clic en el botón **Agregar**.

   Se abre un asistente para administrar las cuentas del Agente de autenticación.

5. Seleccione el tipo de comando **Eliminar cuenta**.

6. Seleccione una cuenta de usuario. Puede escribir el nombre de la cuenta manualmente o elegir una de las disponibles en la lista de cuentas de dominio.

7. Guarde los cambios.

8. Active la casilla ubicada junto a la tarea y haga clic en el botón **Iniciar**.

Como resultado, la tarea se completará cuando el equipo vuelva a iniciarse y el usuario no podrá autenticarse ni cargar el sistema operativo. Kaspersky Endpoint Security no permitirá que el usuario acceda a la información cifrada.

Para ver una lista de usuarios que pueden autenticarse con el Agente y cargar el sistema operativo, debe consultar las propiedades del equipo administrado.

Cómo ver la lista de cuentas del Agente de autenticación mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.

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

4. Haga doble clic en un equipo para abrir su ventana de propiedades.

5. En la ventana de propiedades del equipo, elija la sección **Tareas**.

   Se abre la lista de tareas locales.

6. Seleccione la tarea **Administrar cuentas del Agente de autenticación**.

7. En las propiedades de la tarea, vaya a la sección **Opciones**.

Como resultado, obtendrá acceso a la lista de cuentas del Agente de autenticación presentes en el equipo. Solo los usuarios que figuren en esa lista podrán autenticarse con el Agente y cargar el sistema operativo.

Cómo ver la lista de cuentas del Agente de autenticación mediante Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del equipo vinculado a las cuentas del Agente de autenticación en las que esté interesado.

   Se abren las propiedades del equipo.
3. En la ventana de propiedades del equipo, elija la sección **Tareas**.

   Se abre la lista de tareas locales.
4. Seleccione la tarea **Administrar cuentas del Agente de autenticación**.
5. En las propiedades de la tarea, seleccione la ficha **Configuración de la aplicación**.

Como resultado, obtendrá acceso a la lista de cuentas del Agente de autenticación presentes en el equipo. Solo los usuarios que figuren en esa lista podrán autenticarse con el Agente y cargar el sistema operativo.

## Uso de un token y de una tarjeta inteligente con el Agente de autenticación

Se puede utilizar un token o una tarjeta inteligente para la autenticación cuando se está accediendo a discos duros cifrados. Para utilizar este método, es necesario agregar el archivo del certificado electrónico del token o tarjeta inteligente a la tarea *Administrar cuentas del Agente de autenticación*.

El uso de un token o de una tarjeta inteligente está disponible solo si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, se rechazará la adición del archivo de certificado electrónico al comando.

Kaspersky Endpoint Security es compatible con los siguientes dispositivos, lectores de tarjetas inteligentes y tarjetas inteligentes:

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K Java
- SafeNet eToken 4100-72K (Java)
- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 7300
- EMC RSA SID 800
- Gemalto IDPrime.NET 510
- Gemalto IDPrime.NET 511
- Rutoken ECP

- Rutoken ECP Flash
- Aladdin-RD JaCarta PKI
- Athena IDProtect Laser
- SafeNet eToken PRO 72K Java
- Aladdin-RD JaCarta PKI

Para agregar el archivo de certificado electrónico de un token o de una tarjeta inteligente al comando para crear una cuenta del Agente de autenticación, primero deberá exportar el archivo con software de otros proveedores para la administración de certificados, y guardar el archivo.

El certificado del token o de la tarjeta inteligente debe tener las siguientes propiedades:

- El certificado debe cumplir con el estándar X.509, y el archivo del certificado debe tener el cifrado DER.
- El certificado contiene una clave RSA con una longitud de al menos 1024 bits.

Si el certificado electrónico del token o de la tarjeta inteligente no cumple con estos requisitos, el archivo del certificado no podrá incluirse en el comando con el que se crean las cuentas del Agente de autenticación.

El parámetro `KeyUsage` del certificado debe tener los valores `keyEncipherment` o `dataEncipherment`. El parámetro `KeyUsage` determina la finalidad del certificado. Si el parámetro tiene cualquier otro valor, Kaspersky Security Center descargará el archivo del certificado, pero mostrará una advertencia.

Si un usuario pierde su tarjeta inteligente o token, el administrador deberá agregar el archivo del certificado electrónico de una tarjeta inteligente o token de reemplazo al comando que se utiliza para crear las cuentas del Agente de autenticación. A continuación, el usuario debe completar el procedimiento de recibir acceso a dispositivos cifrados o restaurar datos en los dispositivos cifrados.

## Descifrado de discos duros

Puede descifrar discos duros aun si no hay licencia 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 cual 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** si quiere descifrar todos los discos duros cifrados.
- Agregue los discos duros cifrados que quiera descifrar a la tabla **No cifrar los siguientes discos duros**.

  Esta opción solo está disponible para la tecnología de Cifrado de disco de Kaspersky.

8. Guarde los cambios.

Si desea monitorear el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.

Si el usuario apaga o reinicia el equipo durante el descifrado del disco duro cifrado con tecnología de Cifrado de disco de Kaspersky, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el descifrado de discos duros después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo.

Si el sistema operativo pasa al modo de hibernación mientas se están descifrando discos duros cifrados con tecnología de Cifrado de disco de Kaspersky, el Agente de autenticación se carga cuando el sistema operativo sale del modo de hibernación. Kaspersky Endpoint Security reanuda el descifrado de discos duros después de la autenticación correcta en el agente de autenticación y el inicio del sistema operativo. Después del descifrado de discos duros, el modo de hibernación no está disponible hasta el primer reinicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el descifrado de discos duros, Kaspersky Endpoint Security reanuda el descifrado cuando el sistema operativo sale del modo de suspensión sin cargar el Agente de autenticación.

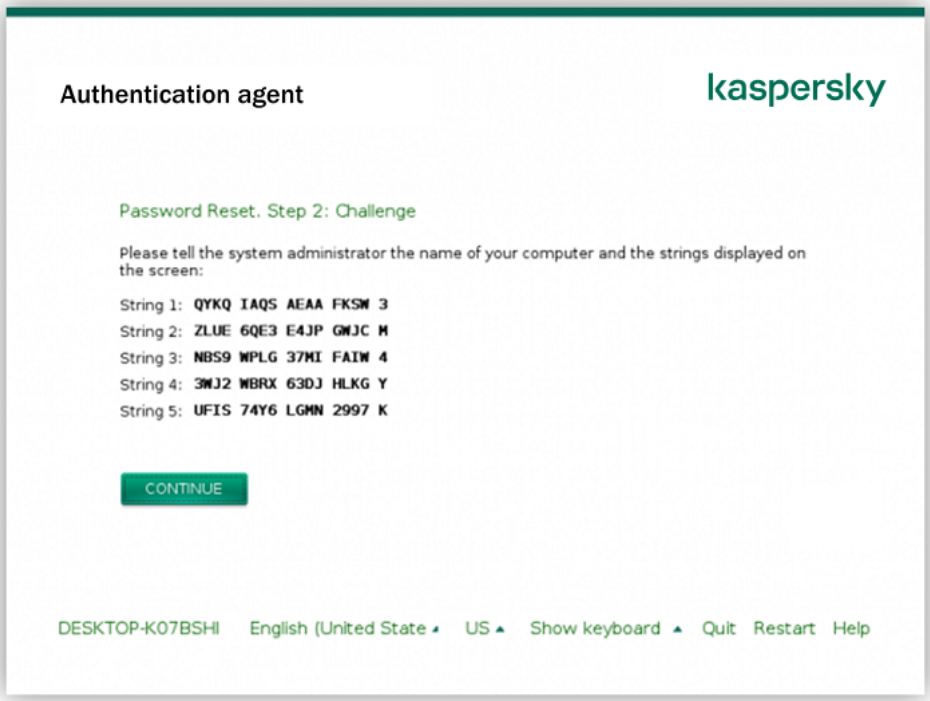
## Restaurar el acceso a una unidad protegida con la tecnología Cifrado de disco de Kaspersky

Si un usuario olvida la contraseña que le permite acceder a un disco duro protegido con la tecnología de Cifrado de disco de Kaspersky, debe iniciar el procedimiento de recuperación (un procedimiento de solicitud y respuesta).

### Restaurar el acceso al disco duro del sistema

El siguiente es el procedimiento para restaurar el acceso a un disco duro del sistema que se ha protegido con la tecnología de Cifrado de disco de Kaspersky:

1. El usuario le indica al administrador cuáles son los bloques de su solicitud (vea la imagen de más abajo).
2. El administrador introduce los bloques de la solicitud en Kaspersky Security Center, obtiene los bloques de respuesta y se los comunica al usuario.
3. El usuario escribe los bloques de la respuesta en la interfaz del Agente de autenticación y obtiene acceso al disco duro.




Restaurar el acceso a un disco duro del sistema protegido con Cifrado de disco de Kaspersky

Para iniciar el procedimiento de recuperación, el usuario debe hacer clic en el vínculo **Olvidé la contraseña** que se muestra en la interfaz del Agente de autenticación.

Cómo obtener, mediante la Consola de administración (MMC), los bloques de respuesta para un disco duro del sistema protegido con Cifrado de disco de Kaspersky

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione el elemento **Otorgar acceso en el modo fuera de línea**.
6. En la ventana que se abre, seleccione la ficha **Agente de autenticación**.
7. En la sección **Algoritmo de cifrado en uso**, seleccione un algoritmo de cifrado: **AES56** o **AES256**.

   El algoritmo de cifrado depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución. Están disponibles tanto una variante de cifrado "fuerte" *(AES256)* como una de cifrado "ligero" *(AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.
8. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación creada para el usuario que necesita acceder al disco.
9. En la lista desplegable **Disco duro**, seleccione el disco duro cifrado para el cual tiene que recuperar el acceso.
10. En la sección **Solicitud del usuario**, complete los bloques de solicitud según lo indica el usuario.

    Como resultado, en el campo **Clave de acceso** se mostrarán los bloques generados en respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de su cuenta del Agente de autenticación. Indíquele al usuario el contenido de estos bloques.

[Cómo obtener, mediante Web Console, los bloques de respuesta para un disco duro del sistema protegido con Cifrado de disco de Kaspersky](#)

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentre la unidad a la que se necesite acceso.
3. Haga clic en el botón **Compartir dispositivo sin conexión**.
4. En la ventana que se abre, elija la sección **Agente de autenticación**.
5. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación creada para el usuario que está solicitando la recuperación del nombre de usuario y la contraseña de la cuenta del Agente de autenticación.
6. Escriba los bloques de solicitud que haya recibido del usuario.

Como resultado, en la parte inferior de la ventana se mostrarán los bloques generados en respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de su cuenta del Agente de autenticación. Indíquele al usuario el contenido de estos bloques.

Una vez que se complete el procedimiento de recuperación, el Agente de autenticación le pedirá al usuario que cambie la contraseña.

## Restaurar el acceso a un disco duro que no sea el del sistema

El siguiente es el procedimiento para restaurar el acceso a un disco duro que no es el del sistema y que se ha protegido con la tecnología de Cifrado de disco de Kaspersky:

1. El usuario le envía al administrador un archivo de solicitud de acceso.
2. El administrador agrega el archivo de solicitud de acceso en Kaspersky Security Center; a continuación, crea un archivo de clave de acceso y se lo envía al usuario.
3. El usuario agrega el archivo de clave de acceso en Kaspersky Endpoint Security y obtiene acceso al disco duro.

Para iniciar el procedimiento de recuperación, el usuario debe tratar de acceder al disco duro. Cuando lo haga, Kaspersky Endpoint Security creará un archivo de solicitud de acceso, que tendrá la extensión KESDC. El usuario deberá enviarle ese archivo al administrador por correo electrónico o por cualquier otro medio.

**Cómo obtener, mediante la Consola de administración (MMC), un archivo de clave de acceso para un disco duro cifrado que no sea el del sistema**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione el elemento **Otorgar acceso en el modo fuera de línea**.
6. En la ventana que se abre, seleccione la ficha **Cifrado de datos**.
7. En la ficha **Cifrado de datos**, haga clic en el botón **Examinar**.
8. En la ventana para seleccionar el archivo de solicitud de acceso, especifique la ruta al archivo que le haya enviado el usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.

**Cómo obtener, mediante Web Console, un archivo de clave de acceso para un disco duro cifrado que no sea el del sistema**

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los archivos a los que se necesite acceso.
3. Haga clic en el botón **Compartir dispositivo sin conexión**.
4. Elija la sección **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión KESDC).

   Web Console le mostrará información sobre la solicitud. Encontrará, entre otros datos, el nombre del equipo que contiene los archivos a los que el usuario necesita acceder.
6. Haga clic en el botón **Guardar clave** y seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión KESDR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

## Actualización del sistema operativo

A la hora de actualizar el sistema operativo de un equipo protegido con la característica Cifrado de disco completo (FDE), existen ciertas consideraciones que se deben tener en cuenta. La actualización debe realizarse de este modo: primero se debe actualizar el SO de un único equipo, luego el de un grupo reducido de equipos y, finalmente, el de todos los equipos conectados a la red.

Cuando se utiliza la tecnología Cifrado de disco de Kaspersky, el Agente de autenticación se carga antes que el sistema operativo. El Agente de autenticación permite que el usuario inicie sesión en el sistema y reciba acceso a las unidades cifradas. Solo entonces comienza la carga del sistema operativo.

Si intenta actualizar el sistema operativo de un equipo protegido con la tecnología Cifrado de disco de Kaspersky, el asistente para actualizar el SO desinstalará el Agente de autenticación. Como resultado, el cargador del SO no podrá acceder al disco cifrado y usted podría quedar sin acceso al equipo.

Para actualizar el sistema operativo de forma segura, consulte los detalles en la Base de conocimientos del Servicio de soporte técnico.

El sistema operativo puede actualizarse automáticamente bajo 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 es la 11.2.0 o posterior.

Si se cumplen las condiciones anteriores, puede actualizar el sistema operativo con normalidad.

Si está utilizando la tecnología 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 interruptor `/ReflectDrivers` y especifique la carpeta que contiene los controladores guardados:

   ```
   setup.exe /ReflectDrivers C:\fde_drivers
   ```

Cuando se utiliza la tecnología Cifrado de unidad BitLocker, no es necesario descifrar los discos duros para actualizar Windows 10. Para más información sobre BitLocker, visite el *sitio web de Microsoft*.

## Eliminación de errores de actualización de la funcionalidad de cifrado

Cuando Kaspersky Endpoint Security para Windows se actualiza a la versión 11.6.0, también se actualiza la característica Cifrado de disco completo.

Al iniciar la actualización de la funcionalidad Cifrado de disco completo, pueden ocurrir los siguientes errores:

- No se puede inicializar la actualización.
- El dispositivo no es compatible con el Agente de autenticación.

*Para eliminar los errores que ocurrieron al iniciar el proceso de actualización de la funcionalidad de Cifrado de disco completo en la nueva versión de la aplicación:*

1. Descifrar discos duros.
2. Cifrar discos duros una vez más.

Durante la actualización de la funcionalidad Cifrado de disco completo, pueden ocurrir los siguientes errores:

- No se puede completar la actualización.
- La reversión de la actualización de Cifrado de disco completo se completó con un error.

*Para eliminar los errores que ocurrieron durante el proceso de actualización de la funcionalidad Cifrado de disco completo,*

restaurar acceso a dispositivos cifrados con la Utilidad de Restauración.

## Selección del nivel de seguimiento para el Agente de autenticación

La aplicación registra información de servicio sobre el funcionamiento del Agente de autenticación e información acerca de las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

*Para seleccionar un nivel de seguimiento para el Agente de autenticación:*

1. Tan pronto se inicie un equipo con discos duros cifrados, presione el botón **F3** para abrir una ventana para configurar los parámetros del Agente de autenticación.

2. En la ventana de configuración del Agente de autenticación, seleccione el nivel de seguimiento:

   - **Deshabilitar registro de depuración (predeterminado)**. Si se selecciona esta opción, la aplicación no registra la información sobre eventos del Agente de autenticación en el archivo de seguimiento.

- **Habilitar registro de depuración**. Si se selecciona esta opción, la aplicación registra la información sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

- **Habilitar registro detallado**. Si se selecciona esta opción, la aplicación registra información detallada sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

  El nivel de detalle de las entradas de esta opción es mayor en comparación con el nivel de la opción **Habilitar registro de depuración**. Un nivel más alto de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.

- **Habilitar registro de depuración y seleccionar puerto serie**. Si se selecciona esta opción, la aplicación registra la información sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento, y las transmite mediante el puerto COM.

  Si se conecta un equipo con discos duros cifrados a otro equipo mediante el puerto COM, se pueden examinar los eventos del Agente de autenticación desde este otro equipo.

- **Habilitar registro detallado y seleccionar puerto serie**. Si se selecciona esta opción, la aplicación registra información detallada sobre el funcionamiento del Agente de autenticación y las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento, y las transmite mediante el puerto COM.

  El nivel de detalle de las entradas de esta opción es mayor en comparación con el nivel de la opción **Habilitar registro de depuración y seleccionar puerto serie**. Un nivel más alto 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 es necesario, puede enviar el archivo de seguimiento del Agente de autenticación a Kaspersky en forma manual para su análisis.

## Edición de los textos de ayuda del Agente de autenticación

Antes de modificar los mensajes de ayuda del Agente de autenticación, consulte la lista de caracteres que pueden usarse en un entorno de prearranque (véase más abajo).

*Para modificar mensajes de ayuda del Agente de autenticación:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 la sección **Plantillas**, haga clic en el botón **Ayuda**.

   Se abre la ventana **Mensajes de ayuda del Agente de autenticación**.

7. Haga lo siguiente:

   - Seleccione la ficha **Autenticación** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se están ingresando las credenciales de la cuenta.
   - Seleccione la ficha **Cambiar contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se está cambiando la contraseña correspondiente a la cuenta del Agente de autenticación.
   - Seleccione la ficha **Recuperar contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se está recuperando la contraseña correspondiente a la cuenta del Agente de autenticación.

8. Modifique los mensajes de ayuda.

   Si quiere restaurar el texto original, haga clic en el botón **Predeterminado**.

   > Puede ingresar texto de ayuda que contenga 16 líneas o menos. La longitud máxima de una línea es 64 caracteres.

9. Guarde los cambios.

## Compatibilidad limitada de caracteres en los mensajes de ayuda del Agente de autenticación

En un entorno previo al inicio, se admiten los siguientes caracteres Unicode:

- Alfabeto latino básico (0000 - 007F)
- Caracteres latinos adicionales-1 (0080 - 00FF)
- Caracteres latinos extendidos-A (0100 - 017F)
- Caracteres latinos extendidos-B (0180 - 024F)
- Caracteres de ID extendidos sin combinar (02B0 - 02FF)
- Marcas diacríticas combinadas (0300 - 036F)
- Alfabetos griego y copto (0370 - 03FF)
- Alfabeto cirílico (0400 - 04FF)
- Hebreo (0590 - 05FF)
- Alfabeto árabe (0600 - 06FF)
- Latín extendido adicional (1E00 - 1EFF)
- Signos de puntuación (2000 - 206F)

- Símbolos de divisa (20A0 - 20CF)
- Símbolos semejantes a letras (2100 - 214F)
- Figuras geométricas (25A0 - 25FF)
- Formas de presentación del alfabeto árabe-B (FE70 - FEFF)

Los caracteres que no se especifican en esta lista no se admiten en un entorno previo al inicio. No se recomienda usar dichos caracteres en mensajes de ayuda del Agente de autenticación.

## Eliminación de objetos y datos residuales tras evaluar el funcionamiento del Agente de autenticación

Durante la desinstalación de aplicación, si Kaspersky Endpoint Security detecta objetos y datos que permanecen en el disco duro del sistema después de la operación de prueba del Agente de autenticación, se interrumpe la desinstalación de aplicación y no puede reiniciarse hasta eliminar dichos objetos y datos.

Los objetos y datos pueden permanecer en el disco duro del sistema después de la operación de prueba del Agente de autenticación solo en casos excepcionales. Por ejemplo: esto puede suceder si el equipo no se ha reiniciado luego de haber aplicado una directiva de Kaspersky Security Center con configuración de cifrado, o en caso de que la aplicación no pueda iniciarse luego de una operación de prueba del Agente de autenticación.

Puede quitar objetos y datos restantes en el disco duro del sistema después de una operación de prueba del Agente de autenticación de varias maneras:

- Con la directiva de Kaspersky Security Center.
- Con la Utilidad de restauración.

*Para usar una directiva de Kaspersky Security Center para eliminar objetos y datos restantes después de la operación de prueba del Agente de autenticación:*

1. Aplique al equipo una directiva de Kaspersky Security Center con parámetros configurados para descifrar todos los discos duros del equipo.
2. Inicie Kaspersky Endpoint Security.

*Para quitar información sobre incompatibilidad de aplicaciones con el Agente de autenticación,*

escriba el comando `avp pbatestreset` en la línea de comandos.

## Administración de BitLocker

*BitLocker* es una tecnología de cifrado que forma parte de los sistemas operativos Windows. Kaspersky Endpoint Security permite controlar y administrar BitLocker a través de Kaspersky Security Center. La tecnología BitLocker está diseñada para cifrar volúmenes lógicos. No puede utilizarse para cifrar unidades extraíbles. Para más información sobre BitLocker, puede consultar la documentación de Microsoft.

Las claves de acceso de BitLocker pueden almacenarse de manera segura utilizando un TPM (módulo de plataforma segura). Un *módulo de plataforma segura (TPM)* es un microchip que ofrece funciones de seguridad fundamentales (entre ellas, la capacidad de almacenar claves de cifrado). Por lo general, el TPM forma parte de la placa madre del equipo e interactúa con los demás componentes del sistema a través de un bus físico. Es la opción más segura para almacenar las claves de acceso de BitLocker porque permite verificar la integridad del sistema antes del arranque. La ausencia de un TPM no es impedimento para cifrar las unidades de un equipo. En tal caso, se utiliza una contraseña para cifrar la clave de acceso. BitLocker permite emplear los siguientes métodos de autenticación:

- TPM.
- PIN y TPM,
- contraseña.

Cuando se cifra una unidad, BitLocker crea una clave maestra. Kaspersky Endpoint Security transfiere esa clave a Kaspersky Security Center; ello le permitirá restaurar el acceso a la unidad si un usuario olvida su contraseña, por ejemplo.

Si un usuario cifra su disco con BitLocker, Kaspersky Endpoint Security remitirá información sobre la operación a Kaspersky Security Center. Sin embargo, la clave maestra no se transferirá a Kaspersky Security Center, por lo que no será posible restaurar el acceso al disco a través de Kaspersky Security Center. Para que BitLocker pueda interactuar correctamente con Kaspersky Security Center, será necesario descifrar la unidad y utilizar una directiva para volver a cifrarla. El descifrado se puede realizar localmente o con una directiva.

Cuando la unidad del sistema está cifrada, el usuario debe superar la autenticación de BitLocker para iniciar el sistema operativo. BitLocker permitirá que el usuario inicie sesión una vez que se haya autenticado. BitLocker no es compatible con la tecnología de inicio de sesión único (SSO).

Si utiliza directivas de grupo de Windows, deshabilite el control de BitLocker en las mismas. Las directivas de Windows pueden interferir con las de Kaspersky Security Center. Tales interferencias pueden derivar en errores de cifrado.

## Activación del Cifrado de unidad BitLocker

Antes de cifrar un disco completo, recomendamos verificar que el equipo no esté infectado. Para hacerlo, inicie la tarea de Análisis completo o la de Análisis de áreas críticas. La realización del cifrado de disco completo en un equipo que está infectado con un rootkit puede hacer que el equipo se vuelva inoperable.

Para usar la tecnología Cifrado de unidad BitLocker en equipos que tengan una edición de Windows diseñada para servidores, es posible que primero necesite instalar el componente Cifrado de unidad BitLocker. Utilice para ello las herramientas que brinda el sistema operativo (el Asistente para agregar roles y características). Consulte la documentación de Microsoft para más información sobre cómo instalar Cifrado de unidad BitLocker.

**Cómo activar el Cifrado de unidad BitLocker a través de la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 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 podrá solo cargar el sistema operativo en el cual se realizó el cifrado.
8. Configure las opciones avanzadas de Cifrado de unidad BitLocker (vea la tabla de más abajo).
9. Guarde los cambios.

Cómo activar el Cifrado de unidad BitLocker a través de Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos que desee cifrar con Cifrado de unidad BitLocker.

   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 la sección **Control del cifrado**, seleccione **Cifrado de unidad BitLocker**.
6. Haga clic en el vínculo **Cifrado de unidad BitLocker**.

   Se abrirá la ventana Configuración de 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 podrá solo cargar el sistema operativo en el cual se realizó el cifrado.
8. Configure las opciones avanzadas de Cifrado de unidad BitLocker (vea la tabla de más abajo).
9. Haga clic en **Aceptar**.

Si desea monitorear el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.

Luego de aplicar la directiva, la aplicación muestra las siguientes preguntas, según la configuración de la autenticación:

- Solo TPM. No se requiere la entrada del usuario. El disco se cifrará cuando el equipo se reinicie.
- TPM + PIN / Contraseña. Si se encuentra disponible un módulo de TPM, aparece una ventana para escribir el código PIN. Si no hay disponible un módulo de TPM, se mostrará una ventana para escribir la contraseña de autenticación previa al inicio.
- Solo contraseña. Verá una ventana de solicitud de contraseña para la autenticación previa al inicio.

Si el modo de compatibilidad estándar del Procesamiento de información federal está habilitado para el sistema operativo del equipo, entonces en Windows 8 y las versiones anteriores del sistema operativo, se muestra una solicitud para conectar un dispositivo de almacenamiento para guardar el archivo de clave de recuperación. Es posible guardar varios archivos de clave de recuperación en un mismo dispositivo de almacenamiento.

Una vez que defina el PIN o la contraseña, BitLocker le pedirá que reinicie el equipo. Esto es necesario para que se complete el proceso de cifrado. El usuario deberá luego superar el procedimiento de autenticación de BitLocker. Tras autenticarse, el usuario tendrá que iniciar sesión en el sistema. El proceso de cifrado con BitLocker se completará una vez que se cargue el sistema operativo.

De no tener acceso a las claves de cifrado, el usuario puede solicitar una clave de recuperación al administrador de la red de área local (en el caso de que la clave de recuperación se haya perdido o de que no se la haya guardado en el dispositivo de antemano).

Parámetros del componente Cifrado de unidad BitLocker

| Parámetro | Descripción |
|---|---|
| **Habilitar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en pizarras** | Esta casilla de verificación habilita / deshabilita el uso de la autenticación que requiere el ingreso de datos en un entorno previo al inicio del sistema, aun si la plataforma no tiene la capacidad de ingreso previo al inicio del sistema (por ejemplo, con teclados de pantalla táctil en tabletas).<br>La pantalla táctil de las tabletas no está disponible en el entorno previo al inicio. Para completar la autenticación de BitLocker en tabletas, el usuario debe, por ejemplo, conectar un teclado USB.<br>Si se selecciona la casilla de verificación, se permite el uso de la autenticación que requiere ingreso previo al inicio del sistema. Se recomienda usar esta configuración solo para dispositivos que tienen herramientas alternativas de ingreso de datos en un entorno previo al inicio del sistema, como ser, un teclado USB además de teclados de pantalla táctil.<br>Para poder usar la tecnología Cifrado de unidad BitLocker en una tableta, esta casilla debe estar activada. |
| **Usar cifrado de hardware (Windows 8 y versiones posteriores)** | Si se selecciona la casilla de verificación, la aplicación implementa cifrado del hardware. Esto le permite aumentar la velocidad de cifrado y usar menos recursos del equipo. |

| | |
|---|---|
| **Cifrar solo el espacio de disco usado (Windows 8 y versiones posteriores)** | Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado.<br><br>Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado.<br><br>Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se añaden.<br><br>Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente.<br><br>Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables.<br><br>Esta casilla está desactivada por defecto. |
| **Parámetros de autenticación** | **Usar contraseña (Windows 8 y versiones posteriores)**<br><br>Si se selecciona esta opción, Kaspersky Endpoint Security le solicita al usuario una contraseña cuando intenta acceder a una unidad cifrada.<br><br>Esta opción se puede seleccionar cuando no se está utilizando un Módulo de plataforma segura (TPM).<br><br>**Usar el módulo de plataforma segura (TPM)**<br><br>Si se selecciona esta opción, BitLocker usa un Módulo de plataforma segura (TPM).<br><br>Un *módulo de plataforma segura (TPM)* es un microchip que ofrece funciones de seguridad fundamentales (entre ellas, la capacidad de almacenar claves de cifrado). Suele haber un Módulo de plataforma segura instalado en la placa madre del equipo y este módulo interactúa con todos los demás componentes del sistema a través del bus de hardware.<br><br>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.<br><br>Un dispositivo equipado con un Módulo de plataforma segura puede crear claves de cifrado que solo se pueden descifrar con el dispositivo. Un Módulo de plataforma segura cifra claves de cifrado con su propia clave de almacenamiento raíz. La clave de almacenamiento raíz se almacena dentro del Módulo de plataforma segura. Esto proporciona un nivel adicional de protección contra intentos de ataque a claves de cifrado.<br><br>Esta acción está seleccionada por defecto.<br><br>Puede establecer una capa de protección adicional para acceder a la clave de cifrado, y cifrar la clave con una contraseña o PIN: |

| | |
|---|---|
| | • **Usar PIN para TPM**. Si activa esta casilla, los usuarios podrán usar un código PIN para obtener acceso a una clave de cifrado almacenada en un módulo de plataforma segura (TPM).<br>Si desactiva esta casilla, los usuarios no podrán usar un código PIN. Para acceder a la clave de cifrado, deberán utilizar una contraseña.<br>Puede permitir que el usuario use un código PIN mejorado. El *código PIN mejorado* permite usar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.<br><br>• **Usar el módulo de plataforma segura (TPM); si no está disponible, use la contraseña**. Si la casilla de verificación está seleccionada, el usuario puede usar una contraseña para obtener acceso a claves de cifrado cuando un módulo de plataforma segura (TPM) no está disponible.<br><br>Si desactiva esta casilla y no hay un módulo TPM disponible, la función de cifrado de disco completo no se iniciará. |

## Cómo descifrar un disco duro protegido con BitLocker

Puede suceder que un usuario descifre su disco duro utilizando la función *Desactivar BitLocker* del sistema operativo. Si esto ocurre, Kaspersky Endpoint Security le pedirá al usuario repetidamente que vuelva a cifrar la unidad. Para que Kaspersky Endpoint Security deje de hacer esta solicitud, será necesario habilitar el descifrado de la unidad en la directiva.

Cómo descifrar un disco duro protegido con BitLocker a través de la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 unidad BitLocker**.
7. En la lista desplegable **Modo de cifrado**, seleccione **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 la ficha **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos que deban descifrarse.

   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 haga clic en el vínculo para configurar los ajustes.

   Se muestran los ajustes de cifrado.
6. En la lista desplegable **Modo de cifrado**, seleccione **Descifrar todos los discos duros**.
7. Haga clic en **Aceptar**.

Si desea monitorear el cifrado o descifrado del disco en el equipo de un usuario, puede hacerlo con una herramienta llamada Monitoreo de Cifrado. La herramienta Monitoreo de Cifrado puede ejecutarse desde la ventana principal de la aplicación.

## Restaurar el acceso a una unidad protegida con BitLocker

Si un usuario olvida la contraseña para acceder a un disco duro cifrado con BitLocker, debe iniciar el procedimiento de recuperación (procedimiento de solicitud y respuesta).

Si el sistema operativo del equipo es Windows 8 o una versión anterior y tiene habilitado el modo de compatibilidad con el Estándar federal de procesamiento de información (FIPS), habrá guardado un archivo de clave de recuperación en una unidad extraíble antes de que se aplicara el cifrado. Para volver a acceder a la unidad cifrada, conecte la unidad extraíble y siga las instrucciones en pantalla.

El siguiente es el procedimiento para restaurar el acceso a un disco duro cifrado con BitLocker:

1. El usuario le indica al administrador el id. de la clave de recuperación (vea la imagen de más abajo).
2. En Kaspersky Security Center, el administrador abre las propiedades del equipo y verifica el id. de la clave de recuperación. El id. provisto por el usuario debe ser el mismo que aparezca en las propiedades del equipo.
3. Si los id. de la clave de recuperación coinciden, el administrador le brinda al usuario una clave de recuperación o le envía un archivo de clave de recuperación.

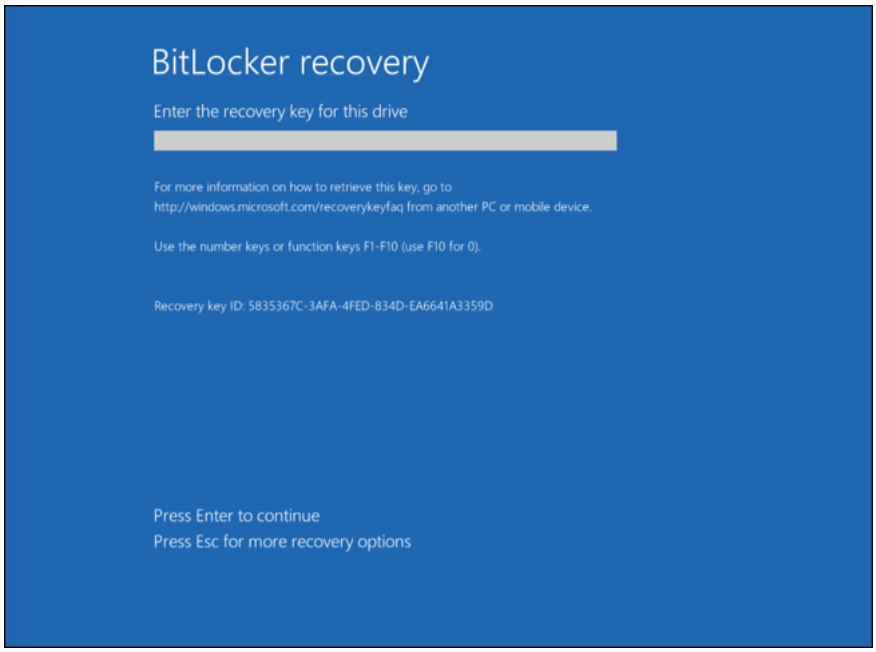
   Los archivos de clave de recuperación se utilizan para equipos con uno de estos sistemas operativos:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011

- Windows Server 2012

Para los demás sistemas operativos, debe usarse en cambio una clave de recuperación.

4. El usuario introduce la clave de recuperación y obtiene acceso al disco duro.




Restaurar el acceso a un disco duro cifrado con BitLocker

## Restaurar el acceso a una unidad del sistema

Para iniciar el procedimiento de recuperación, el usuario debe presionar la tecla **Esc** en la etapa de autenticación de prearranque.

[Cómo ver la clave de recuperación para una unidad del sistema cifrada con BitLocker a través de la Consola de administración (MMC)]

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione el elemento **Otorgar acceso en el modo fuera de línea**.
6. En la ventana que se abre, seleccione la ficha **Acceso a una unidad del sistema protegida con BitLocker**.
7. Solicite al usuario que ingrese el identificador de la clave de recuperación que se indica en la ventana para ingresar la contraseña de BitLocker y compárelo con el identificador presente en el campo **ID de clave de recuperación**.

   Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco de sistema especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

Tras completar estos pasos, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá enviarle al usuario.

### Cómo ver la clave de recuperación para una unidad del sistema cifrada con BitLocker a través de Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Dispositivos → Dispositivos administrados**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentre la unidad a la que se necesite acceso.
3. Haga clic en el botón **Compartir dispositivo sin conexión**.
4. En la ventana que se abre, elija la sección **BitLocker**.
5. Verifique el id. de la clave de recuperación. El id. provisto por el usuario debe ser el mismo que aparezca en las propiedades del equipo.

   Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco de sistema especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.
6. Haga clic en el botón **Recibir clave**.

Tras completar estos pasos, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá enviarle al usuario.

Una vez que se carga el sistema operativo, Kaspersky Endpoint Security solicita al usuario que cambie la contraseña o el código PIN. Después de establecer una nueva contraseña o código PIN, BitLocker creará una nueva clave principal y la enviará a Kaspersky Security Center. De esta manera, se actualizarán la clave de recuperación y el archivo de clave de recuperación. Si el usuario no cambia la contraseña, será posible usar la clave de recuperación antigua la siguiente vez que se cargue el sistema operativo.

Los equipos con Windows 7 no permiten cambiar la contraseña o el código PIN. Una vez que se ingresa la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, es imposible establecer una contraseña nueva o un código PIN. Este problema se origina por las peculiaridades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.

## Restaurar el acceso a una unidad que no sea la del sistema

Para iniciar el procedimiento de recuperación, el usuario debe hacer clic en el vínculo **Olvidé la contraseña** de la ventana que le permite obtener acceso a la unidad. Una vez que tenga acceso a la unidad cifrada, el usuario podrá modificar la configuración de BitLocker para que, cuando se autentique en Windows, la unidad se desbloquee automáticamente.

**Cómo ver la clave de recuperación para una unidad cifrada con BitLocker (que no sea la del sistema) a través de la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Protección y cifrado de datos** → **Dispositivos cifrados**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que necesite crear el archivo de clave de acceso. A continuación, en el menú contextual del dispositivo, seleccione **Obtener acceso al dispositivo en Kaspersky Endpoint Security para Windows (11.6.0)**.
4. Solicite al usuario que ingrese el identificador de la clave de recuperación que se indica en la ventana para ingresar la contraseña de BitLocker y compárelo con el identificador presente en el campo **ID de clave de recuperación**.

   Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

5. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.

**Cómo ver la clave de recuperación para una unidad cifrada con BitLocker (que no sea la del sistema) a través de Web Console y Cloud Console**

1. En la ventana principal de Web Console, seleccione **Operaciones → Protección y cifrado de datos → Dispositivos cifrados**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentre la unidad a la que se necesite acceso.
3. Haga clic en el botón **Compartir dispositivo sin conexión**.

   Se inicia un asistente para otorgar acceso al dispositivo.
4. Siga las instrucciones del asistente para otorgar acceso al dispositivo:

   a. Seleccione el complemento de **Kaspersky Endpoint Security para Windows**.

   b. Verifique el id. de la clave de recuperación. El id. provisto por el usuario debe ser el mismo que aparezca en las propiedades del equipo.

   > Si los identificadores no coinciden, esta clave no es válida para restaurar el acceso al disco de sistema especificado. Asegúrese de que el nombre del equipo seleccionado coincida con el nombre del equipo del usuario.

   c. Haga clic en el botón **Recibir clave**.

Tras completar estos pasos, tendrá acceso a la clave de recuperación o al archivo de la clave de recuperación, que deberá enviarle al usuario.

## Cifrado de archivos en discos de equipos locales.

> Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

La característica de cifrado de archivos está sujeta a las siguientes consideraciones especiales:

- Kaspersky Endpoint Security cifrará o descifrará archivos en las carpetas predefinidas únicamente para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifrará ni descifrará ningún archivo que se encuentre en una carpeta redirigida o en las carpetas predefinidas de un perfil de usuario móvil, un perfil de usuario obligatorio o un perfil de usuario temporal.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo y las aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas están en la lista de exclusiones de cifrado:
  - %WINDIR%
  - %PROGRAMFILES% y %PROGRAMFILES(X86)%
  - Archivos de registro de Windows.

No es posible ver ni modificar la lista de exclusiones de cifrado. Aunque los archivos y carpetas de esta lista pueden agregarse a la lista de cifrado, la característica de cifrado de archivos nunca cifrará esos objetos.

## Cifrado de archivos en discos locales del equipo.

Kaspersky Endpoint Security no cifra los archivos cuyo contenido se encuentra en el almacenamiento de la nube de OneDrive, y bloquea los archivos cifrados para que no se copien en el almacenamiento en la nube de OneDrive, si estos archivos no se agregan a la regla de descifrado.

*Para cifrar archivos en discos 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 ficha **Cifrado**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Según reglas**.
8. En la ficha **Cifrado**, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:

   a. Seleccione el elemento **Carpetas predefinidas** para agregar archivos desde carpetas de perfiles de usuarios locales sugeridos por expertos de Kaspersky a una regla de cifrado.

   - **Documentos**. Archivos que se encuentren en la carpeta *Documentos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.
   - **Favoritos**. Archivos que se encuentren en la carpeta *Favoritos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.
   - **Escritorio**. Archivos que se encuentren en la carpeta *Escritorio* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.
   - **Archivos temporales**. Archivos temporales vinculados al funcionamiento de las aplicaciones instaladas en el equipo. Aquí se incluyen, por ejemplo, las copias de seguridad temporales que se crean al trabajar con documentos en las aplicaciones de Microsoft Office.
   - **Archivos de Outlook**. Archivos vinculados al funcionamiento del cliente de correo electrónico Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de las libretas de direcciones sin conexión (OAB) y archivos de las libretas de direcciones personales (PAB).

   b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de carpeta introducida manualmente a una regla de cifrado.

   Cuando agregue una ruta de carpeta, siga estas reglas:

- Utilice una variable de entorno (por ejemplo, `%CARPETA%\CarpetaDelUsuario\`). Puede usar una sola variable de entorno por ruta, y únicamente al comienzo de la ruta.
- No utilice rutas relativas. Puede utilizar los caracteres `\..\` (por ejemplo, `C:\Usuarios\..\CarpetaDelUsuario\`). Los caracteres `\..\` se utilizan para referirse a la carpeta que se encuentra un nivel más arriba.
- No utilice los caracteres `*` y `?`.
- No utilice rutas UNC.
- Utilice los caracteres `;` o `,` como separadores.

c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo individuales a una regla de cifrado. Kaspersky Endpoint Security cifrará los archivos con las extensiones especificadas en todos los discos locales del equipo.

d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones (por ejemplo, *Documentos de Microsoft Office*) a una regla de cifrado. Kaspersky Endpoint Security cifrará archivos que tengan las extensiones indicadas en los grupos de extensiones en todos los discos locales del equipo.

9. Guarde los cambios.

Tan pronto como se aplique la directiva, Kaspersky Endpoint Security cifrará los archivos incluidos en la regla de cifrado y no incluidos en la regla de descifrado.

La característica de cifrado de archivos está sujeta a las siguientes consideraciones especiales:

- Cuando un archivo aparece al mismo tiempo en una regla de cifrado y en una regla de descifrado, Kaspersky Endpoint Security hace lo siguiente:
  - si el archivo no está cifrado, lo deja sin cifrar;
  - si el archivo está cifrado, lo descifra.
- Kaspersky Endpoint Security se mantiene siempre atento a los archivos nuevos que puedan reunir los criterios de las reglas de cifrado y que, por ende, deban cifrarse. Un archivo existente que no esté cifrado puede pasar a cumplir con los criterios de una regla si, por ejemplo, sus propiedades (ruta o extensión) se modifican. Si Kaspersky Endpoint Security detecta un archivo de este tipo, lo cifrará.
- Cuando el usuario crea un archivo nuevo cuyas propiedades cumplen los criterios de la regla de cifrado, Kaspersky Endpoint Security cifra el archivo tan pronto como se abre.
- Kaspersky Endpoint Security pospone el cifrado de los archivos abiertos hasta que se los cierre.
- Si mueve un archivo cifrado a otra carpeta en el disco local, el archivo permanece cifrado sin importar si esta carpeta figura o no en la regla de cifrado.
- Si descifra un archivo y lo copia a una carpeta local que no esté incluida en una regla de descifrado, la aplicación podría cifrar la copia del archivo. Para que la copia del archivo no se cifre, deberá crear una regla de descifrado para la carpeta de destino.

## Formación de reglas de acceso a archivos cifrados para aplicaciones

*Para formar 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 el elemento **Según reglas**.

   Las reglas de acceso solo se aplican en el modo **Según reglas**. Si aplica las reglas de acceso estando en el modo **Según reglas** y luego pasa al modo **Dejar sin modificar**, Kaspersky Endpoint Security no tendrá en cuenta ninguna de las reglas de acceso. Todas las aplicaciones tendrán acceso a todos los archivos cifrados.

7. En la parte derecha de la ventana, seleccione la ficha **Reglas para aplicaciones**.
8. Si quiere seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.

   a. Especifique los filtros para restringir la lista de aplicaciones que aparecen en la tabla. Para hacerlo, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período de adición**, y todas las casillas de la sección **Grupo**.

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

   c. En la tabla, figurarán las aplicaciones que coincidan con los filtros seleccionados.

   d. En la columna **Aplicaciones**, seleccione las casillas junto a las aplicaciones para las que desea formar las reglas de acceso a archivos cifrados.

   e. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a archivos cifrados.

   f. En la lista desplegable **Acciones para aplicaciones seleccionadas previamente**, seleccione la acción que realizará Kaspersky Endpoint Security sobre las reglas de acceso a archivos cifrados que se formaron previamente para dichas aplicaciones.

   g. Haga clic en **Aceptar**.

   Los detalles de una regla de acceso a archivos cifrados para aplicaciones aparecen en la tabla ficha **Reglas para aplicaciones**.

9. Si quiere seleccionar aplicaciones manualmente, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

   a. En el campo de entrada de datos, escriba el nombre o una lista de nombres de archivos de aplicación ejecutables con sus extensiones.

También puede agregar los nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center si hace clic en el botón **Agregar de la lista de Kaspersky Security Center**.

b. Si es necesario, en el campo **Descripción**, ingrese una descripción de la lista de aplicaciones.

c. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a archivos cifrados.

d. Haga clic en **Aceptar**.

Los detalles de una regla de acceso a archivos cifrados para aplicaciones aparecen en la tabla ficha **Reglas para aplicaciones**.

10. Guarde los cambios.

## Cifrado de archivos que son creados o modificados por aplicaciones específicas

Puede crear una regla según la cual Kaspersky Endpoint Security cifrará todos los archivos creados o modificados por las aplicaciones especificadas en la regla.

No se cifrarán los archivos que fueron creados o modificados por las aplicaciones especificadas antes de aplicarse la regla del cifrado.

*Para configurar el cifrado de archivos que son creados o modificados por aplicaciones específicas:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 el elemento **Según reglas**.

   Las reglas de cifrado se aplican solo en el modo **Según reglas**. Si aplica las reglas de cifrado estando en el modo **Según reglas** y luego pasa al modo **Dejar sin modificar**, Kaspersky Endpoint Security no tendrá en cuenta ninguna de las reglas de cifrado. Los archivos que se cifraron anteriormente permanecerán cifrados.

7. En la parte derecha de la ventana, seleccione la ficha **Reglas para aplicaciones**.
8. Si quiere seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.

   Se abre la ventana **Añadir aplicaciones de la lista de Kaspersky Security Center**.

Haga lo siguiente:

a. Especifique los filtros para restringir la lista de aplicaciones que aparecen en la tabla. Para hacerlo, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período de adición**, y todas las casillas de la sección **Grupo**.

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

En la tabla, figurarán las aplicaciones que coincidan con los filtros seleccionados.

c. En la columna **Aplicaciones**, active las casillas adyacentes a las aplicaciones con las que se crearán los archivos que deban cifrarse.

d. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

e. En la lista desplegable **Acciones para aplicaciones seleccionadas previamente**, seleccione la acción que realizará Kaspersky Endpoint Security sobre las reglas de cifrado de archivos cifrados que se formaron previamente para dichas aplicaciones.

f. Haga clic en **Aceptar**.

La información sobre la regla de cifrado para archivos creados o modificados por las aplicaciones seleccionadas aparece en la tabla de la ficha **Reglas para aplicaciones**.

9. Si quiere seleccionar aplicaciones manualmente, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

Se abre la ventana **Agregar o modificar los nombres de los archivos ejecutables de las aplicaciones**.

Haga lo siguiente:

a. En el campo de entrada de datos, escriba el nombre o una lista de nombres de archivos de aplicación ejecutables con sus extensiones.

También puede agregar los nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center si hace clic en el botón **Agregar de la lista de Kaspersky Security Center**.

b. Si es necesario, en el campo **Descripción**, ingrese una descripción de la lista de aplicaciones.

c. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.

d. Haga clic en **Aceptar**.

La información sobre la regla de cifrado para archivos creados o modificados por las aplicaciones seleccionadas aparece en la tabla de la ficha **Reglas 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.

3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 ficha **Descifrado**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Según reglas**.
8. En la ficha **Descifrado**, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:
   a. Seleccione el elemento **Carpetas predefinidas** para agregar archivos desde carpetas de perfiles de usuarios locales sugeridos por expertos de Kaspersky a una regla de descifrado.
   b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de carpeta introducida manualmente a una regla de descifrado.
   c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo individuales a una regla de descifrado. Kaspersky Endpoint Security no cifrará los archivos con las extensiones especificadas en todos los discos locales del equipo.
   d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones (por ejemplo, *Documentos de Microsoft Office*) a una regla de descifrado. Kaspersky Endpoint Security no cifrará los archivos almacenados en los discos locales del equipo que tengan alguna de las extensiones indicadas en los grupos de extensiones.
9. Guarde los cambios.

Si se agregó el mismo archivo a la lista de cifrado y a la regla de descifrado, Kaspersky Endpoint Security no cifrará este archivo si no está cifrado, y lo descifrará si está cifrado.

## Descifrado de archivos en unidades de disco locales del equipo

*Para descifrar archivos en discos locales:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 ficha **Cifrado**.
7. Elimine de la lista de cifrado los archivos y las carpetas que desea descifrar. Para ello, seleccione los archivos y el elemento **Eliminar regla y descifrar archivos** en el menú contextual del botón **Eliminar**.

Puede eliminar al mismo tiempo varios elementos de la lista de cifrado. Para ello, seleccione los archivos que necesita con el botón izquierdo del mouse mientras mantiene presionada la tecla **CTRL**, y seleccione el elemento **Eliminar regla y descifrar archivos** en el menú contextual del botón **Eliminar**.

Los archivos y las carpetas que se eliminan de la lista de cifrado se agregan automáticamente a la lista de descifrado.

8. Formar una lista de descifrado de archivos.

9. Guarde los cambios.

No bien se implementa la directiva, Kaspersky Endpoint Security descifra los archivos cifrados que se agregaron a la lista de descifrado.

Kaspersky Endpoint Security descifra los archivos cifrados si sus parámetros (ruta de la carpeta, nombre de archivo, extensión de archivo) cambian para coincidir con los parámetros de objetos que se agregaron a la lista de descifrado.

Kaspersky Endpoint Security pospone el descifrado de los archivos abiertos hasta que se los cierre.

## Creación de paquetes cifrados

Si necesita enviarle un archivo a alguien que está fuera de la red corporativa, puede hacerlo en forma segura utilizando un paquete cifrado. Los paquetes cifrados son útiles para compartir archivos de gran tamaño utilizando unidades extraíbles, ya que las aplicaciones de correo electrónico suelen restringir el tamaño de los adjuntos.

Cuando un usuario intente crear un paquete cifrado, Kaspersky Endpoint Security le solicitará una contraseña. Para contribuir con la protección de los datos, es posible definir (y hacer que la aplicación controle) los requisitos con los que deberán cumplir estas contraseñas para que se las considere seguras. Ello evitará que los usuarios utilicen claves simples y cortas, como `1234`.

**Cómo habilitar el control de requisitos para las contraseñas definidas al crear archivos cifrados en la Consola de administración (MMC)**

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.

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

4. Seleccione la directiva correspondiente 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 contraseñas**, haga clic en el botón **Configuración**.

7. En la ventana que se abre, seleccione la ficha **Paquetes cifrados**.

8. Configure los requisitos de complejidad con los que deberán cumplir las contraseñas de los paquetes cifrados.

**Cómo habilitar el control de requisitos para las contraseñas definidas al crear archivos cifrados Web Console**

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desee habilitar el control de requisitos.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Cifrado de datos** → **Cifrado de archivos**.
5. En el bloque **Configuración de contraseña para paquetes cifrados**, defina los requisitos con los que deberán cumplir las contraseñas de los paquetes cifrados que cree en el futuro.

Para crear un paquete cifrado, debe utilizar un equipo con Kaspersky Endpoint Security que tenga la característica Cifrado de archivos habilitada.

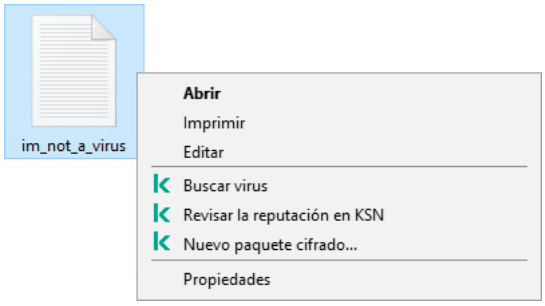
Al agregar un archivo al paquete cifrado cuyo contenido está almacenado en la nube de OneDrive, Kaspersky Endpoint Security descarga el contenido del archivo y luego lo cifra.

*Para crear un paquete cifrado:*

1. En cualquier administrador de archivos, seleccione los archivos o las carpetas que deban formar parte del paquete cifrado. Haga clic con el botón derecho del mouse para abrir su menú contextual.
2. En el menú contextual, seleccione **Nuevo paquete cifrado** (vea la siguiente imagen).
3. En la ventana que se abre, indique en qué ubicación de la unidad extraíble se guardará el paquete cifrado, especifique el nombre del paquete y haga clic en el botón **Guardar**.
4. En la ventana que se abre, defina y confirme la contraseña.

   La contraseña deberá ajustarse a los requisitos de seguridad que se hayan definido en la directiva.
5. Haga clic en el botón **Crear**.

Se inicia el proceso de creación del paquete cifrado. Kaspersky Endpoint Security no realiza la compresión de archivos cuando crea un paquete cifrado. Cuando el proceso finalice, se creará un paquete cifrado autoextraíble en la carpeta de destino. El paquete será un archivo ejecutable (de extensión exe) con el icono y estará protegido con la contraseña que haya definido.




Creación de un paquete cifrado

Para acceder a los archivos de un paquete cifrado, haga doble clic en el paquete y, luego de que se inicie el asistente de desempaquetamiento, escriba la contraseña. Si ha olvidado la contraseña, no podrá recuperarla; quedará, en ese caso, sin acceso a los archivos del paquete. Si lo desea, podrá volver a crear el paquete cifrado.

## Procedimiento para recuperar el acceso a archivos cifrados

Cuando un grupo de archivos se cifra, Kaspersky Endpoint Security recibe una clave de cifrado que permite acceder a ellos en forma directa. Si utiliza esta clave de cifrado, un usuario que esté trabajando con cualquier cuenta de usuario de Windows que esté activa durante el cifrado de archivos podrá acceder directamente a los archivos cifrados. Los usuarios que trabajen con las cuentas de Windows que estaban activas durante el cifrado de archivos deben conectarse a Kaspersky Security Center para acceder a los archivos cifrados.

Los archivos cifrados pueden ser inaccesibles en las siguientes circunstancias:

- El equipo del usuario almacena claves de cifrado, pero no hay conexión con Kaspersky Security Center para administrar las claves. En este caso, el usuario debe solicitar acceso a los archivos cifrados al administrador de la red LAN.

  Si el acceso a Kaspersky Security Center no existe, debe:

  - solicitar una clave de acceso para el acceso a archivos cifrados en los discos duros del equipo;
  - para acceder a los archivos cifrados almacenados en unidades extraíbles, solicite otra clave de acceso para los archivos cifrados de cada disco extraíble.

- Los componentes del cifrado se eliminan desde el equipo del usuario. En este caso, el usuario puede abrir los archivos cifrados en discos locales y extraíbles, pero los contenidos de esos archivos aparecerán cifrados.

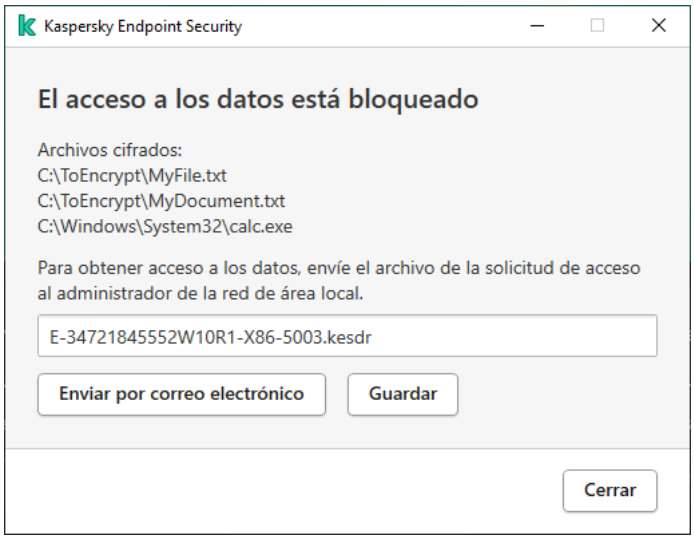
  El usuario puede trabajar con archivos cifrados en las siguientes circunstancias:

  - Los archivos se encuentran dentro de paquetes cifrados creados en un equipo con Kaspersky Endpoint Security instalado.
  - Los archivos están almacenados en unidades extraíbles en las cuales se ha autorizado el modo portátil.

El usuario que necesite acceder a los archivos cifrados deberá iniciar un procedimiento de recuperación (un procedimiento de solicitud y respuesta).

El procedimiento para recuperar acceso a los archivos cifrados consiste en lo siguiente:

1. El usuario le envía al administrador un archivo de solicitud de acceso (vea la imagen de abajo).
2. El administrador agrega el archivo de solicitud de acceso en Kaspersky Security Center; a continuación, crea un archivo de clave de acceso y se lo envía al usuario.
3. El usuario agrega el archivo de clave de acceso en Kaspersky Endpoint Security y obtiene acceso a los archivos.




Procedimiento para recuperar el acceso a archivos cifrados

Para iniciar el procedimiento de recuperación, el usuario debe tratar de acceder a un archivo. Cuando lo haga, Kaspersky Endpoint Security creará un archivo de solicitud de acceso, que tendrá la extensión KESDC. El usuario deberá enviarle ese archivo al administrador por correo electrónico o por cualquier otro medio.

Kaspersky Endpoint Security genera archivos de solicitud de acceso que permiten acceder a todos los archivos cifrados almacenados en la unidad (disco local o unidad extraíble) del equipo.

Cómo obtener un archivo de clave de acceso para archivos cifrados mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione el elemento **Otorgar acceso en el modo fuera de línea**.
6. En la ventana que se abre, seleccione la ficha **Cifrado de datos**.
7. En la ficha **Cifrado de datos**, haga clic en el botón **Examinar**.
8. En la ventana para seleccionar el archivo de solicitud de acceso, especifique la ruta al archivo que le haya enviado el usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.

Cómo obtener un archivo de clave de acceso para archivos cifrados mediante Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los archivos a los que se necesite acceso.
3. Haga clic en el botón **Compartir dispositivo sin conexión**.
4. Elija la sección **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión KESDC).

   Web Console le mostrará información sobre la solicitud. Encontrará, entre otros datos, el nombre del equipo que contiene los archivos a los que el usuario necesita acceder.
6. Haga clic en el botón **Guardar clave** y seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión KESDR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

Una vez que lo reciba, el usuario deberá hacer doble clic en el archivo de clave de acceso para ejecutarlo. Kaspersky Endpoint Security le permitirá entonces acceder a todos los archivos cifrados de la unidad. Si el usuario necesita acceso a los archivos cifrados de una unidad diferente, deberá obtener un nuevo archivo de clave de acceso, exclusivo para esa unidad.

## Restauración del acceso a datos cifrados después de una falla del sistema operativo

Ante un problema con el sistema operativo, únicamente podrá recuperar el acceso a la información que se haya cifrado con la tecnología de cifrado de archivos (FLE). La información para la que se haya usado el cifrado de disco completo (FDE) no podrá restaurarse.

*Para recuperar el acceso a sus datos cifrados después de una falla del sistema operativo:*

1. Reinstale el sistema operativo sin formatear el disco duro.
2. Instale Kaspersky Endpoint Security.
3. Establezca una conexión entre el equipo y el Servidor de administración de Kaspersky Security Center que controlaba el equipo al momento de cifrarse los datos.

Los datos cifrados volverán a estar disponibles bajo las mismas condiciones de acceso que hayan estado vigentes antes del problema con el sistema operativo.

## Modificación de plantillas de mensajes de acceso a archivos cifrados

*Para modificar plantillas de mensajes de acceso a archivos cifrados:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 la sección **Plantillas**, haga clic en el botón **Plantillas**.

   Se abre la ventana **Plantillas**.
7. Haga lo siguiente:

   - Si quiere modificar la plantilla del mensaje del usuario, seleccione la ficha **Mensaje del usuario**. Cuando un usuario intente acceder a un archivo cifrado sin que haya en su equipo una clave que le permita hacerlo, se abrirá la ventana **El acceso a los datos está bloqueado**. El mensaje basado en esta plantilla se crea automáticamente cuando el usuario hace clic en el botón **Enviar por correo electrónico** de la ventana **El acceso a los datos está bloqueado**. Este mensaje se envía al administrador de la red de área local corporativa junto con el archivo para solicitar acceso a archivos cifrados.
   - Si quiere modificar la plantilla del mensaje del administrador, seleccione la ficha **Mensaje del administrador**. Este mensaje se crea automáticamente al hacer clic en el botón **Enviar por correo electrónico** de la ventana **Solicitar acceso a archivos cifrados** y se envía al usuario después de que se le otorga acceso a los archivos cifrados.
8. Modifique las plantillas de mensaje.

   Puede usar el botón **Predeterminado** y la lista desplegable **Variable**.
9. Guarde los cambios.

## Cifrado de unidades extraíbles

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si se conecta una unidad extraíble con un sistema de archivos no compatible al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Para proteger la información almacenada en una unidad extraíble, puede usar los siguientes tipos de cifrado:

- Cifrado de disco completo (FDE).

  Cifrado de la unidad extraíble completa, incluido su sistema de archivos.

Tenga en cuenta que no se podrá acceder a la información cifrada fuera de la red corporativa. Aun dentro de la red corporativa, tampoco será posible acceder a esta información si el equipo no está conectado a Kaspersky Security Center (es decir, si se utiliza un equipo invitado).

- Cifrado de archivos (FLE).

  Cifrado únicamente de los archivos almacenados en la unidad extraíble. El sistema de archivos no se modifica.

  Si cifra los archivos de una unidad extraíble, podrá utilizar un modo especial —llamado *modo portátil*— para acceder a la información fuera de la red corporativa.

Kaspersky Endpoint Security crea una clave maestra como parte del proceso de cifrado. La clave maestra se guarda en los siguientes repositorios:

- Kaspersky Security Center
- El equipo del usuario

  La clave maestra se cifra con la clave secreta del usuario.
- Unidad extraíble

  La clave maestra se cifra con la clave pública de Kaspersky Security Center.

Una vez que haya cifrado una unidad extraíble, mientras se encuentre dentro de la red corporativa, podrá acceder a sus datos como si estuviera utilizando una unidad convencional sin cifrado.

## Acceso a datos cifrados

Cuando se conecta una unidad extraíble con información cifrada, Kaspersky Endpoint Security hace lo siguiente:

1. Busca una clave maestra en el repositorio local del equipo del usuario.

   Si encuentra la clave maestra pertinente, el usuario puede acceder a la información de la unidad extraíble.

   Si no encuentra la clave maestra, Kaspersky Endpoint Security hace lo siguiente:

   a. Envía una solicitud a Kaspersky Security Center.

      Tras recibir la solicitud, Kaspersky Security Center envía una respuesta con la clave maestra.

   b. Kaspersky Endpoint Security guarda la clave maestra en el repositorio local del equipo para poder operar con la unidad extraíble cifrada.
2. Descifra la información.

## Consideraciones especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles está sujeto a las siguientes consideraciones especiales:

- La directiva con los ajustes preestablecidos para el cifrado de unidades extraíbles se crea para un grupo específico de equipos administrados. Por lo tanto, el resultado de la aplicación de la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al cual está conectada la unidad extraíble.

- Kaspersky Endpoint Security no cifra ni descifra los archivos de solo lectura que puedan encontrarse en las unidades extraíbles.
- Los siguientes tipos de dispositivo se admiten como unidad extraíble:
  - Medios de datos conectados por medio de un bus USB
  - Discos duros conectados por medio de buses USB y FireWire
  - Unidades SSD conectadas por medio de buses USB y FireWire

## Inicio del cifrado de unidades extraíbles

Para descifrar una unidad extraíble, puede utilizarse una directiva. Las directivas en las que se definen los ajustes de cifrado de unidades extraíbles se crean para grupos de administración específicos. Por lo tanto, el resultado del descifrado de datos en unidades extraíbles depende del equipo al cual esté conectada la unidad extraíble.

Kaspersky Endpoint Security admite el cifrado de 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 la unidad extraíble completa** (FDE). Kaspersky Endpoint Security cifrará el contenido de las unidades extraíbles sector por sector. Con ello, se cifrarán no solo los archivos de las unidades, sino también sus sistemas de archivos, incluidos los nombres de los archivos y las estructuras de carpetas.
   - **Cifrar todos los archivos** (FLE). Kaspersky Endpoint Security cifrará todos los archivos que se encuentren en las unidades extraíbles. Los sistemas de archivos no se cifrarán, con lo cual los nombres de los archivos y las estructuras de carpetas quedarán sin cambios.
   - **Solo cifrar archivos nuevos** (FLE). De los archivos de las unidades extraíbles, Kaspersky Endpoint Security cifrará únicamente aquellos que se hayan agregado o modificado desde la última aplicación de la directiva de Kaspersky Security Center.

   Si una unidad extraíble ya está cifrada, Kaspersky Endpoint Security no la vuelve a cifrar.

7. Si desea que las unidades extraíbles se cifren en modo portátil, active la casilla **Modo portátil**.

   El *modo portátil* es un modo de funcionamiento de la característica de cifrado de archivos (FLE). Brinda la capacidad de acceder a la información de una unidad extraíble cifrada cuando se está fuera de la red corporativa. También permite trabajar con información cifrada en equipos que no tienen Kaspersky Endpoint Security instalado.

8. Para cifrar unidades extraíbles nuevas, recomendamos activar la casilla **Cifrar solo el espacio de disco usado**. Si se cancela la selección de la casilla, Kaspersky Endpoint Security cifrará todos los archivos que encuentre en una unidad, incluidos los remanentes de archivos eliminados o modificados.

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, seleccione la casilla **Permitir cifrado de unidades extraíbles en el modo sin conexión**.

    El *modo de cifrado sin conexión* se utiliza para cifrar unidades extraíbles, mediante la tecnología de FDE, cuando no hay conexión con Kaspersky Security Center. Durante el cifrado, Kaspersky Endpoint Security guarda la clave maestra únicamente en el equipo del usuario. La clave maestra se envía a Kaspersky Security Center cuando se realiza la siguiente sincronización.

    Si el equipo en el que está almacenada la clave maestra sufre un desperfecto y los datos no se transfirieron a Kaspersky Security Center, será imposible acceder a la unidad extraíble.

    Si la casilla **Permitir cifrado de unidades extraíbles en el modo sin conexión** no está activada y no hay conexión con Kaspersky Security Center, las unidades extraíbles no se podrán cifrar.

11. Guarde los cambios.

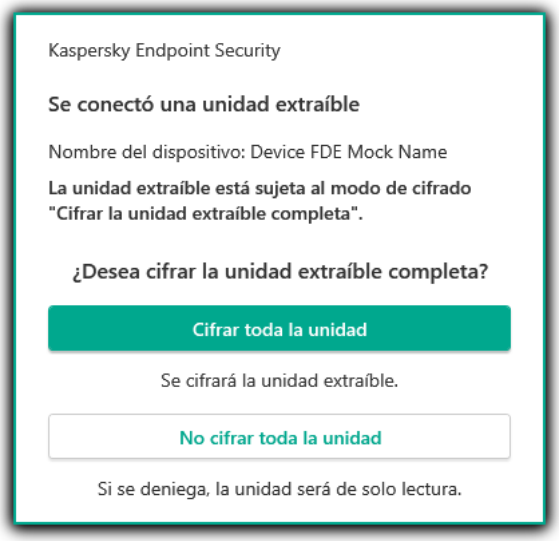
Cuando se conecte una unidad extraíble (o cuando ya haya una unidad extraíble conectada) después de que se aplique la directiva, Kaspersky Endpoint Security le solicitará al usuario que confirme la operación de cifrado (vea la imagen de más abajo).

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 solicitud se repetirá la siguiente vez que se aplique una directiva de Kaspersky Security Center o cuando se vuelva a conectar la misma unidad extraíble.

Si el usuario intenta expulsar una unidad extraíble en forma segura mientras su información se está cifrando, Kaspersky Endpoint Security interrumpirá el proceso de cifrado antes de que se complete y permitirá extraer la unidad. El proceso de cifrado se reanudará cuando el usuario conecte la unidad nuevamente al equipo.

Si tiene problemas para cifrar una unidad extraíble, consulte el informe de **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Puede ocurrir que otra aplicación impida el acceso a los archivos. En tal caso, desconecte la unidad extraíble y vuelva a conectarla.




Solicitud de cifrado para una unidad extraíble

## Agregar una regla de cifrado para unidades extraíbles

*Para añadir una regla de cifrado para unidades extraíbles:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 sobre el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:
   - Si quiere agregar reglas de cifrado para unidades extraíbles que están en la lista de dispositivos de confianza del componente Control de dispositivos, seleccione **De la lista de dispositivos de confianza de esta directiva**.
   - Si quiere agregar reglas de cifrado para unidades extraíbles que están en la lista de Kaspersky Security Center, seleccione **De la lista de dispositivos de Kaspersky Security Center**.
7. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione la acción que realizará Kaspersky Endpoint Security en los archivos almacenados en las unidades extraíbles seleccionadas.
8. Seleccione la casilla **Modo portátil** si desea que Kaspersky Endpoint Security prepare las unidades extraíbles antes del cifrado, lo que permite que sea posible utilizar los archivos cifrados almacenados en esas unidades en modo portátil.

   El modo portátil le permite usar archivos cifrados almacenados en unidades extraíbles conectadas a equipos sin funcionalidad de cifrado.
9. Seleccione la casilla **Solo cifrar el espacio de disco usado** si quiere que Kaspersky Endpoint Security cifre solo los sectores del disco que estén ocupados por archivos.

Si está aplicando el cifrado a un disco que ya está en uso, le recomendamos que cifre todo el disco. De esta manera, se asegurará de que todos los datos estén protegidos, incluso los datos eliminados que todavía podrían contener información recuperable. Se recomienda usar la función **Solo cifrar el espacio de disco usado** en el caso de discos nuevos sin uso previo.

Si un dispositivo ya se cifró con la función **Solo cifrar el espacio de disco usado**, después de aplicar una directiva en el modo **Cifrar la unidad extraíble completa**, no se cifrarán los sectores no ocupados por archivos.

10. En la lista desplegable **Acciones para dispositivos seleccionados previamente**, seleccione la acción que realizará Kaspersky Endpoint Security de acuerdo con las reglas de cifrado previamente definidas para las unidades extraíbles:

    - Si quiere que la regla de cifrado creada anteriormente para el disco extraíble permanezca sin cambios, seleccione **Omitir**.
    - Si quiere que la regla de cifrado creada anteriormente para la unidad extraíble sea reemplazada por la regla nueva, seleccione **Actualizar**.

11. Guarde los cambios.

Las nuevas reglas de cifrado se aplicarán a todas las unidades extraíbles conectadas a los equipos de la organización.

## Exportar e importar una lista de reglas de cifrado para unidades extraíbles

Puede exportar la lista de reglas de cifrado de unidades extraíbles a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de reglas para el mismo tipo de unidades extraíbles. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de reglas o para migrar las reglas a otro servidor.

Cómo exportar e importar una lista de reglas de cifrado de unidades extraíbles a la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 la regla de acceso que desea exportar. Para seleccionar varios puertos, use las teclas **CTRL** o **SHIFT**.
      Si no seleccionó ninguna regla, Kaspersky Endpoint Security exportará todas las reglas.
   b. Haga clic en el vínculo **Exportar**.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Haga clic en el botón **Guardar**.
      Kaspersky Endpoint Security exportará la lista de reglas al archivo XML.
7. Para importar una lista de reglas de cifrado para unidades extraíbles:
   a. Haga clic en el vínculo **Importar**.
      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.
      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
8. Guarde los cambios.

Cómo exportar e importar una lista de reglas de cifrado de unidades extraíbles a 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 correspondiente a los equipos en los desee exportar o importar una lista de reglas de cifrado de unidades extraíbles.

   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 dispositivos seleccionados**, haga clic en el vínculo **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 la regla de acceso que desea exportar.
   b. Haga clic en el botón **Exportar**.
   c. Confirme que desea exportar solo las reglas seleccionadas, o bien exporte la lista completa.
   d. Haga clic en el botón **Exportar**.

      Kaspersky Endpoint Security exporta la lista de reglas a un archivo XML en la carpeta de descargas predeterminada.
7. Para importar la lista de reglas:
   a. Haga clic en el vínculo **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Haga clic en el botón **Abrir**.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Endpoint Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
8. Guarde los cambios.

## Modo portátil para acceder a unidades extraíbles con archivos cifrados

El *modo portátil* es un modo de funcionamiento de la característica de cifrado de archivos (FLE). Brinda la capacidad de acceder a la información de una unidad extraíble cifrada cuando se está fuera de la red corporativa. También permite trabajar con información cifrada en equipos que no tienen Kaspersky Endpoint Security instalado.

El modo portátil es útil en los siguientes casos:

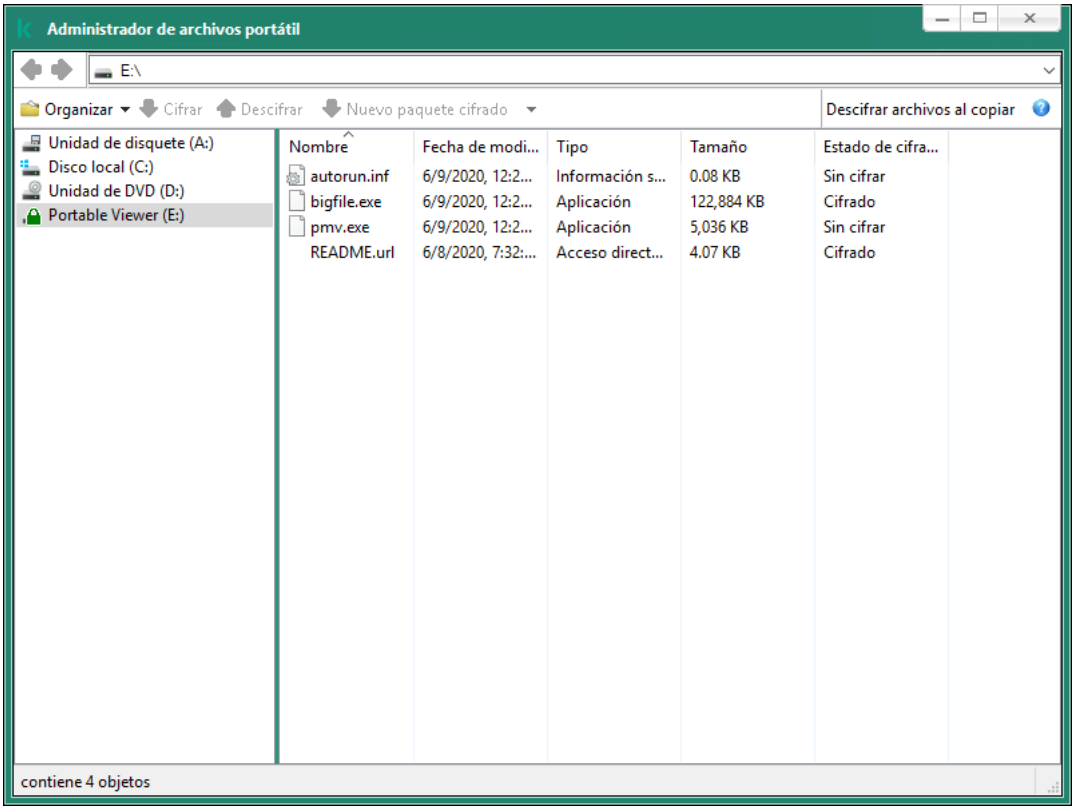
- cuando no hay conexión entre el equipo y el Servidor de administración de Kaspersky Security Center,
- cuando la infraestructura se ha modificado debido a un cambio de Servidor de administración de Kaspersky Security Center,
- cuando Kaspersky Endpoint Security no está instalado en el equipo.

## Administrador de archivos portátiles

Para que una unidad extraíble pueda utilizarse en modo portátil, Kaspersky Endpoint Security instala en ella un módulo de cifrado especial, llamado *Administrador de archivos portátil*. A través de su interfaz, el Administrador de archivos portátil permite operar con información cifrada cuando Kaspersky Endpoint Security no está instalado en un equipo (vea la imagen de más abajo). Cuando Kaspersky Endpoint Security está instalado en un equipo, la información de una unidad extraíble cifrada puede manipularse con cualquier administrador de archivos (por ejemplo, el Explorador de Windows).

El Administrador de archivos portátil almacena una clave que se utiliza para cifrar los archivos de la unidad extraíble. Esta clave, a su vez, está cifrada con una contraseña que define el usuario. El usuario establece la contraseña antes de que se cifren los archivos de la unidad.

Cuando conecte una unidad extraíble a un equipo que no tenga Kaspersky Endpoint Security instalado, el Administrador de archivos portátil se ejecutará automáticamente. Si la autoejecución de aplicaciones está deshabilitada en el equipo, deberá abrir el Administrador de archivos portátil en forma manual. Para hacer esto, ejecute el archivo pmv.exe, que encontrará en la unidad extraíble.




Administrador de archivos portátiles

## Habilitar el modo portátil para operar con archivos cifrados

[Cómo habilitar, mediante la Consola de administración (MMC), el uso del modo portátil para operar con los archivos cifrados de una unidad extraíble]

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 todos los archivos** o **Solo cifrar archivos nuevos**.

   El modo portátil solo es compatible con la tecnología de cifrado de archivos (FLE). No podrá utilizar el modo portátil con la tecnología de cifrado de disco completo (FDE).

7. Seleccione la casilla **Modo portátil**.
8. De ser necesario, agregue reglas de cifrado para unidades extraíbles específicas.
9. Guarde los cambios.
10. Aplique la directiva y conecte la unidad extraíble al equipo.
11. Confirme la operación de cifrado del disco extraíble.

    Se abre una ventana en la que puede crear una contraseña para el Administrador de archivos portátil.
12. Especifique una contraseña que cumpla con los requisitos de seguridad y confírmela.
13. Haga clic en **Aceptar**.

Kaspersky Endpoint Security cifrará los archivos de la unidad extraíble. El Administrador de archivos portátil se copiará a la unidad extraíble para que pueda trabajar con los archivos cifrados. Si la unidad ya contiene archivos cifrados, Kaspersky Endpoint Security los volverá a cifrar con su propia clave. De este modo, el usuario podrá acceder a todos los archivos de la unidad cuando utilice el modo portátil.

**Cómo habilitar, mediante Web Console, el uso del modo portátil para operar con los archivos cifrados de una unidad extraíble**

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security correspondiente a los equipos en los que desee permitir el uso del modo portátil.

   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 la sección **Control del cifrado**, seleccione **Cifrar todos los archivos** o **Solo cifrar archivos nuevos**.

   El modo portátil solo es compatible con la tecnología de cifrado de archivos (FLE). No podrá utilizar el modo portátil con la tecnología de cifrado de disco completo (FDE).
6. Seleccione la casilla **Modo portátil**.
7. De ser necesario, agregue reglas de cifrado para unidades extraíbles específicas.
8. Guarde los cambios.
9. Aplique la directiva y conecte la unidad extraíble al equipo.
10. Confirme la operación de cifrado del disco extraíble.

    Se abre una ventana en la que puede crear una contraseña para el Administrador de archivos portátil.
11. Especifique una contraseña que cumpla con los requisitos de seguridad y confírmela.
12. Haga clic en **Aceptar**.

Kaspersky Endpoint Security cifrará los archivos de la unidad extraíble. El Administrador de archivos portátil se copiará a la unidad extraíble para que pueda trabajar con los archivos cifrados. Si la unidad ya contiene archivos cifrados, Kaspersky Endpoint Security los volverá a cifrar con su propia clave. De este modo, el usuario podrá acceder a todos los archivos de la unidad cuando utilice el modo portátil.

## Acceder a los archivos cifrados de una unidad extraíble

Tras cifrar los archivos de una unidad extraíble que permita usar el modo portátil, podrá acceder al contenido de las siguientes maneras:

- Si Kaspersky Endpoint Security no está instalado en el equipo, el Administrador de archivos portátil le pedirá una contraseña. Deberá introducir esta contraseña cada vez que reinicie el equipo o reconecte la unidad extraíble.
- Si el equipo tiene Kaspersky Endpoint Security instalado, pero se encuentra fuera de la red corporativa, la aplicación le pedirá que introduzca una contraseña o que le envíe al administrador una solicitud para acceder a los archivos. Una vez que tenga acceso a los archivos de la unidad extraíble, Kaspersky Endpoint Security guardará la clave secreta en el repositorio de claves del equipo. De esta manera, podrá acceder a los archivos cuando lo necesite sin tener que escribir la contraseña o pedirle autorización al administrador.

- Si el equipo tiene Kaspersky Endpoint Security instalado y se encuentra dentro de la red corporativa, podrá acceder al dispositivo sin introducir ninguna contraseña. Kaspersky Endpoint Security obtendrá la clave secreta del Servidor de administración de Kaspersky Security Center al que se encuentre conectado el equipo.

## Recuperar la contraseña definida para el modo portátil

Si olvida la contraseña que definió para usar el modo portátil, conecte la unidad extraíble a un equipo que tenga Kaspersky Endpoint Security instalado y que se encuentre conectado a la red corporativa. Se le permitirá acceder a los archivos de la unidad puesto que la clave secreta estará almacenada en el repositorio de claves del equipo o en el Servidor de administración. Descifre los archivos y vuelva a cifrarlos con una nueva contraseña.

## Propiedades del modo portátil cuando una unidad extraíble se conecta a un equipo vinculado a otra red

Si su equipo tiene Kaspersky Endpoint Security instalado, pero se encuentra fuera de la red corporativa, dispone de las siguientes alternativas para acceder a los archivos:

- **Acceder a los archivos utilizando una contraseña**

  Una vez que introduzca la contraseña, tendrá la capacidad de ver, modificar y guardar archivos en la unidad extraíble (tendrá *acceso transparente*). Kaspersky Endpoint Security podría otorgarle acceso de solo lectura a la unidad si el cifrado de unidades extraíbles está configurado del siguiente modo en la directiva:

  - El modo portátil está deshabilitado.
  - El modo seleccionado es **Cifrar todos los archivos** o **Solo cifrar archivos nuevos**.

  En los demás casos, tendrá acceso completo (de lectura y escritura) a la unidad extraíble. Podrá agregar y eliminar archivos.

  Los permisos de acceso a una unidad pueden modificarse en cualquier momento, incluso mientras la unidad está conectada al equipo. Si los permisos se modifican, Kaspersky Endpoint Security bloqueará el acceso a los archivos y le pedirá la contraseña nuevamente.

  Una vez que introduzca la contraseña, no podrá aplicar ajustes de directiva de cifrado para la unidad extraíble. En tal caso, no podrá descifrar los archivos de la unidad ni volver a cifrarlos.

- **Solicitarle al administrador que le brinde acceso a los archivos**

  Si ha olvidado la contraseña que definió para utilizar el modo portátil, comuníquese con el administrador para que le brinde acceso a los archivos. Para realizar el pedido, deberá enviarle al administrador un archivo de solicitud de acceso, que tendrá la extensión KESDC. El archivo puede enviarse por correo electrónico o por cualquier otro medio. El administrador le enviará a usted un archivo de acceso (un archivo de extensión KESDR), que le permitirá acceder a los archivos cifrados.

  Tras completar el procedimiento de solicitud y respuesta para recuperar la contraseña, tendrá acceso total (de lectura y escritura) a la unidad extraíble y acceso transparente a los archivos que contenga.

  Podrá aplicar una directiva de cifrado de unidades extraíbles y, con ello, descifrar archivos o realizar otras acciones. Una vez que haya recuperado la contraseña, o cuando se actualice la directiva, Kaspersky Endpoint Security le pedirá que confirme los cambios.

  Cómo obtener un archivo de acceso a datos cifrados mediante la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que le haya pedido acceso a los archivos cifrados. A continuación, haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione el elemento **Otorgar acceso en el modo fuera de línea**.
6. En la ventana que se abre, seleccione la ficha **Cifrado de datos**.
7. En la ficha **Cifrado de datos**, haga clic en el botón **Examinar**.
8. En la ventana para seleccionar el archivo de solicitud de acceso, especifique la ruta al archivo que le haya enviado el usuario.

Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.

**Cómo obtener un archivo de acceso a datos cifrados mediante Web Console**

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los archivos a los que se necesite acceso.
3. Haga clic en el botón **Compartir dispositivo sin conexión**.
4. Elija la sección **Cifrado de datos**.
5. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión KESDC).

   Web Console le mostrará información sobre la solicitud. Encontrará, entre otros datos, el nombre del equipo que contiene los archivos a los que el usuario necesita acceder.
6. Haga clic en el botón **Guardar clave** y seleccione la carpeta en la que se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión KESDR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

## Descifrado de unidades extraíbles

Para descifrar una unidad extraíble, puede utilizarse una directiva. Las directivas en las que se definen los ajustes de cifrado de unidades extraíbles se crean para grupos de administración específicos. Por lo tanto, el resultado del descifrado de datos en unidades extraíbles depende del equipo al cual esté conectada la unidad extraíble.

*Para descifrar unidades extraíbles:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente 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 quiere descifrar todos los archivos cifrados almacenados en las unidades extraíbles, en la lista desplegable **Modo de cifrado**, seleccione **Descifrar la unidad extraíble completa**.
7. Para descifrar datos almacenados en unidades extraíbles individuales, modifique las reglas de cifrado para las unidades extraíbles que contienen los datos que quiera descifrar. Para hacerlo:
   a. En la lista de unidades extraíbles para las que se configuraron reglas de cifrado, seleccione una entrada correspondiente a la unidad extraíble que necesita.
   b. Haga clic en el botón **Establecer una regla** para modificar la regla de cifrado para el disco extraíble seleccionado.
      Se abre el menú contextual del botón **Establecer una regla**.
   c. Seleccione el elemento **Descifrar todos los archivos** en el menú contextual del botón **Establecer una regla**.
8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security descifra las unidades extraíbles que ya se encuentren conectadas al equipo o que el usuario conecte. La aplicación le advierte al usuario que el proceso de descifrado puede durar algunos minutos. Si el usuario inicia la extracción segura de un disco extraíble durante el descifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de descifrado de datos y permite la extracción del disco extraíble antes de que finalice la operación de descifrado. El proceso de descifrado se reanudará cuando el usuario conecte la unidad al equipo nuevamente.

Si no consigue descifrar una unidad extraíble, consulte el informe de **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Puede ocurrir que otra aplicación impida el acceso a los archivos. En tal caso, desconecte la unidad extraíble y vuelva a conectarla.

## Visualización de detalles del cifrado de datos

En el transcurso del cifrado o descifrado, Kaspersky Endpoint Security envía información sobre el estado de los parámetros de cifrado correspondientes a los equipos cliente de Kaspersky Security Center.

Pueden aparecer los siguientes valores de estado de cifrado:

- *Directiva de cifrado no definida*. No se ha definido una directiva de cifrado de Kaspersky Security Center para el equipo.
- *Aplicación de la directiva*. El cifrado/descifrado de datos está en curso en el equipo.

- *Error*. Se produjo un error durante el cifrado o descifrado de datos en el equipo.
- *Es necesario reiniciar*. Se debe reiniciar el sistema operativo para poder comenzar o finalizar el cifrado o descifrado de datos en el equipo.
- *Cumple con la directiva*. Se completó el cifrado de datos en el equipo de acuerdo con los parámetros de cifrado especificados en la directiva de Kaspersky Security Center implementada en el equipo.
- *Cancelado por el usuario*. El usuario se ha negado a confirmar la operación de cifrado del archivo en el disco extraíble.

## Visualización del estado de cifrado

*Para ver el estado de 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 con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.

   En la ficha **Dispositivos** del espacio de trabajo se muestran las propiedades de los equipos del grupo de administración seleccionado.
4. En la ficha **Dispositivos** del espacio de trabajo, deslice la barra de desplazamiento hasta el extremo derecho.
5. Si no se muestra la columna **Estado de cifrado**:

   a. Haga clic con el botón derecho del mouse para abrir el encabezado de la tabla.

   b. En el menú contextual, en la lista desplegable **Ver**, seleccione **Agregar/Eliminar columnas**.

   Se abre la ventana **Agregar/Eliminar columnas**.

   c. En la ventana **Agregar/Eliminar columnas**, seleccione la casilla **Estado de cifrado**.

   d. Haga clic en **Aceptar**.

La columna **Estado de cifrado** muestra el estado de cifrado de los datos de los equipos del grupo de administración seleccionado. Este estado se forma en base a la información sobre el cifrado de archivos en los discos locales del equipo y sobre el cifrado de disco completo.

## Cómo ver las estadísticas de cifrado en los paneles de Kaspersky Security Center

*Para ver el estado de cifrado en los paneles de Kaspersky Security Center:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione el nodo **Servidor de administración – <Nombre del equipo>**.

3. En el espacio de trabajo que se encuentra a la derecha del árbol de la Consola de administración, seleccione la ficha **Estadísticas**.

4. Cree una página nueva con paneles de detalles que contengan estadísticas de cifrado de datos. Para hacerlo:

   a. En la ficha **Estadísticas**, haga clic en el botón **Personalizar vista**.

      Se abre la ventana **Propiedades: Estadísticas**.

   b. En la ventana **Propiedades: Estadísticas**, haga clic en **Agregar**.

      Se abre la ventana **Propiedades: Nueva página**.

   c. En la sección **General** de la ventana **Propiedades: Nueva página**, escriba el nombre de la página.

   d. En la sección **Paneles de detalles**, haga clic en el botón **Agregar**.

      Se abre la ventana **Nuevo panel de detalles**.

   e. En la ventana **Nuevo panel de detalles** del grupo **Estado de la protección**, seleccione el elemento **Cifrado de dispositivos**.

   f. Haga clic en **Aceptar**.

      Se abre la ventana **Propiedades: <Control del cifrado>**.

   g. Si es necesario, modifique la configuración del panel de detalles. Para ello, use las secciones **Ver** y **Dispositivos** de la ventana **Propiedades: Cifrado de dispositivos**.

   h. Haga clic en **Aceptar**.

   i. Repita los pasos d al h de las instrucciones: seleccione el elemento **Cifrado de unidades extraíbles** en la sección **Estado de la protección** de la ventana **Nuevo panel de detalles**.

      Los paneles de detalles agregados aparecerán en la lista **Paneles de detalles** de la ventana **Propiedades: Nueva página**.

   j. En la ventana **Propiedades: Nueva página**, haga clic en **Aceptar**.

      El nombre de la página con los paneles de detalles que creó en los pasos anteriores aparecerá en la lista **Páginas** de la ventana **Propiedades: Estadísticas**.

   k. En la ventana **Propiedades: Estadísticas**, haga clic en **Cerrar**.

5. En la ficha **Estadísticas**, abra la página que se creó en los pasos anteriores de las instrucciones.

Aparecen los paneles de detalles, que muestran el estado de cifrado de los equipos y unidades extraíbles.

## Visualización de errores de cifrado en unidades de disco locales del equipo

*Para visualizar errores de cifrado en unidades de disco locales del equipo:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración que incluya al equipo cliente cuya lista de errores de cifrado quiera ver.

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

4. En la ficha **Dispositivos**, 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 **Propiedades: <Nombre del equipo>**, seleccione la sección **Protección**.

6. En la sección de **Protección** de la ventana **Propiedades: <nombre del equipo>**, haga clic en el vínculo **Ver lista de errores de cifrado de datos** para abrir la ventana **Errores de cifrado de datos**.

Esta ventana muestra los destalles de los errores de cifrado de archivos que se produjeron en las unidades locales del equipo. Cuando se corrige un error, Kaspersky Security Center elimina los detalles del error de la ventana **Errores de cifrado de datos**.

## Visualización del informe de cifrado de datos

*Para ver el informe de cifrado de datos:*

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la ficha **Informes**.

3. Haga clic en el botón **Nueva plantilla de informe**.

   Se inicia el Asistente de plantilla de informe.

4. Siga las instrucciones del Asistente de plantilla de informe. En la ventana **Seleccionar tipo de plantilla de informe** de la sección **Otro**, seleccione los siguientes elementos:

   - **Informe de estado de cifrado del dispositivo administrado**.
   - **Informe de estado de cifrado de almacenamiento masivo**.
   - **Informe de errores de cifrado del archivo**.
   - **Informe de acceso bloqueado a archivos cifrados**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la ficha **Informes**.

5. Seleccione la plantilla del informe que se creó en los pasos anteriores de las instrucciones.

6. En el menú contextual de la plantilla, seleccione **Mostrar informe**.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

## Trabajar con dispositivos cifrados cuando no tenemos acceso a ellos

### Obtención de acceso a dispositivos cifrados

Se puede requerir a un usuario que solicite acceso a dispositivos cifrados en los siguientes casos:

- El disco duro se cifró en un equipo diferente.

- La clave de cifrado para un dispositivo no está en el equipo (por ejemplo, después del primer intento de acceder a la unidad extraíble cifrada en el equipo), y el equipo no está conectado a Kaspersky Security Center.

  Después de que el usuario ha aplicado la clave de acceso al dispositivo cifrado, Kaspersky Endpoint Security guarda la clave de cifrado en el equipo del usuario y permite el acceso a este dispositivo aun si no hay conexión con Kaspersky Security Center.

El acceso a dispositivos cifrados se puede obtener de las siguientes maneras:

1. Desde la interfaz de Kaspersky Endpoint Security, el usuario crea un archivo de solicitud de acceso (que tendrá la extensión kesdc) y se lo envía al administrador de la LAN corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso (que tendrá la extensión kesdr) y se lo envía al usuario.
3. El usuario aplica la clave de acceso.

### Restaurar datos de dispositivos cifrados

Un usuario puede usar la Utilidad de restauración de dispositivos cifrados (en adelante también llamada Utilidad de restauración) para trabajar con dispositivos cifrados. Esto puede resultar necesario en los siguientes casos:

- El procedimiento de usar una clave de acceso para obtener acceso falló.
- No se han instalado los componentes de cifrado en el equipo con el dispositivo cifrado.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración residen en la memoria del equipo del usuario de forma no cifrada desde hace algún tiempo. Para reducir el riesgo de acceso no autorizado a tales datos, se le aconseja restaurar el acceso a los dispositivos cifrados en equipos de confianza.

Los datos en dispositivos cifrados se pueden restaurar de la siguiente forma:

1. Mediante la Utilidad de restauración, el usuario crea un archivo de solicitud de acceso (que tendrá la extensión fdertc) y se lo envía al administrador de la LAN corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso (que tendrá la extensión fdertr) y se lo envía al usuario.
3. El usuario aplica la clave de acceso.

Para restaurar datos en discos duros del sistema cifrados, el usuario también puede especificar las credenciales de la cuenta del Agente de autenticación en la Utilidad de restauración. Si los metadatos de la cuenta del Agente de autenticación se han dañado, el usuario debe completar el procedimiento de restauración usando un archivo de solicitud de acceso.

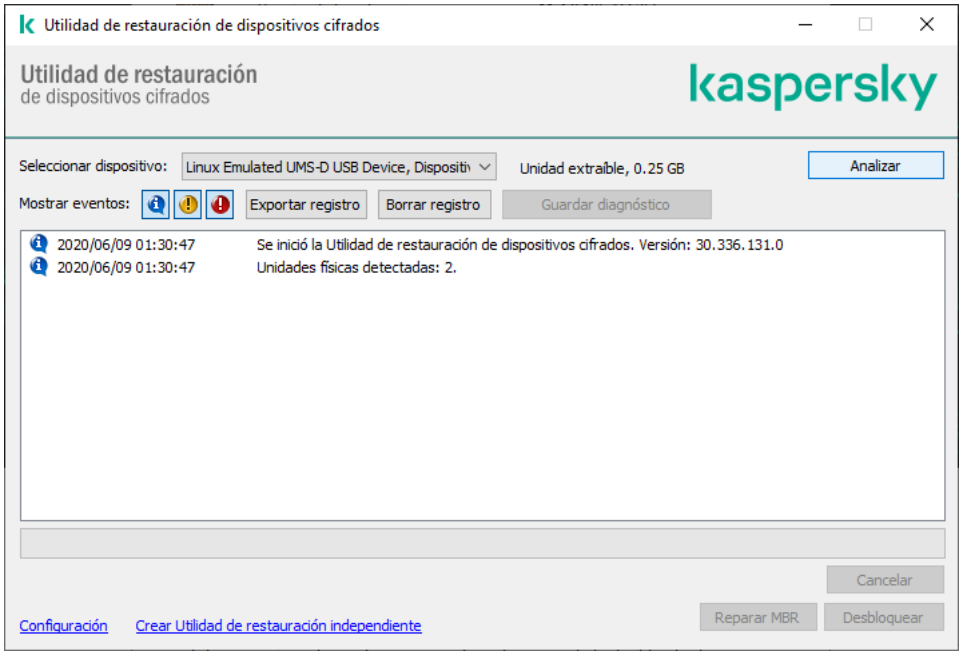
Antes de restaurar datos de dispositivos cifrados, se recomienda cancelar la directiva de Kaspersky Security Center o deshabilitar el cifrado en la configuración de la directiva de Kaspersky Security Center en el equipo donde se realizará el procedimiento. Ello evitará que el dispositivo vuelva a cifrarse.

## Recuperación de datos con la Utilidad de restauración FDERT

Cuando un disco duro sufre un daño, su sistema de archivos puede presentar irregularidades. Ante esta situación, la información que se haya protegido con la tecnología Cifrado de disco de Kaspersky quedará inaccesible. En tal caso, puede descifrar la información y copiarla a un nuevo disco duro.

Para recuperar los datos de una unidad protegida con Cifrado de disco de Kaspersky, siga estos pasos:

1. Cree una Utilidad de restauración independiente (vea la imagen de más abajo).
2. Conecte el disco a un equipo en el que no se hayan instalado los componentes de cifrado de Kaspersky Endpoint Security.
3. Ejecute la Utilidad de restauración y realice un diagnóstico del disco duro.
4. Acceda a los datos del disco. Para ello, introduzca las credenciales del Agente de autenticación o realice el procedimiento de recuperación (procedimiento de solicitud y respuesta).




Utilidad de restauración FDERT

## Creación de una Utilidad de restauración independiente

*Para crear el archivo ejecutable de la Utilidad de Restauración:*

1. En la ventana principal de la aplicación, haga clic en el botón **Soporte**.
2. En la ventana que se abre, haga clic en el botón **Restaurar dispositivo cifrado**.

   Se inicia la Utilidad de restauración de dispositivos cifrados.
3. Haga clic en el botón **Crear Utilidad de Restauración Independiente** en la ventana de la Utilidad de Restauración.
4. Guarde la Utilidad de restauración independiente en el equipo.

El archivo ejecutable de la Utilidad de restauración (fdert.exe) se guardará en la carpeta que haya seleccionado. Copie la Utilidad de restauración a un equipo en el que no se hayan instalado los componentes de cifrado de Kaspersky Endpoint Security. Esto evita que la unidad vuelva a cifrarse.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración residen en la memoria del equipo del usuario de forma no cifrada desde hace algún tiempo. Para reducir el riesgo de acceso no autorizado a tales datos, se le aconseja restaurar el acceso a los dispositivos cifrados en equipos de confianza.

## Recuperación de los datos almacenados en el disco duro

*Para restaurar el acceso a dispositivos cifrados con la Utilidad de Restauración:*

1. Ejecute el archivo fdert.exe (el archivo ejecutable de la Utilidad de restauración). Este archivo es creado por Kaspersky Endpoint Security.

2. En la ventana Utilidad de restauración, en la lista desplegable **Seleccionar dispositivo**, seleccione el dispositivo cifrado para el cual desea restaurar el acceso.

3. Haga clic en el botón **Analizar** para permitir que la utilidad defina cuál de las acciones debe realizar en el dispositivo: si se lo debe desbloquear o descifrar.

   Si el equipo tiene acceso a la funcionalidad del cifrado de Kaspersky Endpoint Security, la utilidad de restauración le solicita desbloquear el dispositivo. Si bien desbloquear el dispositivo no lo descifra, el dispositivo queda accesible directamente por estar desbloqueado. Si el equipo no tiene acceso a la funcionalidad del cifrado de Kaspersky Endpoint Security, la utilidad de restauración le solicita descifrar el dispositivo.

4. Si desea importar la información de diagnóstico, haga clic en el botón **Guardar diagnóstico**.

   La utilidad guardará un archivo comprimido, que contendrá los archivos con la información de diagnóstico.

5. Haga clic en el botón **Reparar MBR** si el diagnóstico del disco duro cifrado del sistema ha generado un mensaje sobre problemas relacionados con el registro de arranque maestro (MBR) del dispositivo.

   Reparar el registro de arranque maestro puede reducir el tiempo que requiere obtener la información necesaria para desbloquear o descifrar el dispositivo.

6. Haga clic en el botón **Desbloquear** o **Descifrar** según los resultados de diagnóstico.

7. Si desea utilizar una cuenta del Agente de autenticación para restaurar los datos, seleccione la opción **Usar la configuración de la cuenta del Agente de autenticación** e introduzca las credenciales del Agente de autenticación.

   Este método solo es posible al restaurar datos de un disco duro del sistema. Si el disco duro del sistema está dañado y se han perdido los datos de la cuenta del Agente de autenticación, debe obtener una clave de acceso del administrador de la red de área local corporativa para restaurar los datos de un dispositivo cifrado.

8. Si desea iniciar el procedimiento de recuperación, haga lo siguiente:

   a. Seleccione la opción **Especificar manualmente la clave de acceso del dispositivo**.

   b. Haga clic en el botón **Recibir clave de acceso** y guarde el archivo de solicitud de acceso (un archivo de extensión FDERTC) en el equipo.

   c. Envíe el archivo de solicitud de acceso al administrador de la red LAN corporativa.

   No cierre la ventana **Recibir clave de acceso del dispositivo** hasta que haya recibido la clave de acceso. Cuando esta ventana se abra nuevamente, no podrá aplicar la clave de acceso creada anteriormente por el administrador.

d. El administrador de la LAN corporativa creará y le enviará un archivo de acceso, cuya extensión será FDERTR. Guarde este archivo (consulte las instrucciones a continuación).

e. Descargue el archivo de acceso a través de la ventana **Recibir clave de acceso al dispositivo**.

9. Si necesita descifrar el dispositivo, deberá configurar algunas opciones adicionales:

- Especifique el área para descifrar:
  - Si desea descifrar todo el dispositivo, seleccione la opción **Descifrar todo el dispositivo**.
  - Si desea descifrar solo parte de los datos del dispositivo, seleccione la opción **Descifrar áreas individuales del dispositivo** y especifique los límites del área para descifrar.
- Seleccione la ubicación para escribir los datos descifrados:
  - Si desea que los datos del dispositivo original se vuelvan a escribir con los datos descifrados, anule la selección de la casilla de selección **Guardar datos descifrados en un archivo de imagen de disco**.
  - Si desea guardar los datos descifrados por separado de los datos cifrados originales, seleccione la casilla de selección **Guardar datos descifrados en un archivo de imagen de disco** y el botón **Examinar** para especificar la ruta donde desea guardar el archivo VHD.

10. Haga clic en **Aceptar**.

Se inicia el proceso de desbloqueo o descifrado del dispositivo.

Cómo crear un archivo de clave de acceso para archivos cifrados en la Consola de administración (MMC)

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Protección y cifrado de datos** → **Dispositivos cifrados**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el que necesite crear el archivo de clave de acceso. A continuación, en el menú contextual del dispositivo, seleccione **Obtener acceso al dispositivo en Kaspersky Endpoint Security para Windows (11.6.0)**.

   Si no sabe con seguridad a qué equipo corresponde el archivo de solicitud de acceso, en el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Protección y cifrado de datos** y luego, en el espacio de trabajo, haga clic en el vínculo **Obtener la clave de cifrado del dispositivo en Kaspersky Endpoint Security para Windows (11.6.0)**.

4. En la ventana que se abre, seleccione el algoritmo de cifrado que se deba usar: **AES256** o **AES56**.

   El algoritmo de cifrado depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución. Están disponibles tanto una variante de cifrado "fuerte" *(AES256)* como una de cifrado "ligero" *(AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

5. Haga clic en el botón **Examinar**. En la ventana que se abre, introduzca la ruta al archivo de solicitud de acceso (un archivo de extensión FDERTC) que recibió del usuario.
6. Haga clic en el botón **Abrir**.

Verá información sobre la solicitud del usuario. Kaspersky Security Center generará un archivo de clave. Envíele al usuario el archivo de clave de acceso generado. Puede para ello usar el correo electrónico. Si lo prefiere, guarde el archivo y transfiéralo por cualquier otro medio.

[Cómo crear un archivo de clave de acceso para archivos cifrados en Web Console]

1. En la ventana principal de Web Console, seleccione **Operaciones** → **Protección y cifrado de datos** → **Dispositivos cifrados**.

2. Active la casilla ubicada junto al nombre del equipo en el que se encuentren los datos a los que se necesite acceso.

3. Haga clic en el botón **Compartir dispositivo sin conexión**.

   Se inicia un asistente para otorgar acceso al dispositivo.

4. Siga las instrucciones del asistente para otorgar acceso al dispositivo:

   a. Seleccione el complemento de **Kaspersky Endpoint Security para Windows**.

   b. Seleccione el algoritmo de cifrado que se deba usar: **AES256** o **AES56**.

      El algoritmo de cifrado depende de qué biblioteca de cifrado AES está incluida en el paquete de distribución. Están disponibles tanto una variante de cifrado "fuerte" *(AES256)* como una de cifrado "ligero" *(AES56)*. La biblioteca de cifrado AES se instala junto con la aplicación.

   c. Haga clic en el botón **Seleccionar archivo** y seleccione el archivo de solicitud de acceso que le haya enviado el usuario (el archivo tendrá la extensión FDERTC).

   d. Haga clic en el botón **Guardar clave** e indique en qué carpeta se guardará el archivo de clave de acceso para los archivos cifrados (el archivo tendrá la extensión FDERTR).

Como resultado, podrá obtener la clave de acceso para los archivos cifrados, que deberá enviarle al usuario.

## Creación de un disco de rescate del sistema operativo

El disco de rescate del sistema operativo puede ser útil cuando no se puede acceder al disco duro cifrado por algún motivo y no se puede cargar el sistema operativo.

Puede cargar una imagen del sistema operativo Windows con el disco de rescate y restaurar el acceso al disco duro cifrado mediante la Utilidad de restauración incluida en la imagen del sistema operativo.

*Para crear un disco de rescate del sistema operativo:*

1. Cree un archivo ejecutable para la Utilidad de restauración de dispositivos cifrados.

2. Cree una imagen personalizada del entorno previo al arranque de Windows. Al crear la imagen personalizada del entorno previo al arranque de Windows, agregue el archivo ejecutable de la Utilidad de Restauración a la imagen.

3. Guarde la imagen personalizada del entorno previo a la instalación de Windows en un medio de inicio, como ser un CD o un disco extraíble.

   Consulte los archivos de ayuda de Microsoft si desea conocer las instrucciones para crear una imagen personalizada del entorno previo al arranque de Windows (por ejemplo, en el recurso Microsoft TechNet).

# 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>`.

Debe escapar los caracteres especiales en el comando. Para escapar &, |, (, ), <, >, ^, utilice el carácter ^ (por ejemplo, para usar el carácter `&`, escriba `^&`). Para escapar el carácter `%`, escriba `^%`.

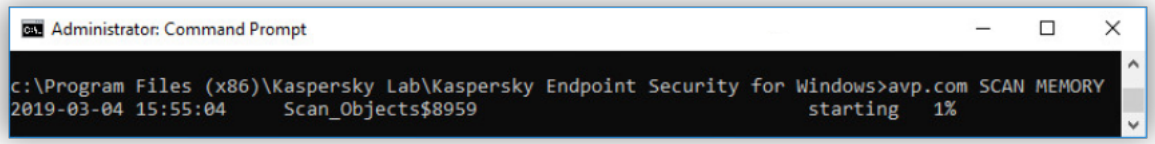
## Comando de AVP

*Para administrar Kaspersky Endpoint Security a través de la línea de comandos:*

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para ejecutar un comando, escriba lo siguiente:

```
avp.com <comando> [opciones]
```

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 [<alcance 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>]
```

| **Alcance del análisis** | |
|---|---|
| `<archivos` | Lista de archivos y carpetas, separados con espacios. Las rutas largas deben estar entre |

| | |
|---|---|
| para analizar> | comillas. Las rutas cortas (en formato de MS-DOS) no necesitan las comillas. Por ejemplo:<br>• `"C:\Archivos de programa (x86)\Carpeta de ejemplo"` (ruta larga).<br>• `C:\ARCHIV~2\CARPET~1` (ruta corta). |
| `/ALL` | Ejecutar la tarea *Análisis completo*. Kaspersky Endpoint Security analiza los siguientes objetos:<br>• Memoria del kernel<br>• Objetos cargados al iniciar el sistema operativo<br>• Sectores de inicio<br>• Copia de seguridad del sistema operativo<br>• Todos los discos duros y unidades extraíbles |
| `/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:<br>• `"C:\Archivos de programa (x86)\Carpeta de ejemplo"` (ruta larga).<br>• `C:\ARCHIV~2\CARPET~1` (ruta corta). |

| **Acción al detectar una amenaza** | |
|---|---|
| `/i0` | Informar. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos. |
| `/i1` | Desinfectar; bloquear si falla la desinfección. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas. |
| `/i2` | Desinfectar; eliminar si falla la desinfección. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.<br>Esta acción está seleccionada por defecto. |

| | |
|---|---|
| `/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 según su extensión. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión. |
| `/fi` | Archivos analizados según su formato. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares. |
| `/fa` | Todos los archivos. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones).<br>Esta es la configuración por defecto. |

| **Exclusiones de 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 archivo>` | No analizar los archivos que coincidan con la máscara de archivo especificada. Por ejemplo:<br>• Si utiliza la máscara `*.exe`, se excluirán del análisis las rutas a todos los archivos de extensión EXE.<br>• Si utiliza la máscara `ejemplo*`, se excluirán del análisis las rutas a todos los archivos de nombre EJEMPLO. |
| `-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 al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |
| `/iSwift=on\|off` | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS. |

| La configuración avanzada | |
|---|---|
| `/C:<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: `[<alcance 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 bases de datos y módulos de software de la aplicación

Ejecute la tarea de *Actualización*.

Sintaxis del comando

```
UPDATE [local] ["<origen de actualizaciones>"] [/R[A]:<archivo de informe>] [/C:<archivo de configuración de actualizaciones>]
```

| Configuración de la tarea de actualización | |
|---|---|
| `local` | Inicio de la tarea de *Actualización* que se creó automáticamente después de instalar la aplicación. Puede cambiar la configuración de la tarea *Actualización* en la interfaz de la aplicación local o en la consola de Kaspersky Security Center. Si esta opción no está configurada, Kaspersky Endpoint Security inicia la tarea *Actualización* con la configuración predeterminada o con la configuración especificada en el comando. Puede definir la configuración de la tarea Actualización de la siguiente manera: |

| | |
|---|---|
| | • `UPDATE` inicia la tarea de *Actualización* con la configuración predeterminada: el origen de actualizaciones está en los servidores de actualizaciones de Kaspersky, la cuenta es Sistema y demás configuraciones predeterminadas.<br>• `UPDATE local` inicia la tarea de *Actualización* que se creó automáticamente luego de la instalación (tarea predefinida).<br>• `UPDATE <configuración de actualización>` inicia la tarea de *Actualización* con la configuración establecida manualmente (que figura a continuación). |

| **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 el origen predeterminado: los servidores de actualizaciones 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. |

| **La 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 del 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. Seguimiento

Habilitar o deshabilitar la función de seguimiento. Los archivos de seguimiento quedarán guardados en el equipo mientras la aplicación esté instalada; cuando desinstale la aplicación, los archivos se eliminarán de forma permanente. Los archivos de seguimiento, excepto los del Agente de autenticación, se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\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 de los archivos de seguimiento. Valores disponibles:<br>• `100` (crítico). Solo mensajes sobre errores graves.<br>• `200` (alto). Mensajes sobre todos los errores, incluidos los graves.<br>• `300` (diagnóstico). Mensajes sobre todos los errores, además de las advertencias.<br>• `400` (importante). Todos los mensajes de error y de advertencia, así como otra información adicional.<br>• `500` (normal). Mensajes sobre todos los errores y advertencias, así como información detallada sobre el funcionamiento de la aplicación en modo normal (predeterminado).<br>• `600` (bajo). Todos los mensajes. |

| **La configuración avanzada** | |
|---|---|
| `all` | Ejecutar un comando con los parámetros `dbg`, `file` y `mem`. |
| `dbg` | Usar la función OutputDebugString y guardar el archivo de seguimiento. La función OutputDebugString le envía una cadena de caracteres al depurador de la aplicación para que se la muestre en pantalla. Para más detalles, visite el *sitio web de MSDN*. |
| `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 habilitar un componente de protección).

Sintaxis del comando

```
START <perfil> [/R[A]:<archivo de informe>]
```

| **Perfil** | |
|---|---|
| `<perfil>` | Nombre de perfil. Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Para ver la lista de perfiles disponibles, utilice el comando `HELP START`. |

| **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 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 habilitada. El usuario debe contar con los permisos **Deshabilitar componentes de protección** y **Deshabilitar componentes de control**.

Sintaxis del comando

```
STOP <perfil> /login=<nombre de usuario> /password=<contraseña>
```

| Perfil | |
|---|---|
| `<perfil>` | Nombre de perfil. Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Para ver la lista de perfiles disponibles, utilice el comando `HELP STOP`. |

| Autenticación | |
|---|---|
| `/login=<nombre de usuario> /password=<contraseña>` | Credenciales de cuenta de usuario con los permisos de Protección con contraseña requeridos. |

## STATUS. Estado del perfil

Mostrar en qué estado se encuentran los perfiles de la aplicación (por ejemplo, `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 Servicio de soporte técnico de Kaspersky.

Sintaxis del comando

```
STATUS [<perfil>]
```

## 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.) Para ver la lista de perfiles disponibles, ejecute el comando `HELP STATISTICS`.

Sintaxis del comando

```
STATISTICS <perfil>
```

## RESTORE. Restaurar archivos

De ser necesario, puede restaurar un archivo almacenado en Copias de seguridad a su carpeta original. Si en la ruta especificada ya existe un archivo con el mismo nombre, se agrega 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 habilitada. El usuario debe tener el permiso **Restaurar objetos de Copias de seguridad**.

El depósito *Copia de seguridad* contiene copias de respaldo de los archivos que se modifican o eliminan cuando se realiza una desinfección. Una *copia de seguridad* es una copia del archivo creada antes de desinfectar o eliminar el archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. Se conceden accesos limitados a esta carpeta al usuario cuya cuenta se utilizó para instalar Kaspersky Endpoint Security.

Kaspersky Endpoint Security no brinda la capacidad de configurar permisos de acceso de usuario a copias de seguridad de archivos.

Sintaxis del comando

```
RESTORE [/REPLACE] <nombre de archivo> /login=<nombre de usuario> /password=
<contraseña>
```

| La 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 Protección con contraseña 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>
```

| Perfil | |
|---|---|
| `<perfil>` | Nombre de perfil. Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Para ver la lista de perfiles disponibles, utilice el comando `HELP EXPORT`. |

| Archivo para la exportación | |
|---|---|
| `<nombre` | Nombre del archivo en el que se guardarán los ajustes de configuración exportados. Los |

| | |
|---|---|
| de archivo> | 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 ajustes de la aplicación

Importar en Kaspersky Endpoint Security los ajustes de configuración que se guardaron en un archivo creado con el comando `EXPORT`.

Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada. El usuario debe tener el permiso **Configurar los parámetros de la aplicación**.

Sintaxis del comando

```
IMPORT <nombre de archivo> /login=<nombre de usuario> /password=<contraseña>
```

| **Archivo para importar** | |
|---|---|
| <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. |

| **Autenticación** | |
|---|---|
| /login=<nombre de usuario> /password=<contraseña> | Credenciales de cuenta de usuario con los permisos de Protección con contraseña requeridos. |

Ejemplo:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

## ADDKEY. Aplicar un archivo de clave.

Aplicar un archivo de clave para activar Kaspersky Endpoint Security. Si la aplicación ya está activada, la clave se agregará como clave de reserva.

Sintaxis del comando

```
ADDKEY <nombre de archivo> /login=<nombre de usuario> /password=<contraseña>
```

| Archivo de clave | |
|---|---|
| `<nombre de archivo>` | Nombre del archivo de clave. |

| Autenticación | |
|---|---|
| `/login=<nombre de usuario> /password=<contraseña>` | Credenciales de una cuenta de usuario. Estos datos solo se necesitan si la protección con contraseña está habilitada. |

Ejemplo:
`avp.com ADDKEY file.key`

## LICENSE. Administración de licencias

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 habilitada. El usuario debe tener el permiso **Eliminar una clave**.

Sintaxis del comando

```
LICENSE <operación> [/login=<nombre de usuario> /password=<contraseña>]
```

| Operación | |
|---|---|
| `/ADD <nombre de archivo>` | Aplicar un archivo de clave para activar Kaspersky Endpoint Security. Si la aplicación ya está activada, la clave se agregará 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 agregará como clave de reserva. |
| `/REFRESH <nombre de archivo>` | Renovar la licencia usando un archivo de clave. Como resultado, se agregará una clave de reserva. Se activa cuando caduca la licencia. El comando no se puede utilizar para agregar una clave activa. |
| `/REFRESH <código de activación>` | Renovar la licencia usando un código de activación. Como resultado, se agregará una clave de reserva. Se activa cuando caduca la licencia. El comando no se puede utilizar para agregar una clave activa. |
| `/DEL /login=<nombre de usuario> /password= <contraseña>` | Eliminar una clave de licencia. La clave de reserva también se eliminará. |

| Autenticación | |
|---|---|
| `/login=<nombre de usuario> /password=<contraseña>` | Credenciales de cuenta de usuario con los permisos de Protección con contraseña requeridos. |

Ejemplo:

- `avp.com LICENSE /ADD file.key`

- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

## RENEW. Adquisición de una licencia

Abrir el sitio web de Kaspersky para comprar o renovar una licencia.

## PBATESTRESET. Restablecer los resultados de la comprobación del disco antes de cifrarlo

Restablecer los resultados de la prueba de compatibilidad con el cifrado de disco completo (FDE), el cual puede estar basado en las tecnologías Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker.

Antes de aplicar el cifrado de disco completo, la aplicación realiza una serie de pruebas para verificar que el equipo pueda, efectivamente, cifrarse. Cuando se determina que el equipo no es compatible con el cifrado de disco completo, Kaspersky Endpoint Security deja constancia de la incompatibilidad. Si se intenta realizar una nueva operación de cifrado, la aplicación omite la verificación y simplemente advierte que el cifrado no puede aplicarse. Por ello, ante un cambio en el hardware del equipo, los resultados de la verificación deben descartarse y se debe volver a comprobar si el disco duro es compatible con las tecnologías Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker.

## 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 habilitada. El usuario debe tener el permiso **Salir de la aplicación**.

Sintaxis del comando

```
EXIT /login=<nombre de usuario> /password=<contraseña>
```

## EXITPOLICY. Deshabilitar una directiva

Deshabilitar una directiva de Kaspersky Security Center en el equipo. Todos los parámetros de Kaspersky Endpoint Security, incluidos los que tuvieran un candado cerrado (🔒) en la directiva, quedarán desbloqueados y podrán configurarse.

Para ejecutar este comando, es necesario que la protección con contraseña esté habilitada. El usuario debe tener el permiso **Deshabilitar la directiva de Kaspersky Security Center**.

Sintaxis del comando

```
EXITPOLICY /login=<nombre de usuario> /password=<contraseña>
```

## STARTPOLICY. Habilitar una directiva

Habilitar una directiva de Kaspersky Security Center en el equipo. Los parámetros de la aplicación tomarán los valores que indique la directiva.

## DISABLE. Deshabilitar la protección

Deshabilitar el componente Protección contra archivos peligrosos 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

Habilitar o deshabilitar la detección de spyware. De manera predeterminada, la detección de spyware está habilitada.

Sintaxis del comando

```
SPYWARE on|off
```

## MDRLICENSE. Activación de MDR

Permite realizar 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. Encontrará el archivo BLOB en el archivo ZIP del archivo de configuración de MDR. Para obtener el archivo ZIP, utilice la consola de Kaspersky Managed Detection and Response. Para más información sobre el archivo BLOB, consulte la *guía de ayuda de Kaspersky Managed Detection and Response*.

Para realizar operaciones con el archivo BLOB, necesitará privilegios de administrador. También será necesario que los ajustes de Managed Detection and Response puedan editarse ( ) en la directiva.

Sintaxis del comando

```
MDRLICENSE <operación> [/login=<nombre de usuario> /password=<contraseña>]
```

| Operación | |
|---|---|
| `/ADD <nombre` | Aplicar el archivo de configuración BLOB para llevar a cabo la integración con Kaspersky Managed Detection and Response (archivo de formato P7). Solo se puede aplicar un único archivo BLOB. Si el equipo ya tiene un archivo BLOB, se lo reemplazará. |

| | |
|---|---|
| de archivo> | |
| /DEL | Eliminar el archivo de configuración BLOB. |

| Autenticación | |
|---|---|
| /login=<nombre de usuario> /password=<contraseña> | Credenciales de cuenta de usuario con los permisos de Protección con contraseña requeridos. |

Ejemplo:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

## KSN. Alternar entre KSN Global y KSN Privada

Permite seleccionar la solución de Kaspersky Security Network que se usará para determinar la reputación de los archivos y los 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*. A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky Security Network, así como a otras clases de información estadística, sin enviar información de sus equipos a KSN. 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 de archivo>

| | |
|---|---|
| **Archivo de configuración de KSN Privada** | |
| <nombre de archivo> | Nombre del archivo —de extensión PKCS7 o PEM— que contiene la configuración del servidor proxy de KSN. |

Ejemplo:

avp.com KSN /global

avp.com KSN /private C:\ksn_config.pkcs7

## Comando de KESCLI

Los comandos de KESCLI le permiten recibir información sobre el estado de la protección del equipo mediante el componente OPSWAT, y le permiten realizar tareas estándar como análisis antivirus y actualizaciones de la base de datos.

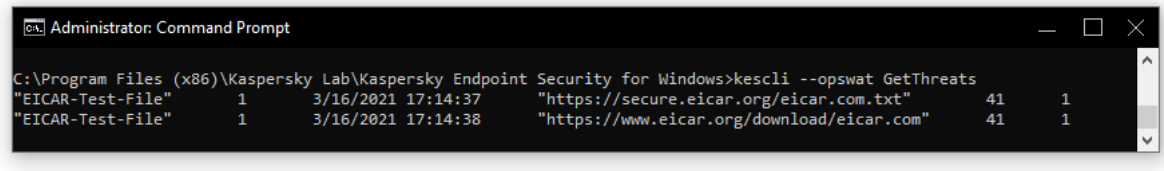
Puede ver la lista de comandos de KESCLI a través del comando `--ayuda` o a través del comando abreviado `-h`.

*Para administrar Kaspersky Endpoint Security a través de la línea de comandos:*

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Endpoint Security.
3. Para ejecutar un comando, escriba lo siguiente:

```
kescli <comando> [opciones]
```

Kaspersky Endpoint Security ejecutará el comando especificado (consulte la siguiente imagen).




Administración de la aplicación desde la línea de comandos

## Análisis. Análisis antivirus

Ejecutar la tarea de análisis antivirus.

Sintaxis del comando

```
--opswat Scan <alcance del análisis> <acción al detectar una amenaza>
```

Puede verificar el estado de la finalización de la tarea de *Análisis completo* a través del comando `GetScanState` y ver la fecha y la hora en que se completó el análisis a través del comando `GetLastScanTime`.

| Alcance del análisis | |
|---|---|
| `<archivos para analizar>` | `;`: lista de archivos y carpetas separados. Por ejemplo: `C:\Program Files (x86)\Example Folder`. |

| Acción al | |
|---|---|

| detectar una amenaza | |
|---|---|
| `0` | Informar. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos. |
| `1` | Desinfectar; eliminar si falla la desinfección. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.<br>Esta acción está seleccionada por defecto. |

Ejemplo:

```
kescli --opswat Análisis C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

## GetScanState. Estado de la finalización del análisis

Reciba la información sobre el estado de la finalización de la tarea de *Análisis completo*:

- `1`: el análisis está en progreso.
- `0`: el análisis no se está ejecutando.

Sintaxis del comando

```
--opswat GetScanState
```

Ejemplo:

```
kescli --opswat GetScanState
```

## GetLastScanTime. Determinación de la hora de finalización del análisis

Reciba la información sobre la fecha y la hora de la última finalización de la tarea de *Análisis completo*.

Sintaxis del comando

```
--opswat GetLastScanTime
```

Ejemplo:

```
kescli --opswat GetLastScanTime
```

## GetThreats. Obtención de datos sobre las amenazas detectadas

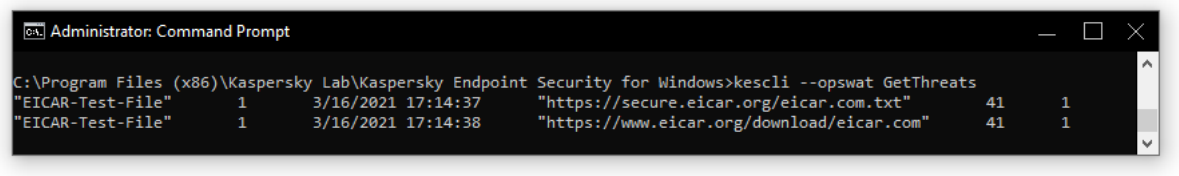
Reciba una lista de amenazas detectadas (*Informe de amenazas*). Este informe contiene información sobre las amenazas y la actividad de los virus durante los últimos 30 días anteriores a la creación del informe.

Sintaxis del comando

```
--opswat GetThreats
```

Cuando se ejecute 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>`




Administración de la aplicación desde la línea de comandos

| Tipo de objeto | |
|---|---|
| `0` | Desconocido (`Desconocido`). |
| 1 | Virus (`Virware`). |
| 2 | Programas troyanos (`Trojware`). |
| 3 | Programa malintencionado (`Malware`). |
| 4 | Programas de publicidad (`Adware`). |
| 5 | Programas de marcador automático (`Pornware`). |
| 6 | Aplicaciones que podrían utilizarse por un ciberdelincuente para hacer daño en el equipo o los datos del usuario (`Riskware`). |
| 7 | Ejecutables comprimidos que puedan tener código malicioso oculto (`Comprimido`). |
| 20 | Objetos desconocidos (`Xfiles`). |
| 21 | Aplicaciones conocidas (`Software`). |
| 22 | Archivos ocultos (`Oculto`). |
| 23 | Aplicación que requiere atención (`Pupware`). |
| 24 | Comportamiento irregular (`Anomalía`). |
| 30 | No determinado (`No detectado`). |
| 40 | Anuncios publicitarios (`Anuncio`). |
| 50 | Ataque de red (`Ataque`). |
| 51 | Acceso del registro (`Registro`). |
| 52 | Actividad sospechosa (`Sospecha`). |
| 60 | Vulnerabilidades (`Vulnerabilidad`). |
| 70 | Suplantación de identidad (`phishing`). |
| 80 | Archivos adjuntos de correo electrónico no deseados (`Archivos adjuntos`). |
| 90 | Malware detectado por Kaspersky Security Network (`Urgente`). |

| | |
|---|---|
| 100 | Vínculo desconocido (URL sospechosa). |
| 110 | Otro malware (Comportamiento). |

| Acción al detectar una amenaza | |
|---|---|
| 0 | Desconocido (desconocido). |
| 1 | Amenaza corregida (aceptar). |
| 2 | El objeto estaba infectado y no ha sido desinfectado (infectado). |
| 5 | El objeto está en un archivo y no ha sido desinfectado (archivo). |
| 9 | El objeto ha sido desinfectado (desinfectado). |
| 10 | El objeto no ha sido desinfectado (no desinfectado). |
| 11 | Se eliminó el objeto (eliminado). |
| 13 | Se creó una copia de seguridad del objeto (copia de seguridad). |
| 15 | Se movió el objeto al depósito de copias 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 | El usuario movió el objeto al depósito de copias de seguridad (agregado por el usuario). |
| 30 | El objeto se agregó a las exclusiones (agregado a las exclusiones). |
| 31 | Se movió el objeto al depósito de copias 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 (no se encontró). |
| 41 | No se puede resolver la amenaza (no se puede resolver). |
| 42 | Se restauró el objeto (restaurado). |
| 43 | El objeto se creó como resultado de una actividad de amenaza (producido por una amenaza). |
| 44 | El objeto se restauró al reiniciar el equipo (restaurar al reiniciar). |
| 0xffffffff | El objeto no se procesó (eliminado). |

| Nivel de peligro de la amenaza | |
|---|---|
| 0 | Desconocido |
| 1 | Alto |
| 2 | Análisis medio |
| 4 | Bajo |
| 8 | Información (menor que *Bajo*) |

## UpdateDefinitions. Actualización de bases de datos y módulos de software de la aplicación

Ejecute la tarea de *Actualización*. Kaspersky Endpoint Security usa la fuente predeterminada: servidores de actualización de Kaspersky.

Sintaxis del comando

```
--opswat UpdateDefinitions
```

Puede ver la fecha y la hora de la última tarea de *Actualización* finalizada a través del comando `GetDefinitionsetState`.

Ejemplo:

```
kescli --opswat UpdateDefinitions
```

## GetDefinitionState. Determinación de la hora de finalización de la actualización

Reciba la información sobre la fecha y la hora de la última finalización de la tarea de *Actualización*.

Sintaxis del comando

```
--opswat GetDefinitionState
```

Ejemplo:

```
kescli --opswat GetDefinitionState
```

## EnableRTP. Habilitación de la protección

Habilite componentes de protección de Kaspersky Endpoint Security en el equipo: Protección contra amenazas de archivos, Protección contra amenazas web, Protección contra amenazas de correo, Protección contra amenazas de red, Prevención contra intrusos.

Sintaxis del comando

```
--opswat EnableRTP
```

Puede verificar el estado del funcionamiento de la Protección contra amenazas de archivo a través del comando `GetRealTimeProtectionState`.

Ejemplo:

```
kescli --opswat EnableRTP
```

## GetRealTimeProtectionState. Estado de la Protección contra amenazas de archivos

Reciba la información sobre el estado del funcionamiento del componente de Protección contra amenazas de archivos:

- `1`: el componente está habilitado.
- `0`: el componente está deshabilitado.

Sintaxis del comando

```
--opswat GetRealTimeProtectionState
```

Ejemplo:
`kescli --opswat GetRealTimeProtectionState`

## Versión. Identificación de la versión de la aplicación

Identifique la versión de Kaspersky Endpoint Security para Windows.

Sintaxis del comando

```
--Versión
```

También puede utilizar el comando abreviado `-v`.

Ejemplo:
`kescli -v`

## 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'`. De forma complementaria, Kaspersky Endpoint Security puede mostrar un código como `error=8947906D` (consulte la siguiente tabla).

Códigos de error

| Código de error | Descripción |
|---|---|
| `09479001` | 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 de clave dañado. |
| 89479006 | Licencia caducada o clave de licencia caducada. |
| 89479007 | No se ha especificado el archivo de clave. |
| 89479008 | No se puede aplicar el archivo de 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 de clave no válido para agregar una clave de reserva. |
| 89479012 | Error del sistema. |
| 89479013 | Lista de bloqueo de claves 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 de 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 agregar una clave de prueba nuevamente. |
| 8947901A | Archivo de clave dañado. |
| 8947901B | La firma digital no existe, está dañada o no coincide con la firma digital de Kaspersky. |
| 8947901C | No se puede agregar una clave si la licencia no comercial correspondiente ha caducado. |
| 8947901E | La fecha de creación o uso del archivo de clave no es válida. Compruebe que la fecha del sistema sea correcta. |
| 8947901F | No se puede agregar una clave para la licencia de prueba: ya hay otra clave que está activa para la licencia de prueba. |
| 89479020 | Falta la lista de bloqueo de claves 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 de clave no válido para agregar 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, comuníquese con su proveedor de Internet. |

| | |
|---|---|
| 89479026 | Error en la respuesta del servidor de activación. |
| 89479027 | No se pude 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 sea correcta. |
| 8947902A | El archivo de clave no es compatible con esta aplicación o la licencia ha caducado. No se puede activar Kaspersky Endpoint Security usando el archivo de clave de otra aplicación. |
| 8947902B | Error al recibir el archivo de clave. Se escribió un código de activación incorrecto. |
| 8947902C | El servidor de activación devolvió el error 400. |
| 8947902D | El servidor de activación devolvió el error 401. |
| 8947902E | El servidor de activación devolvió el error 403. |
| 8947902F | El servidor de activación devolvió el error 404. |
| 89479030 | El servidor de activación devolvió el error 405. |
| 89479031 | El servidor de activación devolvió el error 406. |
| 89479032 | Se requiere autenticación para usar el servidor proxy. Revise la configuración de red. |
| 89479033 | Se agotó el tiempo de espera para la solicitud. |
| 89479034 | El servidor de activación devolvió el error 409. |
| 89479035 | El servidor de activación devolvió el error 410. |
| 89479036 | El servidor de activación devolvió el error 411. |
| 89479037 | El servidor de activación devolvió el error 412. |
| 89479038 | El servidor de activación devolvió el error 413. |
| 89479039 | El servidor de activación devolvió el error 414. |
| 8947903A | El servidor de activación devolvió el error 415. |
| 8947903C | Error interno del servidor. |
| 8947903D | Funcionalidad no compatible. |
| 8947903E | La respuesta de la puerta de vínculo no es válida. Revise la configuración de red. |
| 8947903F | Servicio no disponible (error 503 de HTTP). |
| 89479040 | Se agotó el tiempo de espera para la respuesta de la puerta de vínculo. Revise la configuración 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 de clave en el servidor de activación. |
| 8947904E | La clave está bloqueada. |
| 8947904F | Error interno del servidor de activación. |
| 89479050 | Datos insuficientes en la solicitud de activación. |
| 89479053 | 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 superó 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 activa con una clave caducada. |
| 89479067 | No se puede agregar una clave de reserva que caduque 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 correspondientes a las claves activa y de reserva no coinciden. |
| 8947906D | Componente no compatible con la licencia. |
| 8947906E | No se puede agregar una clave de suscripción como clave de reserva. |
| 89479213 | Error general de capa de transporte. |
| 89479214 | No se pudo establecer conexión con el servidor de activación. |
| 89479215 | Formato de URL no válido. |
| 89479216 | No se pudo convertir la dirección del servidor proxy. |
| 89479217 | No se pudo convertir la dirección del servidor. Verifique la configuración de su conexión a Internet. |
| 89479218 | No se pudo establecer conexión con el servidor de activación o el servidor proxy. |
| 89479219 | Acceso remoto denegado. |
| 8947921A | Se agotó 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 envió un código de activación incorrecto al servidor. |
| 89479408 | El código de activación no es válido para Kaspersky Endpoint Security. No se puede activar Kaspersky Endpoint Security usando el archivo de clave de aplicación desconocida. |
| 89479409 | La solicitud no contiene un código de activación. |
| 8947940B | Licencia caducada (de acuerdo con la información del servidor de activación). |
| 8947940C | Se superó 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 corresponde 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 necesita acceso adicional al servidor de activación. |
| 89479413 | El servidor de activación devolvió el error 643. |
| 89479414 | El servidor de activación devolvió el error 644. |
| 89479415 | El servidor de activación devolvió el error 645. |
| 89479416 | El servidor de activación devolvió el error 646. |
| 89479417 | 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 devolvió una lista de reenvío vacía. |

# Apéndice. Perfiles de la aplicación

Un *perfil* es un componente, tarea o característica de Kaspersky Endpoint Security. Los perfiles permiten administrar la aplicación desde la línea de comandos. Puede usarlos para ejecutar los comandos `START`, `STOP`, `STATUS`, `STATISTICS`, `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 vía 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 contra amenazas de red.
- `IntegrityCheck` – Comprobación de integridad.
- `Mail_Monitoring` o `EM` – Protección contra amenazas de 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 contra amenazas web.
- `WebControl` – Control web.

Kaspersky Endpoint Security también es compatible con los perfiles de servicio. Puede necesitar este tipo de perfil si en alguna oportunidad se comunica con el Servicio de soporte técnico de Kaspersky.

# Uso de la API REST para administrar la aplicación

Si lo desea, puede utilizar una solución desarrollada por un tercero para configurar los ajustes de Kaspersky Endpoint Security, realizar análisis, actualizar las bases de datos antivirus y llevar a cabo otras tareas. La API de Kaspersky Endpoint Security se ha diseñado para ello. La API REST de Kaspersky Endpoint Security funciona sobre el protocolo HTTP y consiste de una serie de métodos de solicitud-respuesta. Gracias a ello, Kaspersky Endpoint Security puede administrarse a través de soluciones de terceros, y no únicamente con la interfaz local de la aplicación o mediante la Consola de administración de Kaspersky Security Center.

Si comienza a utilizar la API REST, deberá instalar Kaspersky Endpoint Security con las opciones necesarias para permitir el uso de la API REST. El cliente de REST que utilice deberá estar instalado en el mismo equipo que Kaspersky Endpoint Security.

Para garantizar que Kaspersky Endpoint Security y el cliente de REST interactúen en forma segura, haga lo siguiente:

- Configure la protección del cliente de REST para evitar accesos sin autorización según las recomendaciones del desarrollador del cliente de REST. Configure la protección de la carpeta del cliente de REST para evitar la escritura con la ayuda de la lista de control de acceso discrecional (LCAD).
- Para ejecutar el cliente de REST, utilice una cuenta diferente con derechos de administrador. Rechace el inicio de sesión interactivo al sistema para esta cuenta.

El acceso a la API REST es a través de http://127.0.0.1 o http://localhost. La API REST no puede utilizarse para administrar Kaspersky Endpoint Security en forma remota.

ABRIR LA DOCUMENTACIÓN DE LA API REST

# Habilitar el uso de la API REST al instalar la aplicación

Si desea administrar la aplicación a través de la API REST, deberá habilitar la compatibilidad con dicha API al instalar Kaspersky Endpoint Security. Si opta por utilizar la API REST, no podrá administrar Kaspersky Endpoint Security a través de Kaspersky Security Center.

*Para instalar Kaspersky Endpoint Security con las opciones necesarias para usar la API REST:*

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Vaya a la carpeta en la que se encuentre el paquete de distribución de Kaspersky Endpoint Security (versión 11.2.0 o posterior).
3. Instale Kaspersky Endpoint Security con los siguientes parámetros:
   - `RESTAPI=1`
   - `RESTAPI_User=<Nombre de usuario>`

     Nombre de usuario que se utilizará para administrar la aplicación a través de la API REST. El nombre de usuario debe especificarse en formato `<DOMINIO>\<NombreDeUsuario>` (por ejemplo, `RESTAPI_User=EMPRESA\Administrador`). La cuenta que defina aquí será la única que podrá administrar la aplicación con la API REST. El uso de la API REST está limitado a un único usuario.
   - `RESTAPI_Port=<Puerto>`

Puerto que se utilizará para intercambiar datos. Este parámetro es opcional. El puerto predeterminado es el 6782.

- `AdminKitConnector=1`

  Permitir que la aplicación se administre a través de un sistema de administración. Esta posibilidad está habilitada por defecto.

Los parámetros para utilizar la API REST también se pueden definir en el archivo setup.ini.

Los parámetros para utilizar la API REST únicamente se pueden definir al momento de instalar la aplicación. No es posible modificarlos una vez que la aplicación está instalada. Si necesita realizar algún cambio, desinstale Kaspersky Endpoint Security y reinstale el programa con los nuevos parámetros de la API REST.

Ejemplo:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=EMPRESA\Administrador /s
```

Como resultado, podrá utilizar la API REST para administrar la aplicación. Para verificar que todo funcione correctamente, envíe una solicitud GET para ver la documentación de la API REST.

Ejemplo:

```
GET http://localhost:6782/kes/v1/api-docs
```

## Uso de la API

La característica de protección con contraseña no puede utilizarse para restringir la capacidad de acceder a la aplicación con la API REST. Por ejemplo, no es posible impedir que una persona utilice la API REST para deshabilitar la protección. Por el contrario, la API REST sí puede utilizarse para configurar la protección con contraseña y limitar el acceso de los usuarios a la interfaz local de la aplicación.

Para administrar la aplicación a través de la API REST, deberá ejecutar un cliente de REST con la cuenta especificada al habilitar el uso de esta API durante la instalación de la aplicación. El uso de la API REST está limitado a un único usuario.

ABRIR LA DOCUMENTACIÓN DE LA API REST

El proceso para administrar la aplicación a través de la API REST se divide en los siguientes pasos:

1. Obtener los valores de configuración vigentes en la aplicación. Para ello, envíe una solicitud GET.

   Ejemplo:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. La aplicación enviará una respuesta con la estructura y los valores de configuración. Kaspersky Endpoint Security admite los formatos XML y JSON.

   Ejemplo:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   ```

```
"enabled": true
}
```

3. Modificar la configuración de la aplicación. Para ello, envíe una solicitud POST. Utilice la estructura de configuración que obtuvo en la respuesta a la solicitud GET inicial.

   Ejemplo:

   ```
   POST http://localhost:6782/kes/v1/settings/ExploitPrevention
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. La aplicación introducirá los cambios de configuración solicitados y enviará una respuesta con la configuración resultante.

# Fuentes de información acerca 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 vínculo a la tienda en línea. Allí podrá comprar o renovar la aplicación.

## Página de Kaspersky Endpoint Security en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico.

En la página de Kaspersky Endpoint Security de la Base de conocimientos, 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 Servicio de soporte técnico.

## Discusión 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.

Allí puede ver temas existentes, publicar sus propios comentarios y crear temas de debate nuevos.

# Contacto con el Servicio de soporte técnico

Si no puede encontrar una solución a su problema en la documentación o en ninguna de las fuentes de información sobre Kaspersky Endpoint Security, le recomendamos que se ponga en contacto con Soporte técnico. Soporte técnico responderá sus preguntas acerca de la instalación y el uso de Kaspersky Endpoint Security.

Kaspersky se compromete a brindar asistencia técnica para Kaspersky Endpoint Security a lo largo de su ciclo de vida (el cual se detalla en esta página). Antes de ponerse en contacto con el Servicio de soporte técnico, lea las reglas del soporte técnico.

Puede comunicarse con el Servicio de soporte técnico de las siguientes maneras:

- Visitando el sitio web del soporte técnico
- Enviando una solicitud al Servicio de soporte técnico de Kaspersky por medio del portal de Kaspersky CompanyAccount.

Después de informar su problema a los especialistas del Servicio de soporte técnico de Kaspersky, posiblemente le soliciten que cree un *archivo de seguimiento*. Este archivo de seguimiento le permite seguir paso a paso el proceso de ejecución de los comandos de la aplicación, además de determinar en qué etapa de la operación se produjo un error.

Es posible que los especialistas del Servicio de soporte técnico también le soliciten información adicional sobre el sistema operativo, los procesos que se están ejecutando en el equipo, los informes detallados sobre el funcionamiento de los componentes de las aplicaciones.

Mientras ejecuta un diagnóstico, los representantes del Servicio de soporte técnico pueden pedirle que cambie la configuración de la aplicación por medio de las siguientes acciones:

- Activar una función que permitirá recibir información de diagnóstico extendida.
- Realizar pequeños ajustes en la configuración de los componentes usando elementos que no están disponibles en la interfaz de usuario estándar.
- Cambiar opciones relativas al almacenamiento de la información de diagnóstico.
- Configurar la intercepción y el registro del tráfico de red.

Los expertos del Servicio de soporte técnico le darán toda la información que necesitará para realizar estas operaciones (descripción de la secuencia de pasos, parámetros que se deben modificar, archivos de configuración, secuencias de comandos, funcionalidad adicional de la línea de comandos, módulos de depuración, utilidades con fines especiales, etc.). También le informarán del alcance de los datos utilizados con fines de depuración. La información de diagnóstico extendida se guarda en el equipo del usuario. Los datos no se transmiten automáticamente a Kaspersky.

Las operaciones mencionadas deben llevarse a cabo solamente bajo la supervisión de especialistas del Servicio de soporte técnico siguiendo sus instrucciones. Los cambios no supervisados en la configuración de aplicaciones realizados de formas diferentes a las descritas en la Guía del administrador o en las instrucciones de los especialistas del Servicio de soporte técnico pueden ralentizar o dañar el sistema operativo, afectar la seguridad del equipo o poner en riesgo la disponibilidad e integridad de los datos que deben procesarse.

# Contenido y almacenamiento de archivos de rastreo

Usted tiene la responsabilidad personal de garantizar que los datos almacenados en su equipo se mantengan protegidos. En particular, es responsable de controlar y restringir el acceso a esta información hasta que se la envíe a Kaspersky.

Los archivos de rastreo se almacenan en su equipo mientras la aplicación está en uso y se eliminan de forma permanente cuando se desinstala la aplicación.

Los archivos de seguimiento, excepto los del Agente de autenticación, se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces.

El nombre de los archivos de seguimiento sigue este formato: `KES<número de versión de servicio_fechaXX.XX_horaXX.XX_pidXXX.><tipo de archivo de seguimiento>.log`.

Puede ver los datos guardados en los archivos de rastreo.

Todos los archivos de rastreo tienen los siguientes datos comunes:

- Hora del evento.
- Número del hilo de ejecución.

  El archivo de seguimiento del Agente de autenticación no contiene esta información.

- Componente de la aplicación que causó el evento.
- Gravedad del evento (evento informativo, advertencia, evento crítico, error).
- Una descripción del evento que involucra la ejecución del comando por un componente de la aplicación y el resultado de la ejecución de ese comando.

Kaspersky Endpoint Security guarda las contraseñas de usuario en un archivo de seguimiento solo en forma cifrada.

## Contenido de los archivos de rastreo SRV.log, GUI.log, y ALL.log

Los archivos de rastreo `SRV.log`, `GUI.log`, y `ALL.log` pueden almacenar la siguiente información además de los datos generales:

- Datos personales, como apellido, nombre de pila y segundo nombre, si esos datos se incluyen en la ruta a los archivos en el equipo local.
- Datos sobre el hardware instalado en el equipo (por ejemplo, datos de la BIOS o del firmware UEFI). Esta información se guarda en los archivos de seguimiento cuando se utiliza la función de cifrado de disco de Kaspersky.

- El nombre de usuario y la contraseña si se transmitieron en forma abierta. Estos datos se pueden registrar en los archivos de rastreo durante el análisis de tráfico de Internet.
- El nombre de usuario y la contraseña si están contenidos en los encabezados HTTP.
- El nombre de la cuenta de Microsoft Windows si el nombre de cuenta se incluye en el nombre del archivo.
- Su dirección de correo electrónico o una dirección web que contenga el nombre de su cuenta y contraseña si están contenidos en el nombre del objeto detectado.
- Los sitios web que visita y se redirige desde esos sitios. Estos datos se escriben en los archivos de rastreo cuando la aplicación analiza sitios web.
- Dirección del servidor proxy, nombre del equipo, puerto, dirección IP y nombre de usuario para iniciar sesión en el servidor proxy. Estos datos se escriben en los archivos de rastreo si la aplicación utiliza un servidor proxy.
- Direcciones IP remotas con las que su equipo estableció conexiones.
- Sujeto del mensaje, identificador, nombre del remitente y dirección del sitio web del remitente del mensaje en una red social. Estos datos se escriben en los archivos de rastreo si está activado el componente Control Web.
- Datos sobre el tráfico de red. Esta información se guarda en los archivos de seguimiento cuando se han habilitado los componentes de monitoreo del tráfico (por ejemplo, Control web).
- Datos recibidos de los servidores de Kaspersky (por ejemplo, la versión de las bases de datos antivirus).
- Estados y datos operativos de los componentes de Kaspersky Endpoint Security.
- Datos sobre las actividades del usuario en la aplicación.
- Eventos del sistema operativo.

## Contenido de los archivos de seguimiento HST.log, BL.log, Dumpwriter.log, WD.log y AVPCon.dll.log

Además de los datos generales, el archivo de seguimiento `HST.log` contiene información sobre la ejecución de una tarea de actualización de la base de datos y del módulo de la aplicación.

Además de los datos generales, el archivo de seguimiento `BL.log` contiene información sobre los eventos que ocurrieron durante la operación de la aplicación, como así también de los datos necesarios para la resolución de problemas de errores de la aplicación. El archivo se crea si la aplicación se inicia con el parámetro avp.exe –bl.

Además de los datos generales, el archivo de seguimiento `Dumpwriter.log` contiene información del servicio necesaria para la resolución de errores que ocurren cuando se escribe el archivo de volcado de la aplicación.

Además de los datos generales, el archivo de seguimiento `WD.log` contiene información sobre los eventos que ocurrieron durante el funcionamiento del servicio avpsus, incluyendo los eventos de actualización de módulos de la aplicación.

Además de los datos generales, el archivo de seguimiento `AVPCon.dll.log` contiene información sobre los eventos que ocurrieron durante la operación del módulo de conectividad de Kaspersky Security Center.

## Contenido de los archivos de seguimiento del rendimiento

El nombre de los archivos de seguimiento del rendimiento tiene este formato: `KES<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 del archivo de seguimiento del componente Protección vía AMSI

Además de los datos generales, el archivo de seguimiento AMSI.log contiene información sobre los resultados del análisis realizado en solicitudes de aplicaciones de terceros.

## Contenidos de los archivos de seguimiento del componente Protección contra amenazas de correo

El archivo de seguimiento `mcou.OUTLOOK.EXE.log` puede contener partes de mensajes de correo electrónico, incluidas las direcciones de correo electrónico, además de datos generales.

## Contenidos de los archivos de seguimiento del componente Análisis desde menú contextual

El archivo de seguimiento `shellex.dll.log` contiene información sobre la finalización de la tarea de análisis y los datos requeridos para depurar la aplicación, además de información general.

## Contenido de los archivos de seguimiento del complemento web de la aplicación

Los archivos de seguimiento del complemento web de la aplicación se almacenan en el equipo en el que se ha instalado Kaspersky Security Center 12 Web Console, dentro de la carpeta Archivos de programa\Kaspersky Lab\Kaspersky Security Center Web Console 12\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 de Internet (servidor proxy).
- Nombre de usuario y contraseña para la tarea *Cambiar componentes de la aplicación*.
- Credenciales de cuentas y rutas especificadas en las propiedades de las directivas y de las tareas de Kaspersky Endpoint Security.

### Contenido del archivo de seguimiento del Agente de autenticación

El archivo de seguimiento del Agente de autenticación se guarda en la carpeta System Volume Information y tiene el siguiente nombre: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Además de los datos generales, el archivo de seguimiento del Agente de autenticación contiene información sobre el funcionamiento del Agente de autenticación y las acciones realizadas por el usuario con el Agente de autenticación.

## Seguimiento de la aplicación

Los *archivos de seguimiento de la aplicación* contienen un registro detallado de las acciones que la aplicación realiza, así como de los mensajes sobre los eventos que ocurren cuando la aplicación está en funcionamiento.

La función de seguimiento de la aplicación solo debe utilizarse bajo la supervisión del servicio de soporte técnico de Kaspersky.

*Para crear un archivo de seguimiento de la aplicación:*

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

   Se abre la ventana **Soporte**.

2. En la ventana **Soporte**, haga clic en el botón **Herramientas de soporte**.

3. Utilice el interruptor **Habilitar seguimiento de la aplicación** para habilitar o deshabilitar el seguimiento del funcionamiento de la aplicación.

4. En la lista desplegable **Seguimientos**, 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 la cantidad máxima de archivos para la rotación y el tamaño máximo de cada archivo.

   - **Guardar en un único archivo**. Guardar un archivo de seguimiento (sin límite de tamaño).

5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento.

   En lo posible, pregúntele por el nivel de seguimiento indicado a un especialista del servicio de soporte técnico. A falta de esta información, use el nivel de seguimiento **Normal (500)**.

6. Reinicie Kaspersky Endpoint Security.

7. Para detener el proceso de seguimiento, regrese a la ventana **Soporte** y desactive el seguimiento.

También puede crear archivos de seguimiento al instalar la aplicación; para ello, realice la instalación a través de la línea de comandos o utilice el archivo setup.ini.

Los archivos de seguimiento quedarán guardados en el equipo mientras la aplicación esté instalada; cuando desinstale la aplicación, los archivos se eliminarán de forma permanente. Los archivos de seguimiento, excepto los del Agente de autenticación, se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. De manera predeterminada, la función está deshabilitada.

# Seguimiento del rendimiento de aplicaciones

Kaspersky Endpoint Security le permite obtener información sobre los problemas que puedan ocurrir en el funcionamiento del equipo al utilizar la aplicación. Por ejemplo, si observa demoras al cargar el sistema operativo tras instalar la aplicación, puede recibir información al respecto. Para brindar esta información, Kaspersky Endpoint Security crea archivos de seguimiento del rendimiento. Realizar un *seguimiento del rendimiento* se refiere a registrar las acciones que la aplicación realiza con el fin de diagnosticar los problemas de rendimiento de Kaspersky Endpoint Security. Para obtener la información, Kaspersky Endpoint Security utiliza el servicio de Seguimiento de eventos para Windows (ETW). Diagnosticar los problemas de Kaspersky Endpoint Security y determinar sus causas es tarea del servicio de soporte técnico de Kaspersky.

La función de seguimiento de la aplicación solo debe utilizarse bajo la supervisión del servicio de soporte técnico de Kaspersky.

*Para crear un archivo de seguimiento del rendimiento:*

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

   Se abre la ventana **Soporte**.

2. En la ventana **Soporte**, haga clic en el botón **Herramientas de soporte**.

3. Utilice el interruptor **Habilitar seguimiento del rendimiento** para habilitar o deshabilitar el seguimiento del rendimiento de las aplicaciones.

4. En la lista desplegable **Seguimientos**, 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.

   - **Guardar en un único archivo**. Guardar un archivo de seguimiento (sin límite de tamaño).

5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento:

   - **Básico**. Kaspersky Endpoint Security analizará los principales procesos 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 seguimiento**, seleccione el tipo de seguimiento:

   - **Información básica**. Kaspersky Endpoint Security analizará los procesos mientras el sistema operativo esté en funcionamiento. Utilice este tipo de seguimiento para problemas que continúen después de que el sistema operativo se haya cargado (por ejemplo, si tiene problemas para acceder a Internet a través del navegador).

   - **Al reiniciar**. Kaspersky Endpoint Security analizará los procesos únicamente mientras el sistema operativo se esté cargando. Una vez que el sistema operativo se haya cargado, Kaspersky Endpoint Security detendrá el proceso de seguimiento. Utilice este tipo de seguimiento si su problema está vinculado a alguna demora durante la carga del sistema operativo.

7. Reinicie el equipo e intente reproducir el problema.

8. Para detener el proceso de seguimiento, regrese a la ventana **Soporte** y desactive el seguimiento.

   De esta manera, se creará un archivo de seguimiento del rendimiento en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces. Envíe ese archivo al servicio de soporte técnico de Kaspersky.

## Creación de archivos de volcado

Un archivo de volcado contiene toda información sobre la memoria operativa de los procesos de Kaspersky Endpoint Security en el momento en que se creó el archivo de volcado.

> Los archivos de volcado guardados pueden contener datos confidenciales. Usted es responsable de velar por la seguridad de estos archivos y controlar el acceso a los datos.

Los archivos de volcado se almacenan en su equipo de una forma modificada que no puede leerse mientras la aplicación está en uso y se eliminan en forma permanente cuando se desinstala la aplicación. Los archivos de volcado se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KES\Traces.

*Para habilitar y deshabilitar la escritura en archivos de volcado:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **General**.
3. En el bloque **Información para depuración**, use la casilla **Habilitar escritura en archivos de volcado** para habilitar o deshabilitar la escritura de volcado de la aplicación.
4. Guarde los cambios.

## Protección de los archivos de volcado y de seguimiento

Los archivos de volcado y los archivos de rastreo contienen la información sobre el sistema operativo y también pueden contener datos del usuario. Para evitar el acceso no autorizado a dichos datos, puede habilitar la protección de archivos de volcado y de rastreo.

Si la protección de archivos de volcado y de rastreo está activada, los siguientes usuarios podrán acceder a los archivos:

- El administrador del sistema y el administrador local, además del usuario que activó la escritura de los archivos de volcado y de rastreo pueden acceder a los archivos de volcado.
- Solo el administrador del sistema y el administrador local pueden acceder a los archivos de rastreo.

*Para habilitar o deshabilitar la protección de los archivos de volcado y de rastreo:*

1. En la parte inferior de la ventana principal de la aplicación, haga clic en el botón ⚙.
2. En la ventana de configuración de la aplicación, seleccione la sección **General**.
3. En el bloque **Información para depuración**, utilice la casilla **Habilitar la protección de los archivos de volcado y de seguimiento** para habilitar o deshabilitar la protección de archivos.

4. Guarde los cambios.

Los archivos de volcado y de rastreo que se escribieron con la protección activa permanecen protegidos incluso luego de deshabilitar esta función.

# Limitaciones y advertencias

Kaspersky Endpoint Security posee numerosas limitaciones que no son críticos para el funcionamiento de la aplicación.

Instalación de la aplicación

- Para obtener más información sobre el soporte técnico de los sistemas operativos Microsoft Windows 10, Microsoft Windows Server 2016 y Microsoft Windows Server 2019, consulte la Base de conocimientos del Servicio de soporte técnico.

- 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.

- Al actualizar desde Kaspersky Endpoint Security 10 Service Pack 2 para Windows (compilación 10.3.0.6294), el componente Prevención de intrusiones en el host está activado.

- Cuando se actualiza Kaspersky Endpoint Security 10 para Windows Service Pack 2 (compilación 10.3.0.6294), los archivos colocados en Cuarentena o en el Depósito de copias de seguridad de la versión antigua se transfieren al Depósito de copias de seguridad en la versión nueva de la aplicación. Los archivos de versiones anteriores a Kaspersky Endpoint Security 10 para Windows Service Pack 2 (compilación 10.3.0.6294) no se transfieren. Para guardarlos, debe restaurar los archivos de Cuarentena y del Depósito de copias de seguridad antes de actualizar la aplicación. Una vez completada la actualización, vuelva a analizar los archivos restaurados.

- Si desea eliminar y volver a instalar el cifrado (FLE o FDE) o el componente Control de dispositivos, debe reiniciar el sistema antes de la reinstalación.

- Cuando utilice el sistema operativo Microsoft Windows 10, debe reiniciar el sistema después de eliminar el componente Cifrado de archivos (FLE).

- Al intentar instalar cualquier versión del módulo de cifrado AES en un equipo que tiene Kaspersky Endpoint Security para Windows 11.6.0, pero sin componentes de cifrado instalados, 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 11.6.0 es incompatible con los 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 el siguiente error: *An application whose name is missing or unreadable is installed on your computer* (Una aplicación cuyo nombre falta o no se puede leer está instalada en su equipo). Esto significa que las aplicaciones no compatibles o fragmentos de ellas permanecen en su equipo. Para eliminar artefactos de aplicaciones no compatibles, envíe una solicitud con una descripción detallada de la situación al Servicio de soporte técnico de Kaspersky a través de Kaspersky CompanyAccount.

- A partir de la versión 11.0.0 de la aplicación, puede instalar el complemento MMC de Kaspersky Endpoint Security para Windows sobre la versión anterior del complemento. Para volver a una versión anterior del

complemento, elimine el complemento actual e instale una versión anterior del complemento.

- Al actualizar Kaspersky Endpoint Security 11.0.0 o 11.0.1 para Windows, la configuración del programa de tareas local para las tareas *Actualización*, *Análisis de áreas críticas*, *Análisis personalizado* y *Comprobación de integridad* no se guarda.

- 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.

- Si está actualizando una versión anterior de la aplicación a la versión 11.6.0, 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.

- 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 que ejecutan Windows 10 versión 1809, 1903 y 1909, no se instalarán los controladores de FDE en la imagen de WinRE.

- Después de instalar Kaspersky Endpoint Security para Windows en algunas configuraciones de Windows 7, Windows Defender continúa funcionando. Se le recomienda que desactive Windows Defender manualmente para no afectar el rendimiento del sistema.

- Una vez que la aplicación se actualiza desde versiones anteriores a Kaspersky Endpoint Security 11 para Windows, se debe reiniciar el equipo.

**Compatibilidad con plataformas de servidor**

- El sistema de archivos ReFS se admite con limitaciones:
  - Una vez que se inicia la comprobación antivirus del servidor, las exclusiones del análisis agregadas con iChecker se restablecen cuando se reinicia el servidor.
  - Kaspersky Endpoint Security no detecta los archivos eicar.com y susp-eicar.com si el archivo meicar.exe existía en el equipo antes de la instalación de Kaspersky Endpoint Security.
- No se admiten las configuraciones de Server Core y Cluster Mode.
- Las tecnologías Cifrado de archivos (FLE) y Cifrado de disco de Kaspersky (FDE) no pueden utilizarse en plataformas de servidor.
- Control de dispositivos no es compatible con las plataformas de servidor.
- Microsoft Windows Server 2008 ya no se considera compatible. - La aplicación no está diseñada para instalarse en una computadora con el sistema operativo Microsoft Windows Server 2008.
- Si inició varias sesiones de trabajo en el servidor de terminales, es posible que las notificaciones de Kaspersky Endpoint Security no funcionen correctamente. Ejemplo: El usuario de la sesión 1 revisa la reputación de un archivo en KSN. Kaspersky Endpoint Security le mostrará una notificación con los resultados de la revisión al usuario de la sesión 2.

Compatibilidad con plataformas virtuales

- No se admite Cifrado de disco completo (FDE) en máquinas virtuales Hyper-V.
- No se admite Cifrado de disco completo (FDE) en plataformas virtuales Citrix.
- Se admite Windows 10 Enterprise multisesión con ciertas limitaciones:
  - Kaspersky Endpoint Security considera Windows 10 Enterprise multisesión como un sistema operativo de servidores. Por lo tanto, Windows 10 Enterprise multisesión se admite con limitaciones específicas de plataformas para servidores. Por ejemplo, los servidores no pueden utilizar algunos de los componentes de Kaspersky Endpoint Security. La aplicación también utiliza una clave de licencia de servidor en lugar de una clave de licencia de estación de trabajo.
  - El cifrado de disco completo (FDE) no es compatible.
  - La administración de BitLocker no es compatible.
  - El uso de Kaspersky Endpoint Security con unidades extraíbles no es compatible. La infraestructura de Microsoft Azure define las unidades extraíbles como unidades de red.
- No se admite la instalación y el uso de Cifrado de archivos (FLE) en plataformas virtuales Citrix.
- Para admitir la compatibilidad de Kaspersky Endpoint Security para Windows con Citrix PVS, realice la instalación con la opción **Garantizar compatibilidad con Citrix PVS** habilitada. Esta opción se puede habilitar en el Asistente de instalación o con el parámetro de línea de comandos `/pCITRIXCOMPATIBILITY=1`. En caso de instalación remota, el archivo KUD debe editarse agregando el siguiente parámetro: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Antes de iniciar la clonación, debe deshabilitar Autoprotección para clonar máquinas virtuales que usan vDisk.
- Al preparar una máquina de plantilla para la imagen principal de Citrix XenDesktop con Kaspersky Endpoint Security para Windows preinstalado y el Agente de red de Kaspersky Security Center, agregue los siguientes tipos de exclusiones al archivo de configuración:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Para obtener detalles sobre Citrix XenDesktop, visite el sitio web de soporte de Citrix.
- En algunos casos, es posible que un intento de desconectar de forma segura una unidad extraíble no se realice correctamente en una máquina virtual implementada en un hipervisor VMware ESXi. Intente desconectar de forma segura el dispositivo una vez más.

Compatibilidad con Kaspersky Security Center

- Puede administrar el componente Control de anomalías adaptativo solo en Kaspersky Security Center versión 11 o posterior.
- Es posible que el informe de amenazas de Kaspersky Security Center 11 no muestre información sobre la acción realizada en las amenazas detectadas por la Protección vía AMSI.
- El estado operativo de los componentes Protección vía AMSI y Control de anomalías adaptativo solo está disponible en Kaspersky Security Center versión 11 o posterior. Puede ver el estado operativo en la Consola de Kaspersky Security Center en las propiedades del equipo, en la sección **Tareas**. También hay informes de estos componentes disponibles solo en Kaspersky Security Center versión 11 o posterior.

### Administración de licencias

- Si aparece el mensaje *Error al recibir los datos*, verifique que el equipo en el que está realizando la activación tenga acceso a la red o defina la configuración de activación a través del proxy de activación de Kaspersky Security Center.
- No se puede activar la aplicación con una suscripción a través de Kaspersky Security Center si la licencia caducó 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 de clave incrustado en un equipo que tiene acceso a Internet inestable puede resultar en la visualización temporal de eventos que indiquen que la aplicación no está activada o que la licencia no permite el funcionamiento del componente. Esto se debe a que 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 prueba, la instalación de cualquier actualización o parche de la aplicación en un equipo que tiene un acceso a Internet inestable puede resultar en la visualización temporal de eventos que indiquen que la aplicación no está activada. Esto se debe a que 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, debe activar manualmente la aplicación.
- Si está usando la versión 11 de Kaspersky Security Center y la versión 11.6.0 de Kaspersky Endpoint Security, es posible que los informes de rendimiento de los componentes no funcionen de forma correcta. Si instaló componentes de Kaspersky Endpoint Security que no se incluyen en la licencia que posee, es posible que un Agente de red envíe errores sobre el estado de los componentes al Registro de eventos de Windows. Para evitar errores, elimine los componentes que no están incluidos en la licencia que posee.

### 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, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Los archivos almacenados en unidades de red o en discos CD o DVD regrabables no pueden restaurarse.
- Los archivos cifrados con el sistema de cifrado de archivos EFS no pueden restaurarse. Para más información sobre el funcionamiento de EFS, visite el *sitio web de Microsoft*.
- La aplicación no controla los cambios que se realizan en los archivos a través de procesos que funcionan en el nivel del núcleo del sistema operativo.
- 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 aplicaciones de bloqueo y reglas de paquetes.
  - Por período de vida del paquete (TTL) en reglas de paquetes en bloque para paquetes entrantes o salientes.
  - Por interfaz de red para paquetes entrantes y salientes o conexiones en reglas de paquetes.
- 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 11.6.0, los estados de los permisos para las siguientes reglas de firewall no se migran:
  - Solicitudes al servidor DNS por TCP.
  - Solicitudes al servidor DNS por UDP.
  - Cualquier actividad de la red.
  - Respuestas entrantes inaccesibles del destino de ICMP.
  - Secuencia ICMP entrante.
- Si configuró un adaptador de red o período de vida (TTL) de paquetes para una regla de paquetes permitidos, la prioridad de esta regla es menor que la de una regla de aplicación de bloqueo. En otras palabras, si la actividad de red está bloqueada para una aplicación (por ejemplo, la aplicación está en el grupo de confianza *Restricción máxima*), no puede permitir la actividad de red de la aplicación mediante el uso de una regla de paquete con esta configuración. En todos los demás casos, la prioridad de una regla de paquete es mayor que la de una regla de red de aplicaciones.
- Puede producirse un error en Kaspersky Endpoint Security para Windows 11.5.0-11.6.0 al importar una lista de reglas de paquetes de Firewall. Esto puede provocar la eliminación de las direcciones locales o remotas definidas por el usuario de una regla. Para solucionar el error, póngase en contacto con el Servicio de soporte técnico. El Servicio de soporte técnico le proporcionará una actualización revisada para el complemento. De lo contrario, puede actualizar la aplicación a la siguiente versión después de su lanzamiento.
- Al importar una lista de reglas de paquetes de Firewall, es posible que Kaspersky Endpoint Security cambie los nombres de las reglas. La aplicación identifica las reglas que tienen el mismo conjunto de parámetros principales, como el protocolo, la dirección, los puertos remotos y locales, y el período de vida del paquete (TTL). Si este conjunto de parámetros principales es idéntico para varias reglas, la aplicación asigna el mismo nombre a estas reglas o agrega una etiqueta de parámetro al nombre. Esto significa que Kaspersky Endpoint Security importa todas las reglas de paquetes, pero el nombre de las reglas que tienen parámetros principales idénticos puede cambiar.
- 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 agregó 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.

### Control de aplicaciones

- Cuando se trabaja en Microsoft Windows 10 en modo de lista de bloqueo de aplicaciones, las reglas de bloqueo pueden aplicarse incorrectamente, lo que podría causar el bloqueo de aplicaciones que no están especificadas en las reglas.
- Cuando el componente Control de aplicaciones bloquea las aplicaciones web progresivas (PWA), appManifest.xml se indica como la aplicación bloqueada en el informe.

### Control de dispositivos

- El acceso a los dispositivos de impresora que se agregaron a la lista de confianza está bloqueado por las reglas de bloqueo de dispositivos y bus.
- Para los dispositivos MTP, se admite el control de las operaciones de lectura, escritura y conexión si está utilizando los controladores integrados de Microsoft del sistema operativo. Si un usuario instala un controlador personalizado para trabajar con un dispositivo (por ejemplo, como parte de iTunes o Android Debug Bridge), es posible que el control de las operaciones de lectura y escritura no funcione.
- Cuando se trabaja con dispositivos MTP, las reglas de acceso se cambian después de volver a conectar el dispositivo.
- Si está agregando un dispositivo a la lista de confianza según una máscara de modelo y usa caracteres que están incluidos en el id. pero no en el nombre del modelo, estos dispositivos no se agregan. En una estación de trabajo, estos dispositivos se agregarán a la lista de confianza según una máscara de identificación.

### Control Web

- No se admiten los formatos OGV y WEBM.
- No se admite el protocolo RTMP.

### Control de anomalías adaptativo

- Se recomienda crear exclusiones automáticamente según el evento. Cuando agregue manualmente una exclusión, agregue el carácter * al comienzo de la ruta al especificar el objeto de destino.
- No se puede generar un informe de Reglas de control de anomalías adaptativo si la muestra incluye incluso un evento cuyo nombre contiene más de 260 caracteres.
- No se puede agregar exclusiones del Control de anomalías adaptativo que active el repositorio de reglas si las propiedades de un objeto o un proceso tienen un valor que contenga más de 256 caracteres (por ejemplo, una ruta a un objeto de destino). Puede agregar una exclusión manualmente en la configuración de directivas. También puede agregar una exclusión en el Informe en las reglas activadas del Control de anomalías adaptativo.

**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 AES-NI (Nuevas Instrucciones de Cifrado Avanzado Intel). Si el procesador no es compatible con AES-NI, el rendimiento del equipo podría disminuir.
- Cuando hay procesos que intentan acceder a dispositivos cifrados antes de que la aplicación les haya otorgado acceso a dichos dispositivos, la aplicación muestra una advertencia donde se indica que dichos procesos deben terminarse. Si los procesos no se pueden terminar, vuelva a conectar los dispositivos cifrados.
- Los id. únicos de los discos duros se muestran en las estadísticas de cifrado del dispositivo en formato invertido.
- No se recomienda formatear los dispositivos mientras se cifran.
- Cuando se conectan simultáneamente varias unidades extraíbles a un equipo, la directiva de cifrado se puede aplicar a una sola unidad extraíble. Cuando se vuelven a conectar los dispositivos extraíbles, la directiva de cifrado se aplica correctamente.
- Es posible que el cifrado no se inicie en un disco duro muy fragmentado. Desfragmente el disco duro.
- Cuando los discos duros están cifrados, la hibernación se bloquea desde el momento en que comienza la tarea de cifrado hasta el primer reinicio de un equipo con Microsoft Windows 7/8/8.1/10, y después de la instalación del cifrado del disco duro hasta el primer reinicio de sistemas operativos Microsoft Windows 8/8.1/10. Cuando se descifran los discos duros, la hibernación se bloquea desde el momento en que la unidad de arranque se descifra por completo hasta el primer reinicio del sistema operativo. Cuando la opción **Inicio rápido** está habilitada en Microsoft Windows 8/8.1/10, el bloqueo de la hibernación evita que apague el sistema operativo.
- Los equipos con Windows 7 no permiten cambiar la contraseña durante la recuperación cuando el disco está cifrado con tecnología BitLocker. Una vez que se ingresa la clave de recuperación y se carga el sistema operativo, Kaspersky Endpoint Security no solicitará al usuario que cambie la contraseña o el código PIN. Por lo tanto, es imposible establecer una contraseña nueva o un código PIN. Este problema se origina por las peculiaridades del sistema operativo. Para continuar, debe volver a cifrar el disco duro.
- No se recomienda utilizar la herramienta xbootmgr.exe con los proveedores adicionales habilitados. Por ejemplo, Despachador, Red o Controladores.
- No se admite el formateo de una unidad extraíble cifrada en un equipo que tenga instalado Kaspersky Endpoint Security para Windows.
- No se admite el formateo de una unidad extraíble cifrada con el sistema de archivos FAT32 (la unidad se muestra como cifrada). Para formatear una unidad, vuelva a formatearla al sistema de archivos NTFS.
- Para obtener detalles sobre cómo restaurar un sistema operativo desde una copia de seguridad a un dispositivo GPT cifrado, visite la Base de conocimientos del Servicio 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 simultáneamente todas estas condiciones:

- No hay conexión con el servidor de Kaspersky Security Center.
- El usuario está intentando completar la autorización con un nuevo token o contraseña.

Si ocurre una situación similar, reinicie el equipo. Una vez reiniciado el equipo, se otorgará acceso a la unidad extraíble cifrada.

- Es posible que el agente de autenticación no admita el descubrimiento de dispositivos USB cuando el modo xHCI para USB está habilitado en la configuración del BIOS.
- El Cifrado de disco de Kaspersky (FDE) para la parte SSD de un dispositivo que se utiliza para almacenar en caché los datos utilizados con más frecuencia no es compatible con dispositivos SSHD.
- No se admite el cifrado de discos duros en sistemas operativos Microsoft Windows 8/8.1/10 de 32 bits que se ejecutan en modo UEFI.
- Reinicie el equipo antes de volver a cifrar un disco duro descifrado.
- El cifrado del disco duro no es compatible con Kaspersky Anti-Virus para UEFI. No se recomienda utilizar el cifrado del disco duro en equipos que tengan instalado Kaspersky Anti-Virus para UEFI.
- La creación de cuentas de Agente de autenticación basadas en cuentas de Microsoft se admite con las siguientes limitaciones:
  - No se admite la tecnología Inicio de sesión único.
  - No se admite la creación automática de cuentas del Agente de autenticación si se selecciona la opción de crear cuentas para los usuarios que inician sesión en el sistema en los últimos N días.
- Si el nombre de una cuenta del Agente de autenticación tiene el formato `<dominio>/<nombre de la cuenta de Windows>`, después de cambiar el nombre del equipo, también debe cambiar los nombres de las cuentas que se crearon para los usuarios locales de este equipo. Por ejemplo, supongamos que hay un usuario local `Ivanov` en el equipo `Ivanov`, y se creó una cuenta de agente de autenticación con el nombre `Ivanov/Ivanov` para este usuario. Si el nombre de equipo `Ivanov` se cambió por `Ivanov-PC`, debe cambiar el nombre de la cuenta del Agente de autenticación para el usuario `Ivanov` de `Ivanov/Ivanov` a `Ivanov-PC/Ivanov`. Puede cambiar el nombre de la cuenta utilizando la tarea de administración de cuentas locales del Agente de autenticación. Antes de que se haya cambiado el nombre de la cuenta, es posible la autenticación en el entorno previo al arranque con el nombre antiguo (por ejemplo, `Ivanov/Ivanov`).
- Si a un usuario se le permite acceder a un equipo que se cifró con la tecnología Cifrado de disco de Kaspersky solo usando un token y este usuario necesita completar el procedimiento de recuperación de acceso, asegúrese de que este usuario tenga acceso basado en contraseña a este equipo después de haber restaurado el acceso al equipo cifrado. Es posible que no se guarde la contraseña que estableció el usuario al restaurar el acceso. En este caso, el usuario tendrá que completar el procedimiento para restaurar el acceso al equipo cifrado nuevamente la próxima vez que se reinicie el equipo.
- Al descifrar un disco duro con la Herramienta de recuperación FDE, el proceso de descifrado puede terminar con un error si los datos del dispositivo de origen se sobrescriben con los datos descifrados. Parte de los datos del disco duro permanecerán cifrados. Se recomienda elegir la opción para guardar los datos descifrados en un archivo en la configuración de descifrado del dispositivo cuando se utiliza la Herramienta de recuperación FDE.
- Si se ha cambiado la contraseña del Agente de autenticación, aparecerá un mensaje con el texto *Your password has been changed successfully (Su contraseña se ha cambiado correctamente). Aparecerá el mensaje Click OK* (Haga clic en Aceptar), y el usuario reinicia el equipo. No se guarda la nueva contraseña. La contraseña anterior se debe utilizar para la autenticación posterior en el entorno de prearranque.

- El cifrado de disco no es compatible con la tecnología Intel Rapid Start.
- El cifrado de disco no es compatible con la tecnología ExpressCache.
- En algunos casos, al intentar descifrar una unidad cifrada con la Herramienta de recuperación FDE, la herramienta detecta por error el estado del dispositivo como "no cifrado" después de que se completa el procedimiento "Solicitud-respuesta". El registro de la herramienta muestra un evento donde se indica que el dispositivo se descifró correctamente. En este caso, debe reiniciar el procedimiento de recuperación de datos para descifrar el dispositivo.
- Una vez que el complemento de Kaspersky Endpoint Security para Windows se actualiza en Web Console, las propiedades del equipo cliente no muestran la clave de recuperación de BitLocker hasta que se reinicia el servicio de Web Console.
- Para ver las otras limitaciones del soporte de cifrado de disco completo y una lista de dispositivos para los que el cifrado de discos duros es compatible con restricciones, consulte la Base de conocimientos del Servicio de soporte técnico.

### Cifrado de archivos (FLE)

- El cifrado de archivos 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 se accede al archivo desde un equipo donde el cifrado no está disponible, se proporcionará acceso directo a este archivo. Un archivo cifrado que se almacena en una carpeta de red en un equipo que tiene la función de cifrado disponible se copia en forma descifrada a un equipo que no tiene la función de cifrado disponible.
- Se recomienda descifrar los archivos que se cifraron con el sistema de cifrado de archivos antes de cifrar archivos con Kaspersky Endpoint Security para Windows.
- Después de cifrar un archivo, su tamaño aumenta 4 kB.
- Después de cifrar un archivo, se establece el atributo *Archivo* en las propiedades del archivo.
- Si un archivo descomprimido desde un archivo cifrado tiene el mismo nombre que un archivo que ya existe en el equipo, el nuevo archivo descomprimido desde un archivo cifrado sobrescribirá al anterior. No se notifica al usuario sobre la operación de sobrescritura.
- 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.
- El Administrador de archivos portátil no se puede utilizar para acceder a una unidad extraíble si se cumplen las siguientes condiciones de manera simultánea:
  - No hay conexión con Kaspersky Security Center
  - Kaspersky Endpoint Security para Windows está instalado en el equipo.
  - No se realizó el cifrado de datos (FDE o FLE) en el equipo.

  En este caso, el acceso no es posible aunque se conozca la contraseña del Administrador de archivos portátil.
- Cuando se utiliza el cifrado de archivos, la aplicación es incompatible con el cliente de correo Sylpheed.
- Kaspersky Endpoint Security para Windows no es compatible con las reglas de restricción de acceso a los archivos cifrados de algunas aplicaciones. Esto se debe a que algunas operaciones de archivo se realizan mediante una aplicación de terceros. Por ejemplo, la copia de archivos la realiza el administrador de archivos y no la aplicación. De este modo, si se deniega el acceso a los archivos cifrados al cliente de correo de Outlook, Kaspersky Endpoint Security permitirá que el cliente de correo acceda al archivo cifrado, siempre y cuando el usuario haya copiado los archivos en el mensaje de correo electrónico a través del portapapeles o mediante la función de arrastrar y soltar. Se realizó la operación de copia a través de un administrador de archivos, para el cual no se especifican las reglas de restricción de acceso a los archivos cifrados, es decir, el acceso está permitido.
- No se admite el cambio de la configuración del archivo de página. El sistema operativo utiliza los valores predeterminados en lugar de los valores de los parámetros especificados.

- Utilice la extracción segura al trabajar con unidades extraíbles cifradas. No podemos garantizar la integridad de los datos si la unidad extraíble no se extrae de forma segura.
- Una vez que los archivos están cifrados, sus originales no cifrados se eliminan de forma segura.
- No se admite la sincronización de archivos sin conexión mediante el Almacenamiento en caché del lado del cliente (CSC). Se recomienda prohibir la administración sin conexión de recursos compartidos en el nivel de directiva de grupo. Los archivos que están en modo sin conexión se pueden editar. Después de la sincronización, es posible que se pierdan los cambios realizados en un archivo sin conexión. 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 del Servicio de soporte técnico.
- No se admite la creación de un archivo cifrado en la raíz del disco duro del sistema.
- Puede experimentar problemas al acceder a archivos cifrados a través de la red. Se recomienda mover los archivos a otro origen o asegurarse de que el equipo que se utiliza como servidor de archivos esté administrado por el mismo Servidor de administración de Kaspersky Security Center.
- Cambiar la distribución del teclado puede hacer que se bloquee la ventana de entrada de contraseña para un archivo autoextraíble cifrado. Para resolver este problema, cierre la ventana de ingreso de contraseña, cambie a la distribución de teclado en su sistema operativo y vuelva a ingresar la contraseña para el archivo cifrado.
- Cuando se utiliza el cifrado de archivos en sistemas que tienen varias particiones en un disco, se recomienda utilizar la opción que determina automáticamente el tamaño del archivo pagefile.sys. Una vez que el equipo se reinicia, el archivo pagefile.sys puede moverse entre las particiones del disco.
- Después de aplicar las reglas de cifrado de archivos, incluidos los archivos de la carpeta Mis documentos, asegúrese de que los usuarios a los que se les ha aplicado el cifrado puedan acceder correctamente a los archivos cifrados. A estos fines, haga que cada usuario inicie sesión en el sistema cuando haya una conexión a Kaspersky Security Center disponible. Si un usuario intenta acceder a archivos cifrados sin una conexión a Kaspersky Security Center, el sistema puede bloquearse.
- Si los archivos del sistema se incluyen de alguna manera en el alcance del cifrado de archivos, es posible que en los informes aparezcan eventos relacionados con errores al cifrar estos archivos. Los archivos especificados en estos eventos no están realmente cifrados.
- No se admiten procesos Pico.
- No se admiten las rutas que distinguen entre mayúsculas y minúsculas. Cuando se aplican reglas de cifrado o reglas de descifrado, las rutas de los eventos del producto se muestran en minúsculas.
- No se recomienda cifrar los archivos que utiliza el sistema al iniciarse. Si estos archivos están cifrados, un intento de acceder a archivos cifrados sin una conexión a Kaspersky Security Center puede hacer que el sistema se bloquee o genere solicitudes de acceso a los archivos no cifrados.
- Cuando las unidades extraíbles están cifradas con el modo portátil, el control de antigüedad de la contraseña no se puede deshabilitar.
- Si los usuarios trabajan conjuntamente con un archivo a través de la red bajo reglas FLE mediante aplicaciones que utilizan el método de asignación de archivo a memoria (como WordPad o FAR) y aplicaciones diseñadas para trabajar con archivos grandes (como Notepad ++), el archivo en forma no cifrada se puede bloquear indefinidamente sin la capacidad de acceder a él desde el equipo donde reside.
- No se admite el cifrado de archivos en las carpetas de sincronización de OneDrive. Agregar carpetas con archivos ya cifrados a la lista de sincronización de OneDrive puede provocar la pérdida de datos en los archivos cifrados.

- Cuando se instala el componente de cifrado de archivos, la administración de usuarios y grupos no funciona en modo WSL (Subsistema de Windows para Linux).
- Cuando está instalado el componente Cifrado de archivos, no se admite POSIX (Portable Operating System Interface) para cambiar el nombre de archivos y eliminarlos.
- Después de actualizar Kaspersky Endpoint Security para Windows versión 11.0.1 o anterior, para acceder a los archivos cifrados luego de reiniciar el equipo, asegúrese de que se esté ejecutando el Agente de red. El Agente de red se inicia con cierto retraso, por lo que no puede acceder a los archivos cifrados inmediatamente después de la carga del sistema operativo. No es necesario esperar a que el Agente de red se inicie después del próximo arranque del equipo.

Otras limitaciones

- En sistemas operativos de servidor, no se muestra ninguna advertencia sobre la necesidad de una desinfección avanzada.
- Las direcciones web que se agregan 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 tráfico HTTP, la aplicación bloquea esta conexión para evitar la descarga de los archivos maliciosos de Internet.
- Kaspersky Endpoint Security no es compatible con el estándar RFC9218 para el protocolo HTTP/2. Si Kaspersky Endpoint Security detecta este formato de intercambio de datos en el tráfico, la aplicación bloquea la conexión y aparece el error ERR_HTTP2_PROTOCOL_ERROR en el navegador. Si necesita acceso a este recurso web, puede excluirlo de los análisis de conexión cifrada o puede comunicarse con el Servicio de soporte técnico para solicitar un parche.
- 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. Posteriormente, la aplicación firmada digitalmente se incluirá en el grupo correcto.
- Al analizar el correo con la extensión Protección contra amenazas de correo para Microsoft Outlook, se recomienda utilizar el modo caché de Exchange (la opción Usar modo caché de Exchange).
- La *tarea de análisis de* antivirus no es compatible con la versión de Microsoft Outlook de 64 bits. Esto quiere decir que Kaspersky Endpoint Security no analiza los archivos de Outlook x64 (archivos PST y OST), incluso si el correo se incluye en el alcance del análisis.
- En Kaspersky Security Center 10, cuando se realiza el cambio de KSN Global a KSN Privada (o viceversa), la opción de participar en Kaspersky Security Network se deshabilita en la directiva del producto específico. Después del cambio, lea atentamente el texto de la Declaración de Kaspersky Security Network y confirme su consentimiento para participar en KSN. Puede leer el texto de la Declaración en la interfaz de la aplicación o al editar la directiva del producto.
- Durante un nuevo análisis de un objeto malicioso bloqueado por software de terceros, no se notifica al usuario cuando se detecta nuevamente la amenaza. El evento de nueva detección de amenazas se muestra en el informe del producto y en el informe de Kaspersky Security Center 10.
- El componente Sensor de Endpoint no se puede instalar en Microsoft Windows Server 2008.
- El informe de Kaspersky Security Center 10 sobre el cifrado de dispositivos no incluirá información sobre los dispositivos que se cifraron con Microsoft BitLocker en plataformas de servidor o en estaciones de trabajo en las que no está instalado el componente Control de dispositivos.
- Cuando se utiliza una jerarquía de directivas, se puede acceder a la configuración de la sección Cifrado de unidades extraíbles en una directiva secundaria para editar si la directiva principal prohíbe la modificación de esa configuración.
- Debe habilitar Auditar inicio de sesión en la configuración del sistema operativo para garantizar el correcto funcionamiento de las exclusiones para la protección de las carpetas compartidas contra el cifrado externo.
- Si la protección de carpetas compartidas está habilitada, Kaspersky Endpoint Security para Windows supervisa los intentos de cifrar las carpetas compartidas para cada sesión de acceso remoto que se inició antes del inicio de Kaspersky Endpoint Security para Windows, incluso si el equipo desde el que se inició la

sesión de acceso remoto ha sido agregado a las exclusiones. Si no desea que Kaspersky Endpoint Security para Windows supervise los intentos de cifrar las carpetas compartidas para las sesiones de acceso remoto que se iniciaron desde un equipo que se agregó a las exclusiones y que se iniciaron antes del inicio de Kaspersky Endpoint Security para Windows, finalice y vuelva a establezca la sesión de acceso remoto o reinicie el equipo en el que está instalado Kaspersky Endpoint Security para Windows.

- Si la tarea de actualización se ejecuta con los permisos de una cuenta de usuario específica, los parches del producto no se descargarán cuando se actualice desde un origen que requiera autorización.
- Es posible que la aplicación no se inicie debido a un rendimiento insuficiente del sistema. Para resolver este problema, use la opción Arranque listo o aumente el tiempo de espera del sistema operativo para iniciar los servicios.
- La aplicación no puede funcionar en Modo a prueba de fallos.
- Para garantizar que Kaspersky Endpoint Security para Windows, versiones 11.5.0 y 11.6.0, puedan funcionar correctamente con el software Cisco AnyConnect, debe instalar Compliance Module, versión 4.3.183.2048 o posterior. Obtenga más información sobre la compatibilidad con Cisco Identity Services Engine en la documentación de Cisco.
- No podemos garantizar que Control de audio funcionará hasta después del primer reinicio posterior a la instalación de la aplicación.
- Cuando los archivos de seguimiento rotados están habilitados, no se crean seguimientos para el componente AMSI y el complemento de Outlook.
- El seguimiento del rendimiento no se puede recopilar manualmente en Windows Server 2008.
- No se admite Seguimiento del rendimiento para el tipo de seguimiento "Reiniciar".
- Ya no se admite la tarea de verificación de disponibilidad de KSN.
- Desactivar la opción "Deshabilitar 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` a partir de la versión del sistema operativo Windows 10RS2). El parámetro `AMPPL` con un valor de `1` habilita el uso de la tecnología de Procesos de Protección para el servicio del producto.
- Para ejecutar un análisis personalizado de una carpeta, el usuario que inicia el análisis personalizado debe tener los permisos para leer los atributos de esta carpeta. De lo contrario, el análisis de carpetas personalizadas será imposible y terminará con un error.
- Cuando una regla de análisis definida en una directiva incluye una ruta sin el carácter `\` al final, por ejemplo, `C:\carpeta1\carpeta2`, el análisis se ejecutará para la ruta C:\carpeta1\.
- Al actualizar la aplicación de la versión 11.1.0 a la 11.6.0, la configuración de Protección vía AMSI se restablecerá a sus valores predeterminados.
- Si hay directivas de restricción de software (SRP) activas en el equipo, puede que tenga problemas para cargar el sistema y vea una pantalla en negro. Se recomienda cambiar la configuración de SRP de la siguiente manera: establezca el valor **Todos los archivos de software, excepto las bibliotecas (como DLL)** para el parámetro **Aplicar directivas de restricción de software a los siguientes objetos**, y agregue reglas con el nivel de seguridad **Sin restricciones** para las rutas a los archivos de la aplicación (`C:\Archivos de programa\Archivos comunes\Kaspersky Lab` y `C:\Archivos de programa\Kaspersky Lab`). Para más información sobre las directivas de restricción de software, consulte la *documentación de Microsoft*.

- No se admite la administración de la configuración del complemento de Outlook a través de la API REST.
- La configuración de ejecución de tareas para un usuario específico no se puede transferir entre dispositivos a través de un archivo de configuración. Después de aplicar la configuración desde un archivo de configuración, especifique manualmente el nombre de usuario y la contraseña.
- Después de instalar una actualización, la tarea de comprobación de integridad no funciona hasta que se reinicia el sistema para aplicar la actualización.
- Cuando el nivel de seguimiento rotado se cambia a través de la utilidad de diagnóstico remoto, Kaspersky Endpoint Security para Windows muestra incorrectamente un valor en blanco para el nivel de seguimiento. Sin embargo, los archivos de seguimiento se escriben de acuerdo con el nivel de seguimiento correcto. Cuando el nivel de seguimiento rotado se cambia a través de la interfaz local de la aplicación, el nivel de seguimiento se modifica correctamente, pero la utilidad de diagnóstico remoto muestra incorrectamente el nivel de seguimiento que la utilidad definió por última vez. Esto puede hacer que el administrador no tenga información actualizada sobre el nivel de seguimiento actual, y la información relevante puede estar ausente de los seguimientos si un usuario cambia manualmente el nivel de seguimiento en la interfaz local de la aplicación.
- En la interfaz local, la configuración de la protección con contraseña no permite cambiar el nombre de la cuenta del administrador (KLAdmin, de forma predeterminada). Para cambiar el nombre de la cuenta del administrador, debe deshabilitar la protección con contraseña, luego habilitar la protección con contraseña y especificar un nuevo nombre para la cuenta del administrador.
- Kaspersky Endpoint Security supervisa el tráfico HTTP que cumple con los estándares RFC 2616, RFC 7540, RFC 7541, RFC 7301. Si Kaspersky Endpoint Security detecta otro formato de intercambio de datos en tráfico HTTP, la aplicación bloquea esta conexión para evitar la descarga de los archivos maliciosos de Internet.
- Al analizar una conexión cifrada, Kaspersky Endpoint Security fuerza HTTP/1.
- 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 portátiles

Aplicación que brinda una interfaz para trabajar con archivos cifrados en unidades extraíbles cuando las funciones de cifrado necesarias para ello no están disponibles en el equipo.

## Agente de autenticación

Interfaz para pasar el proceso de autenticación para acceder a los discos duros cifrados y cargar el sistema operativo una vez que se cifró el disco duro del sistema.

## Agente de red

Un componente de Kaspersky Security Center que habilita la interacción entre el servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es común para todas las aplicaciones de Kaspersky que se ejecutan en Windows. Las versiones dedicadas de Agente de red sirven para aplicaciones que se ejecutan en otros sistemas operativos.

## Alcance de la protección

Los objetos que la Protección básica contra amenazas analiza constantemente cuando está en ejecución. Los alcances de la protección de diferentes componentes tienen diferentes propiedades.

## Alcance del análisis

Los objetos que analiza Kaspersky Endpoint Security cuando realiza una tarea de análisis.

## Archivo de almacenamiento

Uno o varios archivos empaquetados en un solo archivo comprimido. Se necesita una aplicación especializada llamada archivador para comprimir y descomprimir datos.

## Archivo infectable

Un archivo que, por su estructura o formato, puede ser usado por intrusos como "contenedor" para almacenar y propagar código malicioso. Por lo general, son archivos ejecutables con extensiones de archivo tales como .com, .exe y .dll. Existe un riesgo bastante alto de intrusión de código malicioso en estos archivos.

## Archivo infectado

Archivo que contiene código malicioso (código de malware conocido que se detectó al analizar el archivo). Kaspersky no recomienda utilizar estos archivos, ya que podrían infectar el equipo.

## Base de datos de direcciones web de phishing

Lista de las direcciones de correo electrónico que los especialistas de Kaspersky han definido como relacionadas con phishing. La base de datos se actualiza periódicamente y forma parte del kit de distribución de las aplicaciones de Kaspersky.

## Base de datos de direcciones web maliciosas

Lista de direcciones web cuyo contenido se puede considerar peligroso. Los especialistas de Kaspersky crean la lista. Se actualiza periódicamente y se incluye en el kit de distribución de las aplicaciones de Kaspersky.

## Bases de datos antivirus

Las bases de datos que contienen información sobre las amenazas conocidas de seguridad al equipo por parte de Kaspersky como de la fecha de lanzamiento de la base de datos antivirus. Las firmas de la bases de datos antivirus ayudan a detectar código malicioso en los objetos analizados. Las bases de datos antivirus son creadas por los especialistas de Kaspersky y se actualizan cada hora.

## Certificado de licencia

Un documento que transfiere Kaspersky al usuario junto con el archivo de clave o código de activación. Incluye información sobre la licencia otorgada al usuario.

## Clave activa

Clave que está utilizando la aplicación.

## Clave adicional

Clave que certifica el derecho de usar la aplicación pero que no se está utilizando.

## Desinfección

Método de procesamiento de objetos infectados cuyo resultado es la recuperación completa o parcial de los datos. No todos los objetos infectados se pueden desinfectar.

## Emisor de certificado

El centro de certificación que emitió el certificado.

## Falsa alarma

Una falsa alarma se produce cuando la aplicación de Kaspersky indica que un archivo desinfectado está infectado debido a que la firma del archivo es similar a la de un virus.

## Forma normalizada de la dirección de un recurso web

La forma normalizada de la dirección de un recurso web es una representación textual de la dirección del recurso web que se obtiene a través de una normalización. La normalización es un proceso por medio del cual la representación textual de la dirección de un recurso web cambia según reglas específicas (por ejemplo: exclusión del inicio de sesión del usuario, de la contraseña y del puerto de conexión de la representación textual de la dirección del recurso web; además, la dirección del recurso web se modifica de caracteres en mayúscula a caracteres en minúscula).

En el contexto de funcionamiento de los componentes de protección, el fin de la normalización de direcciones de recursos web es evitar el análisis de las direcciones de sitios web que, más de una vez, pueden diferir en la sintaxis pero ser físicamente equivalentes.

Ejemplo:

Forma no normalizada de una dirección: www.Ejemplo.com\.

Forma normalizada de una dirección: www.ejemplo.com.

## Grupo de administración

Un conjunto de dispositivos que tienen funciones en común y el conjunto de aplicaciones de Kaspersky instaladas en ellos. Los dispositivos se agrupan de manera tal que se puedan administrar fácilmente como una unidad. En un grupo, se pueden incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada aplicación instalada en el grupo.

## Máscara

Representación del nombre de un archivo y de su extensión utilizando comodines.

Las máscaras de archivos puede contener cualquier carácter permitido en nombres de archivos, incluidos comodines:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y

de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\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 de análisis.

- El carácter `?` (signo de interrogación) puede usarse para representar cualquier carácter individual. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\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

Se desarrolló un microchip para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Suele haber un Módulo de plataforma segura instalado en la placa madre del equipo y este módulo interactúa con todos los demás componentes del sistema a través del bus de hardware.

## Objeto OLE

Un archivo adjunto o un archivo integrado en otro archivo. Las aplicaciones de Kaspersky permiten analizar objetos OLE en busca de virus. Por ejemplo: si incrusta una tabla de Microsoft Office Excel® en un documento de Microsoft Office Word, la tabla se analiza como un objeto OLE.

## Tarea

Funciones realizadas por la Aplicación Kaspersky como tareas, por ejemplo: Protección de archivos de tiempo real, Análisis completo de dispositivo, Actualización de bases de datos.

# Apéndices

En esta sección encontrará contenidos que complementan la información principal del documento.

# Apéndice 1. Configuración de la aplicación

Puede utilizar una directiva, tareas o la interfaz de la aplicación para configurar Kaspersky Endpoint Security. La información detallada sobre componentes de la aplicación se proporciona en las secciones correspondientes.

## Protección contra amenazas de archivos

El componente Protección contra amenazas de archivos le permite evitar la infección del sistema de archivos del equipo. De manera predeterminada, el componente se mantiene cargado en la RAM del equipo. Protección contra archivos peligrosos analiza los archivos de todas las unidades del equipo, incluidas las que se conectan al mismo. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

El componente analiza los archivos a los que acceden tanto el usuario como las aplicaciones. Cuando se detecta un archivo malintencionado, Kaspersky Endpoint Security bloquea la operación del archivo. El archivo entonces se elimina o se desinfecta, dependiendo de cómo se ha configurado el componente.

Si intenta acceder a un archivo cuyo contenido esté almacenado en la nube de OneDrive, Kaspersky Endpoint Security descargará el contenido y lo analizará.

Parámetros del componente Protección contra amenazas de archivos

| Parámetro | Descripción |
|---|---|
| **Nivel de seguridad**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Para Protección contra archivos peligrosos, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*:<br>• **Alto**. Si se selecciona este nivel de seguridad de archivos, el componente Protección contra amenazas de archivos realiza el control más estricto de todos los archivos abiertos, guardados e iniciados. El componente Protección contra amenazas de archivos analiza todos los tipos de archivo en todos los discos duros, unidades extraíbles y unidades de red del equipo. También analiza archivos de almacenamiento, paquetes de instalación y objetos OLE integrados.<br>• **Recomendado**. Los expertos de Kaspersky Lab recomiendan este nivel de seguridad de archivos. El componente Protección contra amenazas de archivos solo analiza los formatos de archivo especificados en todos los discos duros, unidades extraíbles y unidades de red del equipo, y en los objetos de OLE incorporados. El componente Protección contra amenazas de archivos no analiza paquetes de instalación ni archivos.<br>• **Bajo**. La configuración de este nivel de seguridad de archivos garantiza la máxima velocidad de análisis. El componente Protección contra amenazas de archivos analiza solamente los archivos con las extensiones especificadas en todos los discos duros, unidades extraíbles y unidades de red del equipo. El componente Protección contra amenazas de archivos no analiza archivos compuestos. |

| | |
|---|---|
| **Tipos de archivos**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | **Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones).<br>**Archivos analizados según su formato**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.<br>**Archivos analizados según su extensión**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión. |
| **Alcance de la protección** | Contiene objetos que son analizados por el componente Protección contra amenazas de archivos. Los objetos de análisis pueden ser discos duros, unidades extraíbles o de red, carpetas, archivos individuales o máscaras que engloben varios archivos.<br>De manera predeterminada, el componente Protección contra amenazas de archivos analiza los archivos iniciados en discos duros, unidades extraíbles o unidades de red. El alcance de protección de estos objetos no puede modificarse ni eliminarse. Sí es posible excluir un objeto (por ejemplo, una unidad extraíble) de los análisis. |
| **Aprendizaje automático y análisis de firmas**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | El método aprendizaje automático y análisis de firmas usa las bases de datos de Kaspersky Endpoint Security que contienen descripciones de las amenazas conocidas y las formas para neutralizarlas. La protección que usa este método proporciona el nivel de seguridad mínimo aceptable.<br>Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado. |
| **Análisis heurístico**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br>Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Acción al detectar una amenaza** | **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.<br>**Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.<br>**Bloquear**. Si esta opción está seleccionada, el componente Protección contra amenazas de archivos bloquea automáticamente 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 si se puede desinfectar en el futuro. |
| **Analizar solo archivos nuevos y modificados** | Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como compuestos. |
| **Analizar archivos de almacenamiento** | Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE. |
| **Analizar paquetes de distribución** | Use esta casilla para habilitar/deshabilitar el análisis de paquetes de distribución de terceros. |
| **Analizar archivos de Microsoft Office** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **No desempaquetar archivos compuestos grandes** | Si esta casilla está seleccionada, Kaspersky Endpoint Security no analiza los archivos compuestos si su tamaño excede el valor.<br>Si esta casilla está desactivada, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.<br>Kaspersky Endpoint Security analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla está marcada o no. |
| **Descomprimir archivos compuestos en segundo plano** | Si activa esta casilla, Kaspersky Endpoint Security permitirá acceder a los archivos compuestos que superen el tamaño especificado antes de que se los haya analizado. En este caso, Kaspersky Endpoint Security descomprimirá y analizará los archivos compuestos en segundo plano.<br>Kaspersky Endpoint Security proporciona acceso a los archivos compuestos que son más pequeños que este valor solo después de descomprimir y analizar estos archivos.<br>Si no activa esta casilla, Kaspersky Endpoint Security no permitirá acceder a ningún archivo compuesto, independientemente de su tamaño, hasta que se lo haya descomprimido y analizado. |
| **Modo de análisis**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Kaspersky Endpoint Security analiza los archivos a los que accede el usuario, el sistema operativo o una aplicación que se ejecuta en la cuenta del usuario.<br>**Modo inteligente**. En este modo, Protección contra archivos peligrosos analiza un objeto en función de las operaciones realizadas sobre ese objeto. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento Microsoft Office la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de sobrescritura no originan el análisis del archivo.<br>**Ante operaciones de acceso y modificación**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos siempre que haya un intento de abrirlos o modificarlos. |

| | |
|---|---|
| | **Ante operaciones de acceso**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos solo después de un intento de abrirlos.<br>**Ante operaciones de ejecución**. En este modo, el componente Protección contra archivos peligrosos analiza los objetos después de un intento de ejecutarlos. |
| **Tecnología iSwift**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS. |
| **Tecnología iChecker**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |
| **Pausar Protección contra archivos peligrosos**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Esto suspende temporal y automáticamente la operación de Protección contra archivos peligrosos a la hora especificada o al trabajar con las aplicaciones especificadas. |

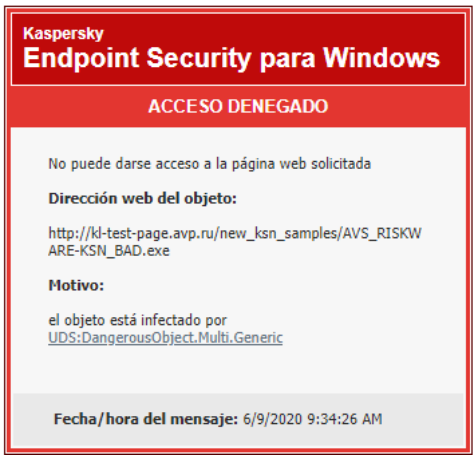
## Protección contra amenazas web

El componente Protección contra amenazas web está diseñado para bloquear sitios web maliciosos y fraudulentos e impedir la descarga de archivos dañinos de Internet. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Kaspersky Endpoint Security tiene la capacidad de analizar tráfico HTTP, HTTPS y FTP. La aplicación analiza tanto direcciones URL como direcciones IP. Puede permitir que Kaspersky Endpoint Security vigile todos los puertos o puede seleccionar los puertos específicos que le interese controlar.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario habilitar el análisis de conexiones cifradas.

Cuando un usuario intente abrir un sitio web malicioso o fraudulento, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia (vea la siguiente imagen).




Mensaje cuando se bloquea el acceso a un sitio web

Configuración del componente Protección contra amenazas web

| Parámetro | Descripción |
|---|---|
| **Nivel de seguridad**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Para la Protección contra amenazas web, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*.<br>• **Alto**. El nivel de seguridad con el cual el componente Protección contra amenazas web realiza el análisis máximo del tráfico web que recibe el equipo a través de los protocolos HTTP y FTP. El componente Protección contra amenazas web analiza en detalle todos los objetos de tráfico web mediante el uso de todas las bases de datos de la aplicación y realiza el análisis heurístico más avanzado posible.<br>• **Recomendado**. Este es el nivel de seguridad que proporciona el equilibrio óptimo entre el rendimiento de Kaspersky Endpoint Security y la seguridad del tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de **análisis medio**. Los especialistas de Kaspersky recomiendan este nivel de seguridad de tráfico web.<br>• **Bajo**. La configuración de este nivel de seguridad de tráfico web asegura la máxima velocidad de análisis de tráfico web. El componente Protección contra amenazas web realiza un análisis heurístico en el nivel de **Análisis superficial**. |
| **Acción al detectar una amenaza** | **Bloquear descarga**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador.<br>**Informar**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web permite que el objeto se descargue al equipo, pero agrega información sobre el mismo a la lista de amenazas activas. |
| **Comprobar si la URL está en la base de datos de direcciones URL malintencionadas** | Analizar los vínculos para determinar si están incluidos en la base de datos de direcciones web malintencionadas le permite rastrear sitios web que estén en la lista de bloqueo. Kaspersky realiza el mantenimiento de la base de datos de direcciones web malintencionadas, la que se incluye en el paquete de instalación de la aplicación y se actualiza durante las actualizaciones de las bases de datos de Kaspersky Endpoint Security. |

| | |
|---|---|
| *(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | |
| **Utilizar el Análisis heurístico**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br>Cuando se analiza el tráfico web en busca de virus y otras aplicaciones que presentan una amenaza, el analizador heurístico sigue las instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Comprobar si la URL está en la base de datos de direcciones URL fraudulentas**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | La base de datos de direcciones web fraudulentas incluye las direcciones web de los sitios que actualmente se sabe que se utilizan para realizar intentos de fraude (phishing). Kaspersky complementa esta base de datos de vínculos fraudulentos con direcciones obtenidas de la organización internacional denominada Anti-Phishing Working Group. La base de datos de direcciones fraudulentas está incluida en el paquete de instalación de la aplicación y se complementa con las actualizaciones de bases de datos de Kaspersky Endpoint Security. |
| **No analizar el tráfico web de las direcciones web de confianza** | Si la casilla está seleccionada, el componente Protección contra amenazas web no analiza el contenido de las páginas o los sitios web cuyas direcciones están incluidas en la lista de direcciones web de confianza. Puede agregar a esta lista tanto direcciones específicas como máscaras de páginas o sitios web. |

## Protección contra amenazas de correo

El componente Protección contra amenazas de correo analiza los archivos adjuntos a los mensajes de correo entrantes y salientes para detectar virus y otras amenazas. También analiza los mensajes en busca de vínculos maliciosos o fraudulentos. De manera predeterminada, el componente se mantiene cargado en la RAM del equipo y analiza todos los mensajes enviados o recibidos mediante los protocolos POP3, SMTP, IMAP y NNTP, o a través del cliente de correo Microsoft Office Outlook (MAPI). Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el análisis heurístico y el servicio de nube Kaspersky Security Network.

Si utiliza un navegador para acceder a su cliente de correo electrónico, el componente Protección contra amenazas de correo no analizará sus mensajes.

Cuando detecta un mensaje con un archivo adjunto malicioso, Kaspersky Endpoint Security cambia el asunto del mensaje de la siguiente manera: `[Mensaje infectado] <asunto del mensaje>` o `[Se eliminó un objeto infectado] <asunto del mensaje>`.

Este componente interactúa con clientes de correo instalados en el equipo. En el caso de Microsoft Office Outlook, existe una extensión con parámetros adicionales. La extensión de la Protección contra amenazas de correo se incorpora al cliente de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

Configuración del componente Protección contra amenazas de correo

| Parámetro | Descripción |
| --- | --- |
| **Nivel de seguridad**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Para Protección contra amenazas de correo, Kaspersky Endpoint Security puede aplicar diferentes grupos de configuraciones. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*.<br>• **Alto**. Cuando este nivel de seguridad del correo electrónico se selecciona, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico más detalladamente. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico profundo. El nivel de seguridad de correo **Alta** se recomienda para entornos de alto riesgo. Un ejemplo de este tipo de entorno es una conexión a un servicio de correo gratuito desde una red doméstica sin protección centralizada del correo.<br>• **Recomendado**. Este es el nivel de seguridad del correo electrónico que proporciona el equilibrio óptimo entre el rendimiento de Kaspersky Endpoint Security y la seguridad del correo electrónico. El componente Protección contra amenazas de correo analiza los mensajes de correo electrónico entrantes y salientes y realiza un análisis heurístico de nivel medio. Los especialistas de Kaspersky recomiendan este nivel de seguridad del tráfico de correo.<br>• **Bajo**. Cuando se selecciona este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo solo analiza los mensajes de correo entrantes, realiza un análisis heurístico superficial y no analiza los archivos adjuntos a los mensajes de correo electrónico. En este nivel de seguridad de correo electrónico, el componente Protección contra amenazas de correo analiza los mensajes de correo electrónico con una velocidad máxima y utiliza lo mínimo de los recursos del sistema operativo. Se recomienda utilizar el nivel de seguridad de correo **Bajo** en un entorno bien protegido. Un ejemplo de este tipo de entorno podría ser una red LAN empresarial con protección de correo electrónico centralizada. |
| **Acción al detectar una amenaza** | **Desinfectar; eliminar si falla la desinfección**. Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security lo elimina. El asunto del mensaje se cambia a `[Se eliminó un objeto infectado] <asunto del mensaje>` para informarle al usuario sobre la acción realizada.<br><br>**Desinfectar; bloquear si falla la desinfección**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security agrega una advertencia al asunto del mensaje: `[Mensaje infectado] <asunto del mensaje>`. El usuario puede acceder al mensaje, con su archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, Kaspersky Endpoint Security intenta desinfectar el objeto. Si el objeto no puede desinfectarse, Kaspersky Endpoint Security bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error. |

| | |
|---|---|
| | **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, Kaspersky Endpoint Security agrega una advertencia al asunto del mensaje: `[Mensaje infectado] <asunto del mensaje>`. El usuario puede acceder al mensaje, con su archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, Kaspersky Endpoint Security bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error. |
| **Alcance de la protección**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | El *Alcance de la protección* incluye objetos que el componente comprueba cuando se ejecuta: **Mensajes entrantes y salientes** o **Solo mensajes entrantes**.<br>Para proteger sus equipos, solo necesita analizar los mensajes entrantes. Puede activar el análisis de mensajes salientes para evitar el envío de archivos infectados. También puede activar el análisis de mensajes salientes si desea evitar el envío de archivos en formatos particulares, como archivos de audio y video, por ejemplo. |
| **Analizar el tráfico POP3/SMTP/NNTP/IMAP** | Esta casilla determina si el componente Protección contra amenazas de correo analizará o no el tráfico POP3, SMTP, NNTP e IMAP. |
| **Conectar extensión de Microsoft Outlook** | Si esta casilla está seleccionada, los mensajes de correo electrónico que se transmitan a través de los protocolos POP3, SMTP, NNTP e IMAP se analizarán con la extensión integrada en Microsoft Outlook.<br>Si planea analizar el correo con la extensión para Microsoft Outlook, recomendamos que use 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. |
| **Análisis heurístico**<br>*(disponible solo en la Consola de administración [MMC] y en la interfaz de Kaspersky Endpoint Security)* | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br>Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Analizar archivos de almacenamiento adjuntos** | Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE.<br>Si, durante el análisis, Kaspersky Endpoint Security detecta una contraseña de un archivo de almacenamiento en el texto del mensaje, esta contraseña se utilizará para analizar el contenido del archivo en busca de aplicaciones maliciosas. En este caso, la contraseña no se guarda. Durante el análisis, el archivo de almacenamiento se descomprime. Si la aplicación genera un error durante el proceso de descompresión, puede eliminar manualmente los archivos descomprimidos que se guardan en la siguiente ruta: %systemroot%\temp. Los archivos tienen el prefijo PR. |
| **Analizar los formatos adjuntos de Office** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **No analizar archivos de almacenamiento mayores** | Si esta casilla está seleccionada, el componente Protección contra amenazas de correo excluye del análisis los archivos adjuntos en los mensajes de correo |

| | |
|---|---|
| **que N MB** | si el tamaño excede el valor especificado. Si se desactiva la casilla, el componente Protección contra amenazas de correo analiza los archivos adjuntos de correo de cualquier tamaño. |
| **No analizar archivos durante más de N seg** | Si la casilla está seleccionada, el tiempo asignado al análisis de archivos adjuntos en los mensajes de correo se limita al período especificado. |
| **Filtrado de documentos adjuntos** | El filtro de documentos adjuntos no se aplica a mensajes de correo electrónico salientes.<br><br>**Deshabilitar el filtrado**. Si selecciona esta opción, el componente Protección contra amenazas de correo no filtrará los archivos adjuntos de los mensajes de correo electrónico.<br><br>**Cambiar el nombre de los archivos adjuntos de los tipos seleccionados**. Si selecciona esta opción, Protección contra amenazas de correo reemplazará el último carácter de extensión encontrado en los archivos adjuntos de los tipos especificados con el carácter de guion bajo (por ejemplo, adjunto.doc_). Por lo tanto, para abrir el archivo, el usuario debe cambiar el nombre del archivo.<br><br>**Eliminar archivos adjuntos de los tipos seleccionados**. Si selecciona esta opción, el componente Protección contra amenazas de correo eliminará de los mensajes de correo electrónico los tipos de archivos adjuntos que especifique.<br><br>Puede especificar los tipos de archivos adjuntos para eliminar de los mensajes de correo electrónico en la lista de máscaras de archivos. |

## Protección contra amenazas de red

El componente Protección contra amenazas de red analiza el tráfico de red entrante en busca de actividad típica de ataques de red. Cuando Kaspersky Endpoint Security detecta un ataque de red contra el equipo del usuario, bloquea la conexión al equipo agresor.

Las distintas clases de ataques de red sobre las que se tiene registro, así como las maneras de combatirlos, se describen en las bases de datos de Kaspersky Endpoint Security. La lista de ataques de red que detecta el componente Protección contra amenazas de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación.

Configuración del componente Protección contra amenazas de red

| Parámetro | Descripción |
|---|---|
| **Detectar ataques de escaneo de puertos y saturación de solicitudes** | Ataques de *saturación de solicitudes*, con los cuales se busca afectar los recursos de red (por ejemplo, los servidores web) de una organización. En esta clase de ataque, se realiza una gran cantidad de solicitudes con el fin de sobrecargar el ancho de banda disponible para los recursos de red. La sobrecarga impide el acceso a los recursos de la organización.<br><br>Ataques de *escaneo de puertos*, en los cuales se realiza un sondeo de los puertos UDP, los puertos TCP y los servicios de red del equipo. El escaneo de puertos permite determinar qué tan vulnerable es un equipo; suele estar seguido por algún tipo de ataque más peligroso. El escaneo también revela el sistema operativo del equipo y permite, así, elegir el ataque de red más apropiado. |

| | |
|---|---|
| | Si activa esta casilla, Kaspersky Endpoint Security buscará indicios de estas clases de ataques en el tráfico de red. Cuando se detecte un ataque, se filtrará y bloqueará el tráfico perjudicial. Con ello, si alguien inicia un ataque de saturación de solicitudes contra el equipo, se evitará que el recurso afectado se sobrecargue. De manera similar, si un atacante realiza un escaneo de los puertos del equipo, la información confidencial del sistema se mantendrá a resguardo.<br>Si alguna de sus aplicaciones autorizadas realiza operaciones que son típicas de estas clases de ataques, puede deshabilitar las funciones de detección pertinentes. Con ello evitará las falsas alarmas. |
| **Agregar el equipo atacante a la lista de equipos bloqueados durante N minutos** | Si la casilla de verificación está seleccionada, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección.<br>Puede acceder a la lista de equipos bloqueados a través de la ventana del Monitor de red.<br>La lista de equipos bloqueados se vacía cada vez que Kaspersky Endpoint Security se reinicia o cuando se modifica la configuración de Protección contra amenazas de red. |
| **Exclusiones** | La lista contiene las direcciones IP de las que la Protección contra amenazas de red no bloquea los ataques de red.<br>Kaspersky Endpoint Security no registra ningún dato sobre los ataques de red provenientes de las direcciones IP de la lista de exclusiones. |
| **Protección contra suplantaciones de MAC** | Ataques de *suplantación de MAC*, que consisten en cambiar la dirección MAC de un dispositivo (tarjeta) de red. Al realizar este cambio, un atacante puede redirigir los datos destinados a un dispositivo a otro dispositivo diferente y, de ese modo, obtener acceso a la información. Kaspersky Endpoint Security le permite saber si se detecta uno de estos ataques y bloquearlo. |

## Firewall

El componente Firewall impide que se establezcan conexiones no autorizadas cuando el equipo está conectado a una red local o a Internet. Firewall también controla la actividad de red de las aplicaciones instaladas en el equipo. Ello ayuda a proteger la LAN corporativa contra ataques de robo de identidad y otras amenazas. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus, el servicio de nube Kaspersky Security Network y las *reglas de red* predefinidas.

El Agente de red se utiliza para interactuar con Kaspersky Security Center. El firewall crea automáticamente las reglas de red necesarias para que la aplicación y el Agente de red funcionen. Como resultado, el firewall abre varios puertos en la computadora. Los puertos que se abren dependen de la función de la computadora (por ejemplo, punto de distribución). Para obtener más información sobre los puertos que se abrirán en la computadora, consulte *la Ayuda de Kaspersky Security Center*.

### Reglas de red

Las reglas de red se pueden configurar en distintos niveles:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Kaspersky Endpoint Security incluye una serie de reglas predefinidas, con permisos configurados según las recomendaciones de los expertos de Kaspersky.

- *Reglas de red de aplicaciones*. Las reglas de red de la aplicación imponen restricciones en la actividad de la red de una aplicación específica. Tienen en cuenta no solo las características del paquete de red, sino también la aplicación específica a la cual se dirige este paquete de red o que los emitió.

Controlar el acceso de las aplicaciones a los datos personales, a los procesos y a los recursos del sistema operativo es tarea del componente Prevención de intrusiones en el host, que utiliza los *derechos* asignados a las aplicaciones para tal fin.

Cuando una aplicación se ejecuta por primera vez, Firewall realiza las siguientes acciones:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.

2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Firewall, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los *grupos de confianza*: De confianza, Restricción mínima, Restricción máxima o No confiables.

   Los grupos de confianza determinan los derechos en los que Kaspersky Endpoint Security se basa para controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea la actividad de red de la aplicación si su grupo de confianza así lo requiere. Por ejemplo, las aplicaciones del grupo Restricción máxima no tienen permitido usar ninguna conexión de red.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Si la aplicación no presenta modificaciones, el componente usa las reglas de red que ya están definidas para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

## Prioridad de las reglas de red

Cada regla tiene una prioridad. Cuanto más arriba en la lista se encuentra una regla, mayor es su prioridad. Cuando un mismo tipo de actividad de red se describe en varias reglas, Firewall se basa en la regla de mayor prioridad para regular la actividad.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si las reglas de paquetes de red y las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se procesa según las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan del siguiente modo: una regla de red para aplicaciones contiene reglas de acceso basadas en un estado de red (*red pública*, *red local* o *red de confianza*). Las aplicaciones del grupo de confianza Restricción máxima, por ejemplo, no tienen permitido realizar ninguna clase de actividad de red, independientemente de que el equipo esté conectado a una red pública, local o de confianza. Cuando se crea una regla de red para una aplicación individual (aplicación principal), dicha regla afecta también a los procesos secundarios de otras aplicaciones. Cuando no existe una regla de red para una aplicación, los procesos secundarios quedan sujetos a la regla de acceso de red correspondiente al grupo de confianza de la aplicación.

Supóngase, por ejemplo, que se prohíbe el tráfico en redes de cualquier estado para todas las aplicaciones, a excepción del navegador X. El navegador X (aplicación principal) se utiliza luego para iniciar la instalación de un navegador Y (proceso secundario). En este caso, el instalador del navegador Y tendrá acceso a la red y podrá descargar los archivos que hagan falta. Tras la instalación, sin embargo, Firewall no permitirá que el navegador Y establezca conexiones de red. Para que el instalador del navegador Y no pueda acceder a la red valiéndose de su condición de proceso secundario, será necesario agregar una regla de red que cubra ese programa específico.

## Estados de las conexiones de red

Firewall puede controlar la actividad de red basándose en el estado de la conexión. Kaspersky Endpoint Security obtiene el estado de la conexión del sistema operativo. El estado informado por el sistema operativo es el que el usuario configura cuando la conexión se establece por primera vez. Si lo desea, puede cambiar el estado de la conexión de red en la configuración de Kaspersky Endpoint Security. A la hora de controlar la actividad de red, Firewall tomará como válido el estado asignado dentro de Kaspersky Endpoint Security en lugar del estado que informe el sistema operativo.

La conexión de la red puede presentar uno de los siguientes tipos de estado:

- **Red pública**. Una red que no está protegida por una aplicación antivirus, un filtro o un firewall (un ejemplo podría ser la red Wi-Fi de una cafetería). Cuando el usuario opera un equipo conectado a una red de ese tipo, el Firewall bloquea el acceso a archivos e impresoras de este equipo. Los usuarios externos tampoco tienen acceso a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella.

  De forma predeterminada, Firewall asigna el estado *Red pública* a Internet. No puede cambiar el estado de Internet.

- **Red local**. Una red en la que los usuarios tienen restricciones para acceder a los archivos y las impresoras del equipo (un ejemplo podría ser una LAN corporativa u hogareña).

- **Red confiable**. Una red segura, en la que el equipo no está expuesto a ningún ataque o a intentos no autorizados de acceder a los datos que contiene. El Firewall permite cualquier actividad de red dentro de redes con este estado.

Configuración del componente Firewall

| Parámetro | Descripción |
|---|---|
| **Reglas de paquetes de red** | Tabla con una lista de reglas para paquetes de red. Las reglas de paquetes de red sirven para imponer restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado.<br>La tabla enumera reglas de paquetes de red preconfiguradas recomendadas por Kaspersky para la protección óptima del tráfico de red de equipos que se ejecutan en sistemas operativos Microsoft Windows. |

| | |
|---|---|
| | Firewall define la prioridad de ejecución de cada regla de paquetes de red. Firewall procesa las reglas de paquetes de red en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba a abajo. Cuando se detecta una conexión de red, el componente busca la primera regla de paquetes pertinente y la aplica a la actividad de red, que se permitirá o bloqueará según corresponda. Las reglas posteriores que también sean aplicables a la conexión de red se desestimarán.<br>Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. |
| **Conexiones de red** | Esta tabla contiene información sobre conexiones de red detectadas por el Firewall en el equipo.<br>El estado asignado por defecto a la Internet es *Red pública*. No puede cambiar el estado de Internet. |
| **Reglas de red** | **Apéndices**<br>Tabla de aplicaciones controladas por el componente Firewall. Cada aplicación está asignada a un grupo de confianza. Los grupos de confianza determinan los derechos en los que Kaspersky Endpoint Security se basa para controlar la actividad de red de las aplicaciones.<br>Puede elegir una aplicación de una lista única en la que se recogen todas las aplicaciones instaladas en los equipos sujetos a una directiva y agregarla a un grupo de confianza.<br>**Reglas de red**<br>Tabla con las reglas de red que se han definido para las aplicaciones de un grupo de confianza. Firewall regula la actividad de red de las aplicaciones basándose en estas reglas.<br>La tabla contiene reglas de red predefinidas y recomendadas por los especialistas de Kaspersky. Dichas reglas se han incluido porque permiten proteger el tráfico de red de los equipos con Windows del mejor modo posible. Las reglas de red predefinidas no se pueden eliminar. |

## Prevención de ataques BadUSB

Algunos virus modifican el firmware de los dispositivos USB para hacer que el sistema operativo considere que el dispositivo USB es un teclado. De esta manera, el virus puede ejecutar comandos en su cuenta de usuario para descargar malware, por ejemplo.

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

Cuando un dispositivo USB se conecta al equipo y es identificado por el sistema operativo como un teclado, la aplicación le solicita al usuario que ingrese un código numérico generado por la aplicación desde este teclado, o con un Teclado en pantalla, si está disponible (vea la siguiente imagen). Este procedimiento se conoce como autorización del teclado.

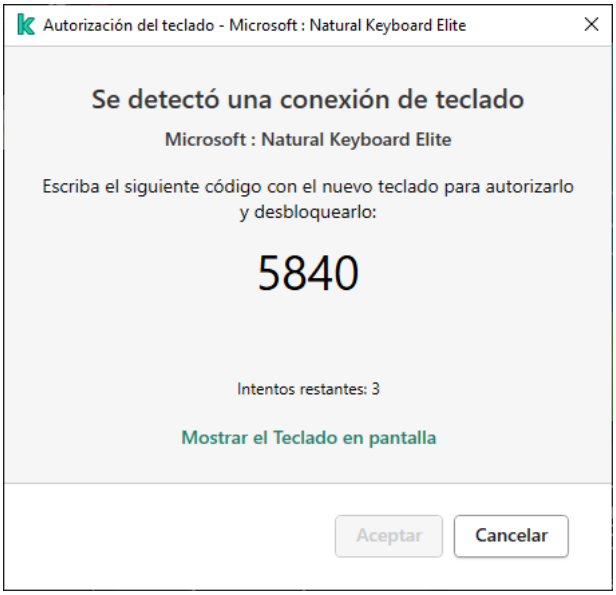
Si el código se ha ingresado correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al cual se ha conectado) en la lista de teclados autorizados. No es necesario repetir la autorización cuando el teclado vuelve a conectarse o después del reinicio del sistema operativo.

Si el teclado autorizado se conecta a otro puerto USB del equipo, la aplicación mostrará otra vez una solicitud de autorización para este teclado.

Si se ha ingresado incorrectamente el código numérico, la aplicación genera un nuevo código. Puede haber tres intentos para ingresar el código numérico. Si el código numérico se ingresa incorrectamente tres veces consecutivas o se cierra la venta **Autorización del teclado <Nombre del teclado>**, la aplicación bloquea la entrada desde este teclado. Cuando el teclado vuelve a conectarse o cuando se reinicia el sistema operativo, la aplicación le solicita al usuario que lleve a cabo nuevamente la autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea un teclado que no haya sido autorizado.

El componente Prevención de ataques BadUSB no se instala por defecto. Si desea utilizarlo, agréguelo en las propiedades del paquete de instalación antes de instalar la aplicación. Si la aplicación ya está instalada, modifique la selección de componentes disponibles.




*Autorización del teclado*

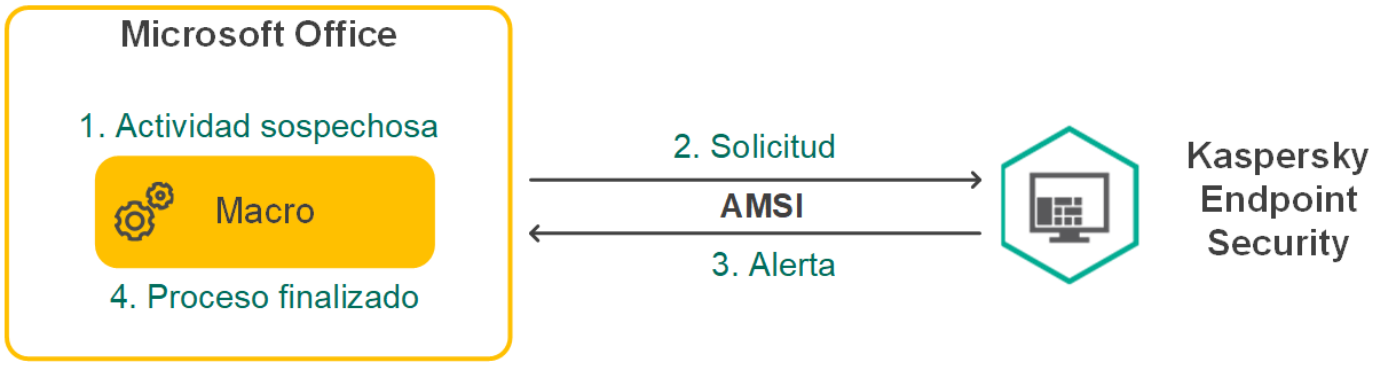
Configuración del componente Prevención de ataques BadUSB

| Parámetro | Descripción |
|---|---|
| **No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB** | Si se selecciona la casilla, la aplicación bloquea el uso del teclado en pantalla para la autorización de un dispositivo USB desde el cual no se puede ingresar un código de autorización. |

## Protección vía AMSI

El componente Protección vía AMSI está diseñado para admitir la interfaz de análisis antimalware 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 información sobre AMSI, consulte la *documentación de Microsoft*.

La Protección vía AMSI únicamente puede detectar amenazas y notificárselo a la aplicación. La aplicación de terceros después de recibir una notificación de una amenaza no le permite realizar acciones maliciosas (por ejemplo, la finaliza).




Ejemplo del funcionamiento de AMSI

El componente Protección vía AMSI puede rechazar una solicitud de una aplicación de terceros, por ejemplo, si esta aplicación excede el número máximo de solicitudes dentro de un intervalo específico. Cuando esto ocurre, Kaspersky Endpoint Security envía información al respecto al Servidor de administración. El componente Protección vía AMSI no rechaza las solicitudes que provienen de aplicaciones de terceros para las que se ha seleccionado la casilla **No bloquear la interacción con el Proveedor de protección para AMSI**

La Protección vía AMSI está disponible para los siguientes sistemas operativos para estaciones de trabajo y servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter

Parámetros del componente Proveedor de protección para AMSI

| Parámetro | Descripción |
|---|---|
| **Analizar archivos de almacenamiento** | Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE. |
| **Analizar paquetes de distribución** | Use esta casilla para habilitar/deshabilitar el análisis de paquetes de distribución de terceros. |
| **Analizar archivos de Microsoft Office** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **No desempaquetar archivos compuestos grandes** | Si esta casilla está seleccionada, Kaspersky Endpoint Security no analiza los archivos compuestos si su tamaño excede el valor.<br>Si esta casilla está desactivada, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.<br>Kaspersky Endpoint Security analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla 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 malintencionado. El ataque permite al exploit instalar malware sin autorización.

Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

Configuración del componente Prevención de exploits

| Parámetro | Descripción |
|---|---|
| **Ante la detección de exploit** | • **Bloquear operación**. Cuando esta opción está seleccionada y se detecta un exploit, Kaspersky Endpoint Security bloquea todas las acciones que intenta llevar a cabo el exploit.<br>• **Informar**. Cuando esta opción está seleccionada y se detecta un exploit, Kaspersky Endpoint Security agrega información sobre el exploit a la lista de amenazas activas, pero no bloquea sus acciones. |
| **Habilitar la protección de la memoria de procesos del sistema** | Si se activa este interruptor, Kaspersky Endpoint Security bloquea los procesos externos que intentan acceder a la memoria de los procesos del sistema. |

## Detección de comportamientos

El componente Detección de comportamientos recibe datos sobre las acciones de las aplicaciones del equipo y transmite esta información a los demás componentes de protección para mejorar su rendimiento.

El componente Detección de comportamientos utiliza firmas de patrones de comportamiento para aplicaciones. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Endpoint Security realiza la acción de respuesta especificada. Las funcionalidades de Kaspersky Endpoint Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo.

Parámetros del componente Detección de comportamientos

| Parámetro | Descripción |
|---|---|
| **Al detectar actividad de malware** | • **Eliminar archivo**. Si se elige esta opción, cuando se detecta actividad malintencionada, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación perjudicial y crea una copia de seguridad del archivo en Copia de seguridad.<br>• **Finalizar la aplicación**. Si se elige esta opción, cuando se detecta actividad malintencionada, Kaspersky Endpoint Security finaliza la aplicación.<br>• **Informar**. Si se elige esta opción, cuando se detecta actividad malintencionada de parte de una aplicación, Kaspersky Endpoint Security permite que la aplicación se siga ejecutando, pero agrega información sobre la actividad malintencionada de esta aplicación a la lista de amenazas activas. |
| **Habilitar protección de carpetas** | Si se activa el interruptor, Kaspersky Endpoint Security analiza la actividad de las carpetas compartidas. Cuando la actividad coincide con una firma de patrones de comportamiento |

| | |
|---|---|
| **compartidas contra el cifrado externo** | que suele verse en actos de cifrado externo, Kaspersky Endpoint Security realiza la acción seleccionada.<br><br>Kaspersky Endpoint Security evita el cifrado externo de solo esos archivos que se localizan en medios que tienen el sistema de archivos NTFS y no están cifrados por el sistema EFS.<br><br>• **Informar**. Si se elige esta opción, cuando se detecta un intento de modificar los archivos de una carpeta compartida, Kaspersky Endpoint Security agrega información sobre el hecho a la lista de amenazas activas.<br><br>• **Bloquear conexión**. Si se elige esta opción, cuando se detecta un intento de modificar los archivos de una carpeta compartida, Kaspersky Endpoint Security bloquea la actividad de red que proviene del equipo en el que se originó el intento y crea copias de seguridad de los archivos modificados.<br><br>Si el componente Motor de reparación se habilita y la opción **Bloquear conexión** se selecciona, Kaspersky Endpoint Security restaura los archivos modificados desde copias de seguridad. |
| **Bloquear conexión por N minutos** | El tiempo durante el cual Kaspersky Endpoint Security bloquea la actividad de red del equipo remoto que realiza el cifrado de carpetas compartidas. |
| **Exclusiones** | La lista de equipos desde los cuales los intentos de cifrar carpetas compartidas no se supervisarán.<br><br>Para aplicar la lista de equipos excluidos de la protección de carpetas compartidas contra el cifrado externo, deberá habilitar la opción "Auditar inicio de sesión" en la directiva de auditoría de seguridad de Windows. De manera predeterminada, la opción "Auditar inicio de sesión" no está habilitada. Para obtener más información sobre la directiva de auditoría de seguridad de Windows, visite el *sitio web de Microsoft*. |

## Prevención contra intrusos

El componente Prevención contra intrusos impide que las aplicaciones realicen acciones que puedan ser peligrosas para el sistema operativo y garantiza el control del acceso a los recursos del sistema operativo y a los datos personales. Para proteger el equipo, el componente se vale de la ayuda de las bases de datos antivirus y el servicio de nube Kaspersky Security Network.

Para controlar el funcionamiento de las aplicaciones, el componente se basa en los *derechos* que estas tienen asignados. Los siguientes parámetros de acceso son algunos de esos derechos:

- Acceso a los recursos del sistema operativo (claves del Registro, opciones de ejecución automática, etc.)
- Acceso a datos personales (archivos, aplicaciones, etc.)

Para controlar la actividad de red de las aplicaciones, se utilizan las *reglas de red* del componente Firewall.

Cuando una aplicación se inicia por primera vez, el componente Prevención de intrusiones en el host hace lo siguiente:

1. Analiza la aplicación con las bases de datos antivirus descargadas para verificar si es segura.
2. Verifica si la aplicación se considera segura en Kaspersky Security Network.

   Para aumentar la eficacia del componente Prevención de intrusiones en el host, se recomienda participar en Kaspersky Security Network.

3. Ubica la aplicación en uno de los *grupos de confianza*: De confianza, Restricción mínima, Restricción máxima o No confiables.

   Los grupos de confianza determinan los derechos en los que Kaspersky Endpoint Security se basa para controlar la actividad de las aplicaciones. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo.

   Cuando Kaspersky Endpoint Security asigna una aplicación a un grupo de confianza, la asignación es válida tanto para Firewall como para Prevención de intrusiones en el host. No es posible introducir un cambio de grupo que afecte únicamente a Firewall o únicamente a Prevención de intrusiones en el host.

   Si opta por no participar en KSN o si no hay conexión a la red, Kaspersky Endpoint Security determinará el grupo de confianza de una aplicación basándose en la configuración del componente Prevención de intrusiones en el host. Si finalmente se obtiene la reputación de KSN, la aplicación puede cambiar de grupo de confianza automáticamente.

4. Bloquea las acciones de la aplicación tomando como referencia el grupo de confianza al que pertenece. Por ejemplo, las aplicaciones del grupo Restricción máxima no pueden acceder a los módulos del sistema operativo.

Cuando la aplicación se inicia por segunda vez, Kaspersky Endpoint Security comprueba que no tenga problemas de integridad. Cuando la aplicación no presenta modificaciones, el componente usa los derechos que ya están vigentes para ella. Si la aplicación presenta modificaciones, Kaspersky Endpoint Security la analiza como si se la estuviera iniciando por primera vez.

Configuración del componente Prevención contra intrusos

| Parámetro | Descripción |
| --- | --- |
| **Derechos de aplicaciones** | **Aplicaciones**<br>Tabla de aplicaciones controladas por el componente Prevención de intrusiones en el host. Cada aplicación está asignada a un grupo de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones.<br><br>Puede elegir una aplicación de una lista única en la que se recogen todas las aplicaciones instaladas en los equipos sujetos a una directiva y agregarla a un grupo de confianza.<br><br>Los derechos de acceso de las aplicaciones se recogen en las siguientes tablas: |

| | |
|---|---|
| | • **Archivos y Registro del sistema**. En esta tabla se muestran los permisos que tienen las aplicaciones de un grupo de confianza para acceder a los recursos del sistema operativo y a los datos personales.<br>• **Derechos**. En esta tabla se muestran los permisos que tienen las aplicaciones de un grupo de confianza para acceder a los procesos y a los recursos del sistema operativo.<br>• **Reglas de red**. Tabla con las reglas de red que se han definido para las aplicaciones de un grupo de confianza. Las reglas le indican a Firewall cómo debe regular la actividad de red de las aplicaciones. La tabla contiene reglas de red predefinidas y recomendadas por los especialistas de Kaspersky. Dichas reglas se han incluido porque permiten proteger el tráfico de red de los equipos con Windows del mejor modo posible. Las reglas de red predefinidas no se pueden eliminar. |
| **Recursos protegidos** | **Nombre**<br>La tabla contiene recursos del equipo clasificado. El componente Prevención contra intrusos supervisa los intentos de otras aplicaciones de tener acceso a los recursos de la tabla.<br>Un recurso puede ser una categoría de registro, archivo, carpeta o clave de registro.<br>**Aplicaciones**<br>Tabla de aplicaciones que el componente Prevención de intrusiones en el host controla en el contexto del recurso seleccionado. Cada aplicación está asignada a un grupo de confianza. Los grupos de confianza definen los derechos que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones. |
| **Grupo de confianza para las aplicaciones que se ejecutan antes del inicio de Kaspersky Endpoint Security** | Grupo de confianza en el que se colocarán las aplicaciones que se inicien antes que Kaspersky Endpoint Security. |
| **Actualizar derechos para aplicaciones anteriormente desconocidas usando la base de datos de KSN** | Si se selecciona esta casilla, el componente Prevención contra intrusos usa la base de datos de Kaspersky Security Network para actualizar los derechos de las aplicaciones anteriormente desconocidas. |
| **Confiar en aplicaciones que tienen firma digital** | Si activa esta casilla, el componente Prevención de intrusiones en el host colocará las aplicaciones que tengan la firma digital de un proveedor de confianza en el grupo De confianza.<br>Se considera proveedor de confianza a todo aquel proveedor de software en el que confía Kaspersky. De ser necesario, puede agregar manualmente el certificado de un proveedor al almacén de certificados de confianza.<br>Si no activa esta casilla, el componente Prevención de intrusiones en el host no dará por sentado que tales aplicaciones sean de confianza y usará otros parámetros para determinar el grupo de confianza al que las asignará. |
| **Eliminar los derechos para aplicaciones que no se han** | Si esta casilla está activada, Kaspersky Endpoint Security eliminará automáticamente la información (grupo de confianza y derechos de acceso) de una aplicación para la que se cumplan las siguientes condiciones: |

| | |
|---|---|
| **iniciado durante más de N días** | • El grupo de confianza o los derechos de acceso de la aplicación se definieron manualmente.<br>• La aplicación no se inició en ningún punto del período definido.<br>Cuando el grupo de confianza y los derechos de una aplicación se determinaron automáticamente, Kaspersky Endpoint Security elimina la información de esa aplicación luego de 30 días. El plazo de almacenamiento de la información no se puede modificar, y tampoco es posible desactivar la eliminación automática.<br>Cuando vuelva a iniciar una aplicación cuya información se haya eliminado, Kaspersky Endpoint Security la analizará como si fuera la primera vez que se la ejecuta. |
| **Grupo de confianza para las aplicaciones que no pudieron agregarse a grupos ya existentes** | Los elementos en esta lista desplegable determinan a qué grupo de confianza Kaspersky Endpoint Security asignará una aplicación desconocida.<br>Puede elegir uno de los siguientes elementos:<br>• **Restricción mínima**.<br>• **Restricción máxima**.<br>• **No confiables**. |

## Motor de reparación

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

Al revertir la actividad del malware en el sistema operativo, Kaspersky Endpoint Security gestiona los siguientes tipos de actividad de malware:

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red).
  - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado.
  - Restaura los archivos que el malware ha modificado o eliminado.

  La capacidad de recuperar archivos está sujeta a algunas limitaciones.

- **Actividad del Registro**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina las claves del Registro que el malware ha creado.
  - No restaura las claves del Registro que el malware ha eliminado o modificado.

- **Actividad del sistema**

  Kaspersky Endpoint Security realiza las siguientes acciones:

- Finaliza los procesos iniciados por el malware.
- Finaliza los procesos en los cuales ha penetrado una aplicación malintencionada.
- No reanuda procesos que el malware haya suspendido.

- **Actividad de 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.

La reversión de las operaciones del malware afecta a un conjunto de datos estrictamente definido. La reversión no tiene efectos negativos en el sistema operativo ni en la integridad de los datos de su equipo.

# Kaspersky Security Network

A fin de proteger el equipo con mayor eficacia, Kaspersky Endpoint Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

*Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Endpoint Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, 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 invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios pueden iniciar o discontinuar su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el sitio web de Kaspersky contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. Encontrará el texto de la Declaración de Kaspersky Security Network en el archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación.

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*. A través de esta solución, quienes utilizan Kaspersky Endpoint Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky Security Network, así como a otras clases de información estadística, sin enviar información de sus equipos a KSN. 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 manera predeterminada, Kaspersky Security Center utiliza KSN Global. Si desea utilizar KSN Privada, puede hacer los cambios de configuración pertinentes con la Consola de administración (MMC), a través de Kaspersky Security Center 12 Web Console o desde la línea de comandos. No es posible usar Kaspersky Security Center Cloud Console para este fin.

Para más información sobre KSN Privada, consulte la documentación de Kaspersky Private Security Network.

## Proxy de KSN

Los equipos de usuarios administrados por el Servidor de administración de Kaspersky Security Center pueden interactuar con KSN a través del servicio Proxy de KSN.

El servicio Proxy de KSN ofrece las siguientes capacidades:

- El equipo del usuario puede consultar KSN y enviarle información, incluso sin 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 *Guía de ayuda de Kaspersky Security Center*.

Parámetros de Kaspersky Security Network

| Parámetro | Descripción |
|---|---|
| **Habilitar modo KSN extendido** | El *modo KSN extendido* es un modo por el cual Kaspersky Endpoint Security remite información adicional a Kaspersky. Kaspersky Endpoint Security utiliza KSN para detectar amenazas independientemente del estado del interruptor. |
| **Habilitar modo nube** | *Modo nube* es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky.<br><br>Si el interruptor está activado, Kaspersky Endpoint Security usa una versión reducida de las bases de datos antivirus para tener un menor impacto en los recursos del sistema operativo. |

| | |
|---|---|
| | Kaspersky Endpoint Security descarga la versión ligera de bases de datos antivirus durante la siguiente actualización después de que la casilla se seleccionó.<br><br>Si el interruptor está desactivado, Kaspersky Endpoint Security usa la versión completa de las bases de datos antivirus.<br><br>Kaspersky Endpoint Security descarga la versión completa de bases de datos antivirus durante la siguiente actualización después de que la casilla se desactivó. |
| **Estado del equipo cuando los servidores de KSN no estén disponibles**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Con los elementos de esta lista desplegable, puede indicar qué estado tendrá un equipo en Kaspersky Security Center cuando los servidores de KSN no estén disponibles. |
| **Utilizar proxy de KSN**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Cuando esta casilla está activada, Kaspersky Endpoint Security usa el servicio proxy de KSN. Los parámetros de este servicio se configuran a través de las propiedades del Servidor de administración. |
| **Utilizar servidores de KSN cuando el proxy de KSN no esté disponible**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky (cuando se utiliza KSN Global) como en la de terceros (cuando se utiliza KSN Privada). |

## 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 intente abrir un sitio web restringido por Control web, Kaspersky Endpoint Security bloqueará el acceso y le mostrará al usuario una advertencia (vea la siguiente imagen).

Kaspersky Endpoint Security solo puede supervisar tráfico HTTP y HTTPS.

Para que la aplicación pueda supervisar el tráfico HTTPS, es necesario habilitar 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. Puede impedir que sus usuarios accedan a sitios catalogados como “Redes sociales", por ejemplo, o a otras categorías.
- **Tipo de datos**. Puede restringir el acceso a ciertos tipos de datos y, por ejemplo, ocultar las imágenes de un sitio web. Kaspersky Endpoint Security determina los tipos de datos basándose en el formato de los archivos, no en sus extensiones.

  Kaspersky Endpoint Security no analiza el contenido de los archivos de almacenamiento. Por ello, si un grupo de imágenes está incluido en un archivo de almacenamiento, Kaspersky Endpoint Security considerará que el tipo de datos es "Archivos de almacenamiento" en lugar de "Archivos de imagen".

- **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 la web".

## Reglas de acceso a sitios web

Control web regula el acceso de los usuarios a los sitios web a través de *reglas de acceso*. Para cada una de estas reglas, puede configurar las siguientes opciones avanzadas:

- Usuarios alcanzados por la regla.

  Permite, por ejemplo, restringir el uso de un navegador para acceder a Internet para todos los usuarios de la empresa, excepto los empleados del departamento de TI.

- Programación de la regla.

  Permite, por ejemplo, restringir el acceso a Internet a través de un navegador solo durante el horario laboral.

## Prioridad de las reglas de acceso

Cada regla tiene una prioridad. Cuanto más arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado a más de una regla. Puede suceder, por ejemplo, que Kaspersky Endpoint Security considere que un portal corporativo es una red social. Para restringir las visitas a las redes sociales y permitir que se acceda al portal web corporativo, deberá crear dos reglas: una que bloquee la categoría de sitios web "Redes sociales" y una que permita el acceso al portal web corporativo. La regla de acceso para el portal web corporativo deberá tener mayor prioridad que la regla de acceso de las redes sociales.


Mensajes de Control web

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 arriba en la lista se encuentra una regla, mayor es su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado a más de una regla. |
| **Regla predeterminada** | La *regla predeterminada* regula el acceso a los recursos web que no están contemplados en ninguna otra regla. Están disponibles los siguientes opciones:<br>• **Permitir todo excepto la lista de reglas**, también denominado modo de lista de bloqueo para sitios web prohibidos.<br>• **Bloquear todo excepto la lista de reglas**, también denominado modo de lista de autorización para sitios web permitidos. |
| **Plantillas de mensajes** | • **Advertencia**. El campo de entrada consiste en una plantilla del mensaje que se muestra si se activa una regla de advertencia acerca de intentos para acceder a un recurso web no deseado.<br>• **Mensaje para bloqueos**. El campo de entrada contiene la plantilla del mensaje que se muestra si se activa una regla que bloquea el acceso a un recurso web.<br>• **Mensaje para el administrador**. El campo de entrada contiene la plantilla del mensaje que se enviará al administrador de la red de área local si el usuario considera que se ha bloqueado por error. |

| | |
|---|---|
| **Registrar el acceso a páginas permitidas** | Kaspersky Endpoint Security dejará constancia de todos los sitios web que se visiten, incluso cuando se trate de sitios web permitidos. Kaspersky Endpoint Security envía eventos a Kaspersky Security Center, al registro local de Kaspersky Endpoint Security y al registro de eventos de Windows. Para supervisar las actividades de los usuarios en Internet, deberá configurar los ajustes de almacenamiento de eventos.<br><br>Si opta por supervisar las actividades en línea de los usuarios, la carga del equipo podría aumentar cuando se necesite descifrar tráfico HTTPS. |

# Control de dispositivos

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El Control de dispositivos administra el acceso de los usuarios a los dispositivos que se instalan o se conectan al equipo (por ejemplo, discos duros, cámaras o módulos Wi-Fi). Esto impide la infección del equipo cuando se conectan dichos dispositivos y evita las pérdidas o fugas de datos.

## Niveles de acceso a dispositivos

El Control de dispositivos controla el acceso a los siguientes niveles:

- **Tipo de dispositivo**. Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

  Puede configurar el acceso a los dispositivos de la siguiente manera:

  - Permitir – .
  - Bloquear – .
  - Depende del bus de conexión (excepto Wi-Fi) – .
  - Bloquear con excepciones (solamente con Wi-Fi) – .

- **Bus de conexión**. El *bus de conexión* es una interfaz utilizada para conectar dispositivos al equipo (por ejemplo, USB o FireWire). De esta forma, puede restringir la conexión de todos los dispositivos, por ejemplo, a través de USB.

  Puede configurar el acceso a los dispositivos de la siguiente manera:

  - Permitir – .
  - Bloquear – .

- **Dispositivos de confianza**. Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

  Puede agregar dispositivos de confianza en función de los siguientes datos:

- **Dispositivos por Id.** Cada dispositivo tiene un identificador único (id. de hardware, también denominado HWID). Puede ver el Id. en las propiedades del dispositivo usando las herramientas del sistema operativo. Un id. de dispositivo típico podría ser `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Si necesita agregar varios dispositivos específicos, recomendamos agregarlos por id.

- **Dispositivos por modelo**. Cada dispositivo tiene un id. de proveedor (VID) y un id. de producto (PID). Puede ver los ID. en las propiedades del dispositivo usando las herramientas del sistema operativo. Los valores VID y PID deben especificarse en este formato: `VID_1234&PID_5678`. Si su organización cuenta con varios dispositivos de un mismo modelo, recomendamos que los agregue por modelo. Podrá agregar todos los dispositivos del mismo modelo con facilidad.

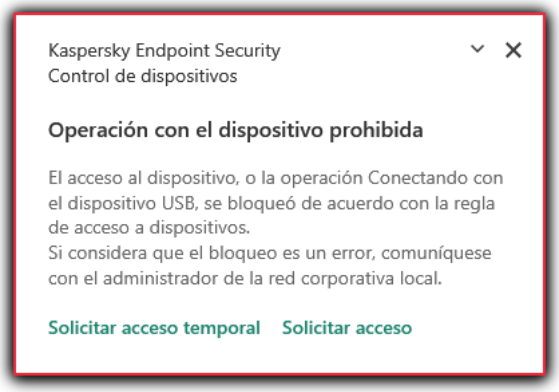
- **Dispositivos por máscara de id.** Si tiene dispositivos con identificadores similares, puede agregarlos a la lista de dispositivos de confianza utilizando máscaras. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Una máscara típica podría ser `WDC_C*`.

- **Dispositivos por máscara de modelo**. Si tiene dispositivos con identificadores VID o PID similares (por ejemplo, dispositivos de un mismo fabricante), puede utilizar máscaras para agregarlos a la lista de dispositivos de confianza. El carácter `*` le permitirá representar cuantos caracteres sea necesario. En Kaspersky Endpoint Security, las máscaras de id. no pueden contener el carácter `?`. Por ejemplo, `VID_05AC & PID_ *`.

El Control de dispositivos regula el acceso de los usuarios a los dispositivos usando *reglas de acceso*. El Control de dispositivos también le permite guardar eventos relacionados con la conexión/desconexión de dispositivos. Para guardar eventos, tiene que configurar el registro de eventos en una directiva.

Cuando el acceso a un dispositivo dependa del bus de conexión (estado ), Kaspersky Endpoint Security no guardará ningún evento relacionado con la conexión o desconexión del dispositivo. Para que Kaspersky Endpoint Security guarde los eventos relacionados con la conexión/desconexión de dispositivos, autorice el acceso al tipo de dispositivo correspondiente (estado ) o agregue el dispositivo a la lista de dispositivos de confianza.

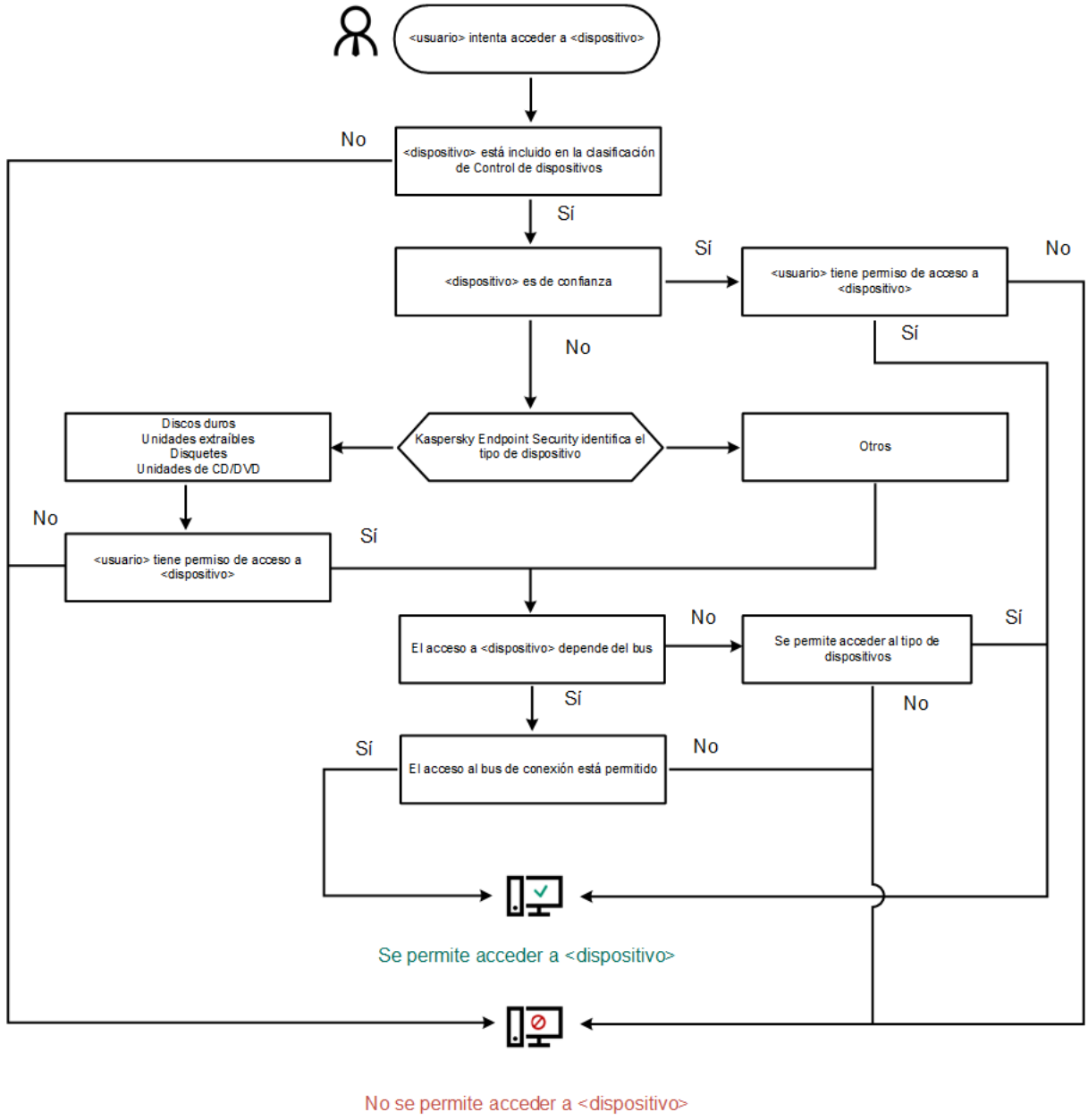
Cuando se conecta al equipo un dispositivo que está bloqueado por el Control de dispositivos, Kaspersky Endpoint Security bloqueará el acceso y mostrará que una notificación (consulte la figura a continuación).




Notificación del Control de dispositivos

## Algoritmo de funcionamiento del Control de dispositivos

Kaspersky Endpoint Security decide si permitirá el acceso a un dispositivo después de que el usuario conecta el dispositivo al equipo de la siguiente imagen.




Algoritmo de funcionamiento del Control de dispositivos

Si conecta un dispositivo y se le permite acceder a él, puede editar la regla de acceso y bloquear la posibilidad de utilizarlo. Cuando alguien intente acceder al dispositivo nuevamente (por ejemplo, para ver la estructura de carpetas o para realizar una operación de lectura o escritura), Kaspersky Endpoint Security bloqueará el acceso. Un dispositivo sin un sistema de archivos se bloqueará solo la próxima vez que el dispositivo se conecte.

Si un usuario del equipo con Kaspersky Endpoint Security instalado debe solicitar acceso a un dispositivo que cree fue bloqueado por error, envíe al usuario las instrucciones para solicitar acceso.

La configuración del componente Control de Dispositivos

| Parámetro | Descripción |
| --- | --- |
| **Permitir solicitudes de acceso temporal** | Si se selecciona la casilla, el botón **Solicitar acceso** estará disponible a través de la interfaz local de Kaspersky Endpoint Security. Al hacer clic en este botón, se abrirá la ventana **Solicitar acceso al dispositivo**. En esta ventana, el usuario puede solicitar acceso temporal a un dispositivo bloqueado. |

| | |
|---|---|
| *(disponible solo en la Consola de Kaspersky Security Center)* | |
| **Dispositivos y redes Wi-Fi** | Esta tabla muestra todos los tipos de dispositivos posibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso. |
| **Buses de conexión** | Una lista con todos los buses de conexión disponibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso. |
| **Dispositivos de confianza** | Una lista con los dispositivos de confianza y los usuarios que tienen acceso a esos dispositivos. |
| **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.<br><br>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.<br><br>Cuando una conexión activa y una conexión nueva son del mismo tipo (por ejemplo, Wi-Fi), Kaspersky Endpoint Security bloquea la conexión activa y permite que se establezca la conexión nueva.<br><br>Cuando una conexión activa y una conexión nueva no son del mismo tipo (por ejemplo, adaptador de red y Wi-Fi), Kaspersky Endpoint Security bloquea la conexión de menor prioridad y autoriza la de mayor prioridad.<br><br>Anti-Bridging puede operar con los siguientes tipos de dispositivos: adaptador de red, Wi-Fi y módem. |
| **Plantillas de mensajes** | • **Mensaje para bloqueos**. Plantilla del mensaje que aparece cuando un usuario intenta acceder a un dispositivo bloqueado. Este es el mismo mensaje que se muestra cuando un usuario intenta realizar una operación que tiene prohibida con el contenido del dispositivo.<br><br>• **Mensaje para el administrador**. Plantilla del mensaje que se envía al administrador de la red de área local cuando el usuario considera que el acceso a un dispositivo se ha bloqueado por error o, de manera similar, que la posibilidad de realizar una operación con el contenido de un dispositivo se ha bloqueado por error. |

## Control de aplicaciones

El componente Control de aplicaciones se utiliza para gestionar la ejecución de aplicaciones en los equipos de los usuarios. Permite, con ello, implementar una política de seguridad corporativa que regule el uso de aplicaciones. Gracias a las restricciones de acceso, el componente también ayuda a reducir el riesgo de que los equipos se infecten.

Los pasos para configurar Control de aplicaciones son los siguientes:

1. Creación de categorías de aplicaciones.

   El administrador crea categorías con las aplicaciones que desea controlar. Las categorías de aplicaciones impactan en todos los equipos de una red corporativa, independientemente del grupo de administración al que pertenecen. Las categorías se crean sobre la base de distintos criterios: categoría KL (por ejemplo, *Navegadores*), hash del archivo, proveedor de la aplicación y otros.

2. Creación de reglas de Control de aplicaciones.

   El administrador crea reglas de Control de aplicaciones dentro de la directiva asignada a un grupo de administración. Las reglas contienen las distintas categorías de aplicaciones y el estado de ejecución (inicio permitido o bloqueado) asignado a las aplicaciones de esas categorías.

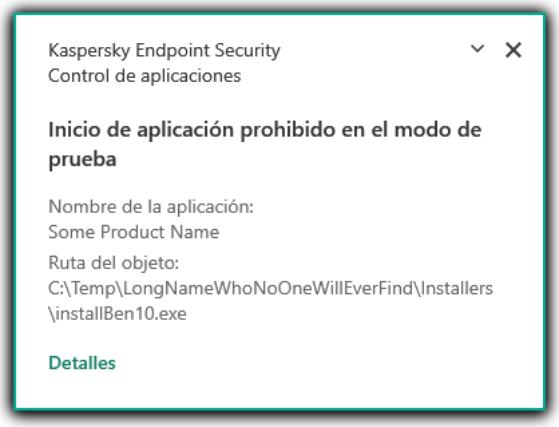
3. Selección del modo de Control de aplicaciones.

   El administrador decide el modo para trabajar con aplicaciones que no están contempladas en ninguna de las reglas (lista de autorización y de bloqueo).

Cuando un usuario intenta ejecutar una aplicación prohibida, Kaspersky Endpoint Security se lo impide y le muestra una notificación (vea la imagen de más abajo).

Existe un *modo de prueba*, diseñado para verificar la configuración de Control de aplicaciones. Cuando se utiliza este modo, Kaspersky Endpoint Security hace lo siguiente:

- Permite que se ejecute cualquier aplicación, esté o no prohibida.
- Muestra una notificación cuando se inicia una aplicación prohibida y agrega el evento al informe almacenado en el equipo del usuario.
- Transfiere información sobre la ejecución de aplicaciones prohibidas a Kaspersky Security Center.




Notificación de Control de aplicaciones

## Modos de funcionamiento de Control de aplicaciones

El componente Control de aplicaciones funciona en dos modos:

- **Lista de bloqueo**. En este modo, Control de aplicaciones permite que los usuarios inicien cualquier aplicación, excepto por las que se hayan prohibido a través de las reglas de Control de aplicaciones.

  Este modo de Control de aplicaciones está habilitado por defecto.

- **Lista de autorización**. En este modo, Control de aplicaciones no permite que ningún usuario inicie ninguna aplicación, excepto por las que se hayan permitido (y no prohibido) a través de las reglas de Control de aplicaciones.

Si se configuran completamente las reglas de autorización del Control de aplicaciones, el componente bloquea el inicio de todas las aplicaciones nuevas que no han sido verificadas por el administrador de la red LAN, mientras que permite el funcionamiento del sistema operativo y de las aplicaciones de confianza de las que dependen los usuarios para hacer su trabajo.

Puede leer las recomendaciones sobre cómo configurar las reglas de control de aplicaciones en el modo de lista de autorización.

El Control de aplicaciones se puede configurar para funcionar en estos modos, tanto a través de la interfaz local de Kaspersky Endpoint Security como por medio de Kaspersky Security Center.

Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas necesarias para las siguientes tareas:

- Creación de categorías de aplicaciones.

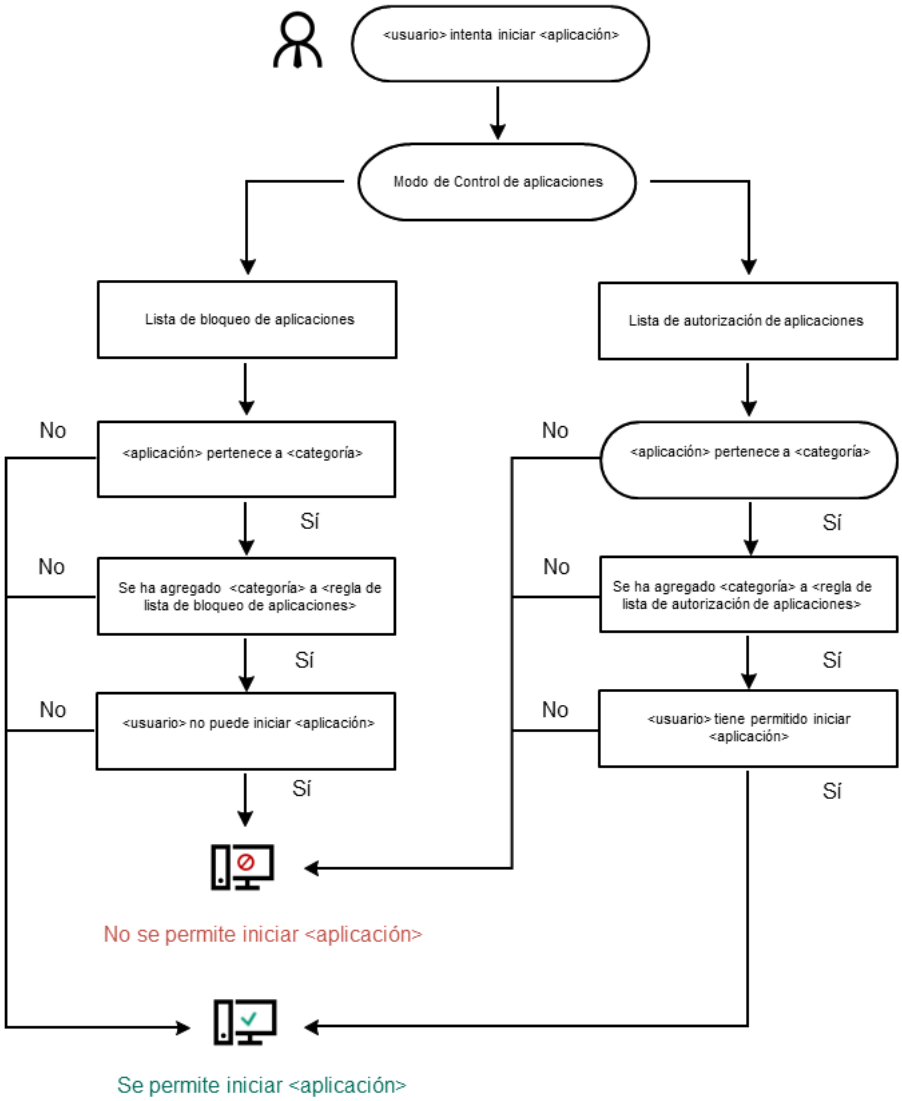
  Las reglas de Control de aplicaciones creadas en la Consola de administración de Kaspersky Security Center se basan en sus categorías de aplicaciones personalizadas, y no en condiciones de inclusión y exclusión como es el caso de la interfaz local de Kaspersky Endpoint Security.

- Recepción de información sobre aplicaciones que se instalan en equipos de redes LAN.

Por este motivo se recomienda utilizar Kaspersky Security Center para configurar el funcionamiento del componente Control de aplicaciones.

## Algoritmo de funcionamiento de Control de aplicaciones

Kaspersky Endpoint Security utiliza un algoritmo para decidir si una aplicación podrá iniciarse (vea la siguiente imagen).




Algoritmo de funcionamiento de Control de aplicaciones

Parámetros del componente Control de aplicaciones

| Parámetro | Descripción |
|---|---|
| **Modo de prueba** | Si se activa el 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. |
| **Modo de Control de aplicaciones** | Puede elegir una de las siguientes opciones:<br>• **Lista de bloqueo**. Si se selecciona esta opción, el Control de aplicaciones permite que todos los usuarios inicien cualquier aplicación, excepto en casos en que las aplicaciones cumplan con las condiciones de las reglas de bloqueo de Control de aplicaciones.<br>• **Lista de autorización**. Si se selecciona esta opción, el Control de aplicaciones bloquea a todos los usuarios de iniciar alguna aplicación, excepto en casos en que las aplicaciones cumplen con las condiciones de reglas de habilitación del Control de aplicaciones.<br>Cuando se selecciona el modo **Lista de autorización**, se crean automáticamente dos Reglas de control de aplicaciones: |

| | |
|---|---|
| | • **Imagen de oro**.<br>• **Actualizadores de confianza**.<br>No puede modificar la configuración ni eliminar las reglas creadas automáticamente. Puede habilitar o deshabilitar estas reglas. |
| **DLL de control** | Si se selecciona la casilla, Kaspersky Endpoint Security controla la carga de módulos de DLL cuando los usuarios intentan iniciar aplicaciones. En el informe se registra información acerca del módulo de DLL y la aplicación que cargó el mismo.<br>Si planea supervisar la carga de controladores y módulos DLL, asegúrese de que una de las siguientes reglas esté habilitada en la configuración de Control de aplicaciones: la **Imagen de oro** predeterminada u otra regla que contenga la categoría KL "Certificados de confianza" y que garantice que los módulos DLL y los controladores de confianza se carguen antes del arranque de Kaspersky Endpoint Security. Habilitar la supervisión de la carga de módulos DLL y controladores cuando la regla **Imagen de oro** está deshabilitada puede causar inestabilidad en el sistema operativo.<br>Kaspersky Endpoint Security solamente supervisa los módulos DLL y los controladores cargados desde que se seleccionó la casilla. Después de seleccionar la casilla, se recomienda reiniciar el equipo para asegurarse de que la aplicación supervise todos los módulos y los controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security. |
| **Plantillas de mensajes** | **Mensaje para bloqueos**. Plantilla del mensaje que se muestra al activarse una regla de Control de aplicaciones que impide iniciar una aplicación.<br>**Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la LAN corporativa si considera que una aplicación se bloqueó por error. |

## Control de anomalías adaptativo

Este componente solo está disponible en Kaspersky Endpoint Security for Business Advanced y Kaspersky Total Security for Business. Para más información sobre Kaspersky Endpoint Security for Business, visite el *sitio web de Kaspersky*.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

El componente Control de anomalías adaptativo detecta y bloquea acciones que no son típicas de los equipos conectados a una red corporativa. Para ello utiliza una serie de reglas, diseñadas para buscar comportamientos que no se consideran usuales (por ejemplo, la regla *Inicio de Microsoft PowerShell desde una aplicación de ofimática*). Los especialistas de Kaspersky crean estas reglas basándose en casos característicos de actividad maliciosa. La manera en que el Control de anomalías adaptativo responde ante cada regla es configurable; esto significa que, por ejemplo, es posible permitir la ejecución de scripts de PowerShell que se hayan creado para automatizar ciertos aspectos de un flujo de trabajo. Las reglas se actualizan junto con las bases de datos de Kaspersky Endpoint Security. No obstante, las actualizaciones para las reglas deben confirmarse manualmente.

## Configuración del Control de anomalías adaptativo

Los pasos para configurar el Control de anomalías adaptativo son los siguientes:

1. Usar el modo de aprendizaje del Control de anomalías adaptativo.

   Una vez que el Control de anomalías adaptativo se habilita, sus reglas entran en un *modo de aprendizaje*. Mientras dicho modo está activo, el Control de anomalías adaptativo monitorea la activación de las reglas y envía los eventos de activación a Kaspersky Security Center. El tiempo de aprendizaje varía según la regla. Quienes definen la duración son los expertos de Kaspersky. Lo normal es que el modo de aprendizaje esté activo por dos semanas.

   Si una regla no se activa en lo absoluto durante el período de aprendizaje, el componente considerará que las acciones asociadas con la regla son atípicas. En consecuencia, Kaspersky Endpoint Security bloqueará cualquier acción vinculada con esa regla.

   Si una regla sí se activa durante el período de aprendizaje, Kaspersky Endpoint Security dejará constancia de los eventos en el informe de activación de las reglas y en el repositorio **Activación de reglas en modo Aprendizaje inteligente**.

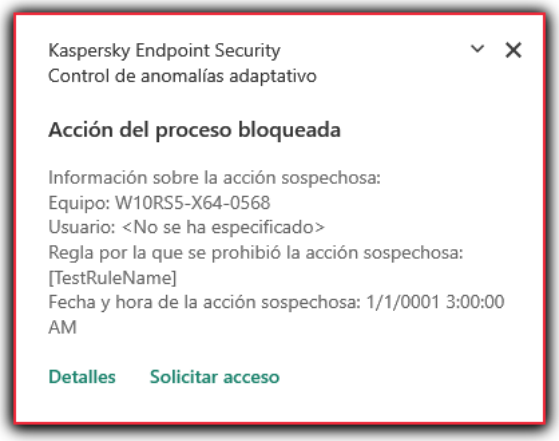
2. Analizar el informe de activación de las reglas.

   El administrador analiza el informe de activación de las reglas o el contenido del repositorio **Activación de reglas en modo Aprendizaje inteligente**. A continuación, selecciona cómo reaccionará el Control de anomalías adaptativo cuando se active una regla; las opciones posibles son permitir y bloquear. El administrador también puede optar por seguir controlando el funcionamiento de la regla y extender la duración del modo de aprendizaje. Si el administrador no realiza ninguna acción, la aplicación seguirá operando en modo de aprendizaje. El plazo de aprendizaje se reiniciará.

El componente Control de anomalías adaptativo se configura en tiempo real. Los canales de configuración son los siguientes:

- El Control de anomalías adaptativo comienza a bloquear automáticamente las acciones asociadas con las reglas que nunca se activaron en el modo de aprendizaje.
- Kaspersky Endpoint Security agrega reglas nuevas o elimina las que han quedado obsoletas.
- El administrador configura el funcionamiento del Control de anomalías adaptativo tras revisar el informe de activación de reglas y el contenido del repositorio **Activación de reglas en modo Aprendizaje inteligente**. Se recomienda revisar el informe de activación de reglas y el contenido **del repositorio Activación de reglas en modo Aprendizaje inteligente**.

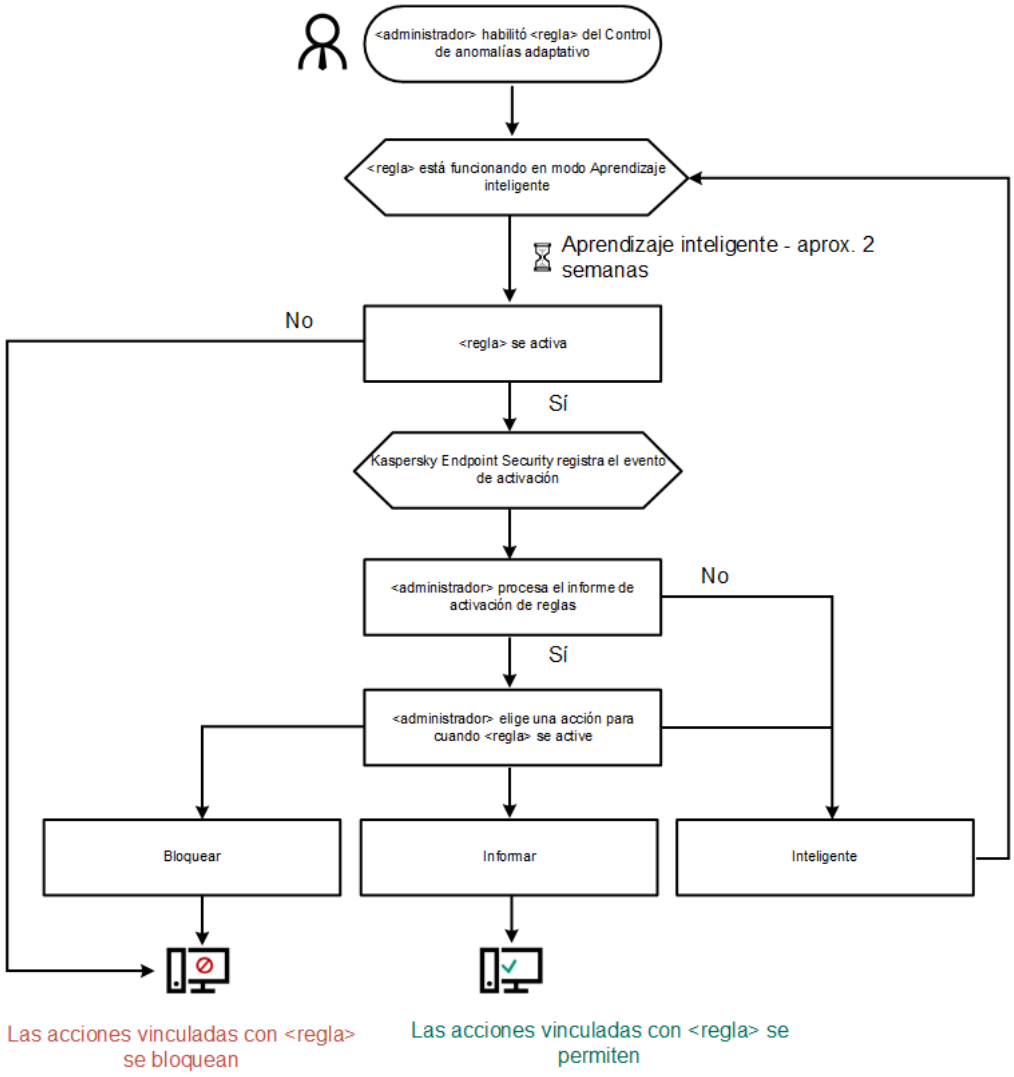
Cuando una aplicación maliciosa intente realizar una acción, Kaspersky Endpoint Security bloqueará el intento y mostrará una notificación (consulte la siguiente imagen).




Notificación del Control de anomalías adaptativo

## Algoritmo de funcionamiento del Control de anomalías adaptativo

Para determinar si una acción asociada a una regla debe permitirse o bloquearse, Kaspersky Endpoint Security usa el algoritmo de la siguiente imagen.




Algoritmo de funcionamiento del Control de anomalías adaptativo

Parámetros del componente Control de anomalías adaptativo

| Parámetro | Descripción |
|---|---|
| | |

| | |
|---|---|
| **Informe de estado de las reglas**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Informe sobre el estado asignado a las reglas de detección del Control de anomalías adaptativo (por ejemplo, *No* o *Bloquear*). El informe se genera para todos los grupos de administración. |
| **Informe de activación de las reglas**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Informe sobre las acciones atípicas detectadas por el Control de anomalías adaptativo. El informe se genera para todos los grupos de administración. |
| **Reglas** | Tabla de reglas del Control de anomalías adaptativo. Los especialistas de Kaspersky crean las reglas basándose en casos característicos de actividad potencialmente maliciosa. |
| **Plantillas** | • **Mensaje para bloqueos**. Plantilla del mensaje que se le mostrará al usuario cuando se active una regla del Control de anomalías adaptativo para bloquear una acción atípica.<br>• **Mensaje para el administrador**. Plantilla del mensaje que el usuario le puede enviar al administrador de la red local corporativa si considera que una acción se bloqueó por error. |

## Sensor de Endpoint

Sensor de Endpoint no forma parte de Kaspersky Endpoint Security 11.4.0.

Para administrar el componente Sensor de Endpoint, puede usar Kaspersky Security Center 12 Web Console o la Consola de administración de Kaspersky Security Center. No es posible usar Kaspersky Security Center Cloud Console para administrar Sensor de Endpoint.

*Sensor de Endpoint* es un componente diseñado para interactuar con Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* es una solución que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. Kaspersky Anti Targeted Attack Platform consta de dos bloques funcionales: Kaspersky Anti Targeted Attack (en adelante también denominada *KATA*) y Kaspersky Endpoint Detection and Response (en adelante también denominada *KEDR*). KEDR puede comprarse por separado. Para más detalles sobre la solución, *consulte la ayuda de Kaspersky Anti Targeted Attack Platform*.

La capacidad de administrar el componente Sensor de Endpoint está sujeta a ciertas restricciones:

- Los ajustes de Sensor de Endpoint pueden configurarse utilizando una directiva si el equipo tiene instalado Kaspersky Endpoint Security versiones 11.0.0 a 11.3.0. Si necesita información adicional para configurar los ajustes de Sensor de Endpoint a través de una directiva, consulte *los artículos de ayuda correspondientes a las versiones anteriores de Kaspersky Endpoint Security*.
- Los ajustes de Sensor de Endpoint no pueden configurarse a través de una directiva si el equipo tiene instalado Kaspersky Endpoint Security 11.4.0 o una versión posterior.

Sensor de Endpoint se instala en los equipos cliente. Una vez instalado, vigila de forma constante los procesos, las conexiones de red activas y los archivos que se modifican en esos equipos. El componente remite entonces la información al servidor de KATA.

La funcionalidad del componente está disponible con los siguientes sistemas operativos:

- Windows 7 Service Pack 1 Home/Professional/Enterprise
- Windows 8.1.1 Professional/Enterprise
- Windows 10 RS3 Home/Professional/Education/Enterprise
- Windows 10 RS4 Home/Professional/Education/Enterprise
- Windows 10 RS5 Home/Professional/Education/Enterprise
- Windows 10 RS6 Home/Professional/Education/Enterprise
- Windows Server 2008 R2 Foundation/Standard/Enterprise (64 bits)
- Windows Server 2012 Foundation/Standard/Enterprise (64 bits)
- Windows Server 2012 R2 Foundation/Standard/Enterprise (64 bits)
- Windows Server 2016 Essentials/Standard (64 bits)

Para obtener más información sobre el funcionamiento de KATA, *consulte la Guía de ayuda de Kaspersky Anti Targeted Attack Platform*.

## Cifrado de disco completo

Puede seleccionar una tecnología de cifrado: Cifrado de disco de Kaspersky o Cifrado disco de BitLocker (en adelante también llamado simplemente "BitLocker").

### Cifrado de Disco de Kaspersky

Una vez cifrados los discos duros del sistema, la próxima vez que se inicie el equipo, el usuario deberá superar la autenticación por medio del Agente de autenticación para poder acceder a los discos duros y cargar el sistema operativo. Para tal fin, podrá introducir la contraseña de un token o de una tarjeta inteligente que conecte al equipo, o el nombre de usuario y la contraseña de su cuenta del Agente de autenticación (cuenta que el administrador de la red de área local habrá creado con la tarea *Administrar cuentas del Agente de autenticación*). Estas cuentas se basan en las cuentas de Microsoft Windows con las que el usuario inicia sesión en el sistema operativo. Existe también la posibilidad de usar la tecnología de inicio de sesión único (SSO), que permite iniciar sesión en el sistema operativo automáticamente con el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

La autenticación de usuarios en el Agente de autenticación se puede realizar de dos formas:

- Ingrese el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red LAN que está utilizando las herramientas de Kaspersky Security Center.

- Ingrese la contraseña de un token o tarjeta inteligente conectados al equipo.

  El uso de un token o de una tarjeta inteligente está disponible solo si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, se rechazará la adición del archivo de certificado electrónico al comando.

## Cifrado de Unidad BitLocker

*BitLocker* es una tecnología de cifrado que forma parte de los sistemas operativos Windows. Kaspersky Endpoint Security permite controlar y administrar BitLocker a través de Kaspersky Security Center. La tecnología BitLocker está diseñada para cifrar volúmenes lógicos. No puede utilizarse para cifrar unidades extraíbles. Para más información sobre BitLocker, puede consultar la documentación de Microsoft.

Las claves de acceso de BitLocker pueden almacenarse de manera segura utilizando un TPM (módulo de plataforma segura). Un *módulo de plataforma segura (TPM)* es un microchip que ofrece funciones de seguridad fundamentales (entre ellas, la capacidad de almacenar claves de cifrado). Por lo general, el TPM forma parte de la placa madre del equipo e interactúa con los demás componentes del sistema a través de un bus físico. Es la opción más segura para almacenar las claves de acceso de BitLocker porque permite verificar la integridad del sistema antes del arranque. La ausencia de un TPM no es impedimento para cifrar las unidades de un equipo. En tal caso, se utiliza una contraseña para cifrar la clave de acceso. BitLocker permite emplear los siguientes métodos de autenticación:

- TPM.
- PIN y TPM,
- contraseña.

Cuando se cifra una unidad, BitLocker crea una clave maestra. Kaspersky Endpoint Security transfiere esa clave a Kaspersky Security Center; ello le permitirá restaurar el acceso a la unidad si un usuario olvida su contraseña, por ejemplo.

Si un usuario cifra su disco con BitLocker, Kaspersky Endpoint Security remitirá información sobre la operación a Kaspersky Security Center. Sin embargo, la clave maestra no se transferirá a Kaspersky Security Center, por lo que no será posible restaurar el acceso al disco a través de Kaspersky Security Center. Para que BitLocker pueda interactuar correctamente con Kaspersky Security Center, será necesario descifrar la unidad y utilizar una directiva para volver a cifrarla. El descifrado se puede realizar localmente o con una directiva.

Cuando la unidad del sistema está cifrada, el usuario debe superar la autenticación de BitLocker para iniciar el sistema operativo. BitLocker permitirá que el usuario inicie sesión una vez que se haya autenticado. BitLocker no es compatible con la tecnología de inicio de sesión único (SSO).

Si utiliza directivas de grupo de Windows, deshabilite el control de BitLocker en las mismas. Las directivas de Windows pueden interferir con las de Kaspersky Security Center. Tales interferencias pueden derivar en errores de cifrado.

Parámetros del componente Cifrado de disco de Kaspersky

| Parámetro | Descripción |
|---|---|
| **Modo de cifrado** | **Cifrar todos los discos duros**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación cifrará todos los discos duros. |

| | |
|---|---|
| | Si el equipo tiene varios sistemas operativos instalados, después del cifrado podrá solo cargar el sistema operativo que tenga la aplicación instalada.<br><br>**Descifrar todos los discos duros**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación descifrará todos los discos duros que se encuentren cifrados.<br><br>**Dejar sin modificar**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación no modificará el estado de las unidades. Si la unidad se cifra, permanece cifrada. Si la unidad se descifra, permanece descifrada. Este elemento está seleccionado por defecto. |
| **Durante el cifrado, crear cuentas del Agente de autenticación automáticamente para los usuarios de Windows** | Cuando esta casilla está activada, la aplicación crea cuentas del Agente de autenticación para las cuentas de usuario de Windows disponibles en el equipo. De manera predeterminada, Kaspersky Endpoint Security utiliza todas las cuentas locales y de dominio con las que el usuario haya iniciado sesión en el sistema operativo en los treinta días anteriores. |
| **Creación de cuentas del Agente de autenticación** | **Todas las cuentas del equipo**. Si se selecciona esta casilla, durante la ejecución de la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas del Agente de Autenticación para todas las cuentas del equipo que alguna vez han estado activas.<br><br>**Todas las cuentas de dominio del equipo**. Si se selecciona esta casilla, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas del Agente de autenticación para todas las cuentas del equipo que pertenecen a un dominio en particular que alguna vez han estado activas.<br><br>**Todas las cuentas locales del equipo**. Si se selecciona esta casilla, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea cuentas del Agente de autenticación para todas las cuentas locales del equipo que alguna vez han estado activas.<br><br>**Administrador local**. Si se selecciona esta casilla, durante la tarea de cifrado de disco completo, Kaspersky Endpoint Security crea una cuenta de administrador local.<br><br>**Administrador del equipo**. Si se selecciona esta casilla, 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.<br><br>**Cuenta activa**. Si se selecciona esta casilla, 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. |
| **Crear cuentas del Agente de autenticación automáticamente para todos los usuarios de este equipo cuando inicien sesión** | Si activa esta casilla de verificación, la aplicación analizará las cuentas de Windows disponibles en el equipo antes de que se inicie el Agente de autenticación. Si detecta que una cuenta de Windows no tiene su correspondiente cuenta para el Agente de autenticación, crea esa cuenta para que el usuario pueda acceder a las unidades cifradas de su equipo. La nueva cuenta del Agente de autenticación tendrá las siguientes opciones por defecto: inicio de sesión con contraseña únicamente y cambio de contraseña obligatorio tras el primer inicio de sesión. Gracias a esta función, ya no necesitará agregar cuentas del Agente de autenticación manualmente con la tarea *Administrar cuentas del Agente de autenticación* para los equipos que ya tengan sus unidades cifradas. |
| **Guardar el nombre de usuario ingresado en el Agente de autenticación** | Si se selecciona la casilla de verificación, la aplicación guarda el nombre de la cuenta del Agente de Autenticación. No se le solicitará que ingrese el nombre de la cuenta la próxima vez que intente completar la autorización en el Agente de Autenticación bajo la misma cuenta. |

| | |
|---|---|
| **Solo cifrar el espacio de disco usado** | Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado.<br><br>Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado.<br><br>Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se añaden.<br>Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente.<br><br>Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables.<br><br>Esta casilla está desactivada por defecto. |
| **Usar Legacy USB Support** | Utilice esta casilla para habilitar o deshabilitar la función Legacy USB Support. *Legacy USB Support* es una función de la BIOS o UEFI que permite utilizar dispositivos USB (por ejemplo, tokens de seguridad) durante el arranque del equipo, en la etapa anterior al inicio del sistema operativo (modo BIOS). La función Legacy USB Support no afecta la capacidad de usar dispositivos USB una vez que el sistema operativo se ha iniciado.<br><br>Si la casilla se selecciona, la compatibilidad con dispositivos USB durante el primer inicio del equipo se habilitará.<br><br>Si habilita la función Legacy USB Support y el Agente de autenticación se ha instalado en modo BIOS, no podrá usar tokens USB. Se recomienda usar esta opción solo cuando hay un problema de compatibilidad del hardware y solo para esos equipos en los cuales el problema ocurrió. |
| **Configuración de contraseñas** | Parámetros relativos a los requisitos de seguridad con los que deben cumplir las contraseñas de las cuentas del Agente de autenticación. También puede habilitar la tecnología de inicio de sesión único (SSO).<br>La tecnología SSO hace posible usar las mismas credenciales de cuenta para acceder a discos duros cifrados e iniciar sesión en el sistema operativo.<br>Si activa la casilla, será necesario introducir las credenciales de cuenta para acceder a los discos duros cifrados, pero el inicio de sesión en el sistema operativo se realizará automáticamente.<br>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. |
| **Textos de ayuda** | **Autenticación**. Texto que se muestra en la ventana del Agente de autenticación al momento de introducir las credenciales de cuenta. |

| | |
|---|---|
| | **Cambiar contraseña**. Texto que se muestra en la ventana del Agente de autenticación cuando se intenta cambiar la contraseña de la cuenta del Agente de autenticación.<br>**Recuperar contraseña**. Texto que se muestra en la ventana del Agente de autenticación cuando se intenta recuperar la contraseña de la cuenta del Agente de autenticación. |

Parámetros del componente Cifrado de unidad BitLocker

| Parámetro | Descripción |
|---|---|
| **Modo de cifrado** | **Cifrar todos los discos duros**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación cifrará todos los discos duros.<br>Si el equipo tiene varios sistemas operativos instalados, después del cifrado podrá solo cargar el sistema operativo que tenga la aplicación instalada.<br>**Descifrar todos los discos duros**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación descifrará todos los discos duros que se encuentren cifrados.<br>**Dejar sin modificar**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación no modificará el estado de las unidades. Si la unidad se cifra, permanece cifrada. Si la unidad se descifra, permanece descifrada. Este elemento está seleccionado por defecto. |
| **Habilitar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en pizarras** | Esta casilla de verificación habilita / deshabilita el uso de la autenticación que requiere el ingreso de datos en un entorno previo al inicio del sistema, aun si la plataforma no tiene la capacidad de ingreso previo al inicio del sistema (por ejemplo, con teclados de pantalla táctil en tabletas).<br>La pantalla táctil de las tabletas no está disponible en el entorno previo al inicio. Para completar la autenticación de BitLocker en tabletas, el usuario debe, por ejemplo, conectar un teclado USB.<br>Si se selecciona la casilla de verificación, se permite el uso de la autenticación que requiere ingreso previo al inicio del sistema. Se recomienda usar esta configuración solo para dispositivos que tienen herramientas alternativas de ingreso de datos en un entorno previo al inicio del sistema, como ser, un teclado USB además de teclados de pantalla táctil.<br>Para poder usar la tecnología Cifrado de unidad BitLocker en una tableta, esta casilla debe estar activada. |
| **Uso de cifrado del hardware** | Si se selecciona la casilla de verificación, la aplicación implementa cifrado del hardware. Esto le permite aumentar la velocidad de cifrado y usar menos recursos del equipo. |
| **Cifrar solo el espacio de disco usado (Windows 8 y versiones posteriores)** | Esta casilla habilita/deshabilita la opción que limita el área del cifrado solo con sectores del disco duro ocupados. Este límite le permite reducir el tiempo de cifrado.<br>Habilitar o deshabilitar la función **Cifrar solo el espacio de disco usado (reduce el tiempo de cifrado)** después de iniciar el cifrado no modifica esta configuración hasta que se descifran los discos duros. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado. |

| | |
|---|---|
| | Si se selecciona la casilla de verificación, solo se cifran partes del disco duro que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se añaden.<br>Si se desactiva la casilla de verificación, se cifra todo el disco duro, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente.<br>Esta opción se recomienda para discos duros nuevos cuyos datos no se han modificado o eliminado. Si está aplicando el cifrado a un disco duro que ya está en uso, le recomendamos que cifre todo el disco. Esto asegura la protección de todos los datos, incluso los datos eliminados que son potencialmente recuperables.<br>Esta casilla está desactivada por defecto. |
| **Parámetros de autenticación** | **Usar contraseña (Windows 8 y versiones posteriores)**<br>Si se selecciona esta opción, Kaspersky Endpoint Security le solicita al usuario una contraseña cuando intenta acceder a una unidad cifrada.<br>Esta opción se puede seleccionar cuando no se está utilizando un Módulo de plataforma segura (TPM).<br>**Usar el módulo de plataforma segura (TPM)**<br>Si se selecciona esta opción, BitLocker usa un Módulo de plataforma segura (TPM).<br>Un *módulo de plataforma segura (TPM)* es un microchip que ofrece funciones de seguridad fundamentales (entre ellas, la capacidad de almacenar claves de cifrado). Suele haber un Módulo de plataforma segura instalado en la placa madre del equipo y este módulo interactúa con todos los demás componentes del sistema a través del bus de hardware.<br>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.<br>Un dispositivo equipado con un Módulo de plataforma segura puede crear claves de cifrado que solo se pueden descifrar con el dispositivo. Un Módulo de plataforma segura cifra claves de cifrado con su propia clave de almacenamiento raíz. La clave de almacenamiento raíz se almacena dentro del Módulo de plataforma segura. Esto proporciona un nivel adicional de protección contra intentos de ataque a claves de cifrado.<br>Esta acción está seleccionada por defecto.<br>Puede establecer una capa de protección adicional para acceder a la clave de cifrado, y cifrar la clave con una contraseña o PIN:<br>• **Usar PIN para TPM**. Si activa esta casilla, los usuarios podrán usar un código PIN para obtener acceso a una clave de cifrado almacenada en un módulo de plataforma segura (TPM).<br>Si desactiva esta casilla, los usuarios no podrán usar un código PIN. Para acceder a la clave de cifrado, deberán utilizar una contraseña.<br>Puede permitir que el usuario use un código PIN mejorado. El *código PIN mejorado* permite usar otros caracteres además de los numéricos: letras latinas mayúsculas y minúsculas, caracteres especiales y espacios.<br>• **Usar el módulo de plataforma segura (TPM); si no está disponible, use la contraseña**. Si la casilla de verificación está seleccionada, el usuario puede usar |

| | |
|---|---|
| | una contraseña para obtener acceso a claves de cifrado cuando un módulo de plataforma segura (TPM) no está disponible.<br>Si desactiva esta casilla y no hay un módulo TPM disponible, la función de cifrado de disco completo no se iniciará. |

## Cifrado de archivos

Puede compilar listas de archivos por extensión o grupo de extensiones y listas de carpetas almacenadas en discos locales del equipo, además de crear reglas para cifrar archivos que son creados por aplicaciones específicas. Luego de que se aplique una directiva, Kaspersky Endpoint Security cifrará y descifrará los siguientes archivos:

- archivos agregados individualmente a listas para cifrado y descifrado;
- archivos almacenados en carpetas agregadas a listas para cifrado y descifrado;
- Archivos creados por aplicaciones por separado.

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

La característica de cifrado de archivos está sujeta a las siguientes consideraciones especiales:

- Kaspersky Endpoint Security cifrará o descifrará archivos en las carpetas predefinidas únicamente para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifrará ni descifrará ningún archivo que se encuentre en una carpeta redirigida o en las carpetas predefinidas de un perfil de usuario móvil, un perfil de usuario obligatorio o un perfil de usuario temporal.
- Kaspersky Endpoint Security no cifra archivos cuya modificación podría dañar el sistema operativo y las aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas están en la lista de exclusiones de cifrado:
  - %WINDIR%
  - %PROGRAMFILES% y %PROGRAMFILES(X86)%
  - Archivos de registro de Windows.

  No es posible ver ni modificar la lista de exclusiones de cifrado. Aunque los archivos y carpetas de esta lista pueden agregarse a la lista de cifrado, la característica de cifrado de archivos nunca cifrará esos objetos.

Parámetros del componente Cifrado de archivos

| Parámetro | Descripción |
|---|---|
| **Control del cifrado** | **Dejar sin modificar**. Si se selecciona este elemento, Kaspersky Endpoint Security no modifica los archivos y carpetas y no los cifra ni descifra.<br>**Cifrar de acuerdo con las reglas**. Si se selecciona este elemento, Kaspersky Endpoint Security cifra los archivos y las carpetas siguiendo las reglas de cifrado, descifra los archivos y las carpetas siguiendo las reglas de descifrado, y regula el acceso de las aplicaciones a los archivos cifrados siguiendo las reglas creadas para las aplicaciones. |

| | |
|---|---|
| | **Descifrar todo**. Si se selecciona este elemento, Kaspersky Endpoint Security descifra todos los archivos y carpetas cifrados. |
| **Reglas de cifrado** | Esta ficha muestra las reglas de cifrado para los archivos almacenados en discos locales. Las opciones para agregar archivos son las siguientes:<br>• **Carpetas predefinidas**. Kaspersky Endpoint Security permite agregar las siguientes áreas:<br>**Documentos**. Archivos que se encuentren en la carpeta *Documentos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.<br>**Favoritos**. Archivos que se encuentren en la carpeta *Favoritos* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.<br>**Escritorio**. Archivos que se encuentren en la carpeta *Escritorio* (carpeta estándar del sistema operativo) y en cualquiera de sus subcarpetas.<br>**Archivos temporales**. Archivos temporales vinculados al funcionamiento de las aplicaciones instaladas en el equipo. Aquí se incluyen, por ejemplo, las copias de seguridad temporales que se crean al trabajar con documentos en las aplicaciones de Microsoft Office.<br>**Archivos de Outlook**. Archivos vinculados al funcionamiento del cliente de correo electrónico Outlook: archivos de datos (PST), archivos de datos sin conexión (OST), archivos de las libretas de direcciones sin conexión (OAB) y archivos de las libretas de direcciones personales (PAB).<br>• **Carpetas**. Puede escribir la ruta de acceso a una carpeta. Cuando agregue una ruta de carpeta, siga estas reglas:<br>Utilice una variable de entorno (por ejemplo, `%CARPETA%\CarpetaDelUsuario\`). Puede usar una sola variable de entorno por ruta, y únicamente al comienzo de la ruta.<br>No utilice rutas relativas. Puede utilizar los caracteres `\..\` (por ejemplo, `C:\Usuarios\..\CarpetaDelUsuario\`). Los caracteres `\..\` se utilizan para referirse a la carpeta que se encuentra un nivel más arriba.<br>No utilice los caracteres `*` y `?`.<br>No utilice rutas UNC.<br>Utilice los caracteres `;` o `,` como separadores.<br>• **Archivos por extensión**. La lista contiene algunos grupos de extensiones que puede seleccionar (por ejemplo, el grupo *Archivos de almacenamiento*). También puede agregar extensiones de archivo manualmente. |
| **Reglas de descifrado** | Esta ficha muestra reglas de descifrado para los archivos almacenados en discos locales. |
| **Reglas para aplicaciones** | La ficha muestra una tabla que contiene reglas de acceso a archivos cifrados para aplicaciones y reglas de cifrado para archivos que se crean o modifican por aplicaciones particulares. |
| **Configuración de contraseña para paquetes cifrados** | Requisitos de seguridad con los que deberá cumplir la contraseña que se defina al momento de crear un paquete cifrado. |

## Cifrado de unidades extraíbles

Para que pueda usar este componente, Kaspersky Endpoint Security debe estar instalado en un equipo con Windows para estaciones de trabajo. El componente no estará disponible si Kaspersky Endpoint Security se ha instalado en un equipo con Windows para servidores.

Kaspersky Endpoint Security admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si se conecta una unidad extraíble con un sistema de archivos no compatible al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y Kaspersky Endpoint Security asigna el estado de solo lectura a la unidad extraíble.

Para proteger la información almacenada en una unidad extraíble, puede usar los siguientes tipos de cifrado:

- Cifrado de disco completo (FDE).

  Cifrado de la unidad extraíble completa, incluido su sistema de archivos.

  Tenga en cuenta que no se podrá acceder a la información cifrada fuera de la red corporativa. Aun dentro de la red corporativa, tampoco será posible acceder a esta información si el equipo no está conectado a Kaspersky Security Center (es decir, si se utiliza un equipo invitado).

- Cifrado de archivos (FLE).

  Cifrado únicamente de los archivos almacenados en la unidad extraíble. El sistema de archivos no se modifica.

  Si cifra los archivos de una unidad extraíble, podrá utilizar un modo especial —llamado *modo portátil*— para acceder a la información fuera de la red corporativa.

Kaspersky Endpoint Security crea una clave maestra como parte del proceso de cifrado. La clave maestra se guarda en los siguientes repositorios:

- Kaspersky Security Center
- El equipo del usuario

  La clave maestra se cifra con la clave secreta del usuario.

- Unidad extraíble

  La clave maestra se cifra con la clave pública de Kaspersky Security Center.

Una vez que haya cifrado una unidad extraíble, mientras se encuentre dentro de la red corporativa, podrá acceder a sus datos como si estuviera utilizando una unidad convencional sin cifrado.

## Acceso a datos cifrados

Cuando se conecta una unidad extraíble con información cifrada, Kaspersky Endpoint Security hace lo siguiente:

1. Busca una clave maestra en el repositorio local del equipo del usuario.

   Si encuentra la clave maestra pertinente, el usuario puede acceder a la información de la unidad extraíble.

   Si no encuentra la clave maestra, Kaspersky Endpoint Security hace lo siguiente:

   a. Envía una solicitud a Kaspersky Security Center.

Tras recibir la solicitud, Kaspersky Security Center envía una respuesta con la clave maestra.

b. Kaspersky Endpoint Security guarda la clave maestra en el repositorio local del equipo para poder operar con la unidad extraíble cifrada.

2. Descifra la información.

## Consideraciones especiales del cifrado de unidades extraíbles

El cifrado de unidades extraíbles está sujeto a las siguientes consideraciones especiales:

- La directiva con los ajustes preestablecidos para el cifrado de unidades extraíbles se crea para un grupo específico de equipos administrados. Por lo tanto, el resultado de la aplicación de la directiva de Kaspersky Security Center configurada para el cifrado o descifrado de unidades extraíbles depende del equipo al cual está conectada la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra los archivos de solo lectura que puedan encontrarse en las unidades extraíbles.
- Los siguientes tipos de dispositivo se admiten como unidad extraíble:
  - Medios de datos conectados por medio de un bus USB
  - Discos duros conectados por medio de buses USB y FireWire
  - Unidades SSD conectadas por medio de buses USB y FireWire

Parámetros del componente Cifrado de unidades extraíbles

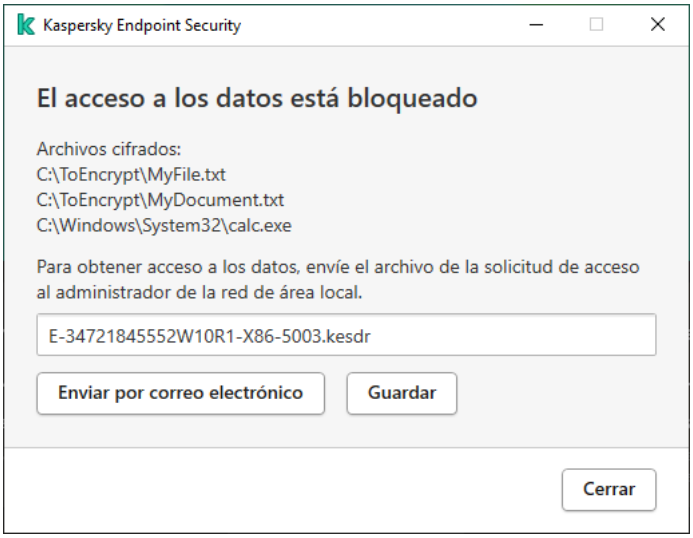
| Parámetro | Descripción |
|---|---|
| **Control del cifrado** | **Cifrar la unidad extraíble completa**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará las unidades extraíbles sector por sector, incluyendo sus sistemas de archivos.<br>**Cifrar todos los archivos**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará todos los archivos almacenados en las unidades extraíbles. Kaspersky Endpoint Security no volverá a cifrar los archivos que ya estén cifrados. Tampoco cifrará el contenido del sistema de archivos de las unidades extraíbles, por lo que los nombres de los archivos cifrados, la estructura de carpetas, etc., seguirán siendo visibles.<br>**Solo cifrar archivos nuevos**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security únicamente cifrará los archivos que se hayan creado o modificado en las unidades extraíbles desde la última aplicación de la directiva de Kaspersky Security Center. Este modo de cifrado es conveniente cuando se usa un disco extraíble para fines personales y laborales. Este modo de cifrado le permite dejar todos los archivos intactos y cifrar solo los archivos que el usuario crea en un equipo de trabajo que tiene instalado Kaspersky Endpoint Security y habilitada la función de cifrado. De este modo, siempre se puede acceder a archivos personales, independientemente de si Kaspersky Endpoint Security se instala en el equipo con la función de cifrado habilitada.<br>**Descifrar la unidad extraíble completa**. Si selecciona este elemento, cuando se aplique la directiva con los ajustes de cifrado para unidades extraíbles, Kaspersky Endpoint Security descifrará todos los archivos de las unidades extraíbles y, si estuvieran cifrados, también sus sistemas de archivos. |

| | |
|---|---|
| | **Dejar sin modificar**. Si selecciona este elemento, cuando se aplique la directiva, la aplicación no modificará el estado de las unidades. Si la unidad se cifra, permanece cifrada. Si la unidad se descifra, permanece descifrada. Este elemento está seleccionado por defecto. |
| **Modo Portátil** | La casilla habilita o deshabilita una opción que permite preparar una unidad extraíble de manera tal que sus archivos puedan manipularse en equipos que no estén conectados a la red corporativa.<br>Si activa esta casilla, cuando se aplique la directiva, Kaspersky Endpoint Security le pedirá al usuario que especifique una contraseña antes de cifrar los archivos de la unidad extraíble. La contraseña dará acceso a los archivos cifrados de la unidad cuando se la conecte a un equipo que no se encuentre en la red corporativa. Puede configurar los requisitos de seguridad con los que deberá cumplir esta contraseña.<br>El modo portátil estará disponible únicamente si ha seleccionado los modos **Cifrar todos los archivos** o **Solo cifrar archivos nuevos**. |
| **Solo cifrar el espacio de disco usado** | Esta casilla de verificación habilita / deshabilita el modo de cifrado en el cual se cifran solo los sectores de disco ocupados. Este modo se recomienda para unidades nuevas cuyos datos no se han modificado o eliminado.<br>Si se selecciona la casilla de verificación, solo se cifran partes de la unidad que contienen archivos. Kaspersky Endpoint Security cifra automáticamente nuevos datos a medida que se añaden.<br>Si se desactiva la casilla de verificación, se cifra la unidad completa, incluidos fragmentos residuales de archivos eliminados y modificados anteriormente.<br>La posibilidad de cifrar solo el espacio de disco usado está disponible únicamente para el modo **Cifrar la unidad extraíble completa**.<br>Activar o desactivar la casilla **Solo cifrar el espacio de disco usado** una vez que se ha iniciado el proceso de cifrado no tiene ningún efecto. Debe seleccionar o deshabilitar la casilla de verificación antes de iniciar el cifrado. |
| **Reglas de cifrado para los dispositivos seleccionados** | Esta tabla contiene dispositivos para los cuales se definen reglas de cifrado personalizadas. Si desea crear una regla de cifrado para una unidad extraíble específica, tiene las siguientes opciones:<br>• Agregar una unidad extraíble que exista en la lista de dispositivos de confianza de Control de dispositivos.<br>• Agregar una unidad extraíble en forma manual:<br>  • por id. de dispositivo (id. de hardware, también denominado HWID),<br>  • por modelo de dispositivo: id. de proveedor (VID) e id. de producto (PID). |
| **Permitir cifrado de unidades extraíbles en el modo offline** | Si se selecciona esta casilla, Kaspersky Endpoint Security cifra unidades extraíbles incluso cuando no hay conexión con Kaspersky Security Center. En este caso, los datos requeridos para descifrar las unidades extraíbles se almacenan en el disco duro del equipo al cual la unidad extraíble se conecta y no se transmite a Kaspersky Security Center.<br>Si se desmarca esta casilla, Kaspersky Endpoint Security no cifra unidades extraíbles sin una conexión con Kaspersky Security Center. |
| **Configuración** | Requisitos de seguridad para la contraseña del Administrador de archivos portátil. |

| | |
|---|---|
| **de contraseña para el modo portátil** | |

## Plantillas (cifrado de datos)

Kaspersky Endpoint Security puede restringir el acceso a los datos que se hayan cifrado en el pasado debido a, por ejemplo, un cambio en la infraestructura de la organización y un cambio en el Servidor de administración de Kaspersky Security Center. Si un usuario descubre que no puede acceder a los datos cifrados que necesita, puede pedirle acceso al administrador. Para ello, debe enviarle al administrador un archivo de solicitud de acceso. El administrador, por su parte, le enviará al usuario un archivo de respuesta, que este deberá cargar en Kaspersky Endpoint Security. La solicitud de acceso para el administrador puede enviarse por correo electrónico (vea la siguiente imagen).




Solicitar acceso a información cifrada

El mensaje con el que se da aviso de la falta de acceso está basado en una plantilla. Si lo desea, puede completar los siguientes campos para que no tenga que hacerlo el usuario:

- **A**. Escriba la dirección de correo de un grupo de administradores que tenga permitido usar las funciones de cifrado de datos.
- **Asunto**. Escriba el asunto del mensaje que se enviará para solicitar acceso a los archivos cifrados. Puede agregar etiquetas que ayuden a filtrar los mensajes.
- **Mensaje**. De ser necesario, modifique el contenido del mensaje. Puede utilizar variables para introducir ciertos datos (por ejemplo, la variable `%USER_NAME%`).

## Exclusiones

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo.

El administrador crea la zona de confianza independientemente, teniendo en cuenta las características de los objetos manejados y las aplicaciones instaladas en el equipo. Puede ser necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a un objeto o una aplicación determinados, si está seguro de que dicho objeto o aplicación no suponen peligro alguno. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza además de la zona de confianza general en una directiva.

## Exclusiones de análisis

Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas.

A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre el software legal que los delincuentes pueden utilizar para dañar el equipo o los datos personales están disponibles en la Enciclopedia de Kaspersky.

Kaspersky Endpoint Security puede bloquear estas aplicaciones. Para prevenir que se bloqueen, puede configurar la exclusión del análisis para las aplicaciones en uso. Busque para ello el nombre (o la máscara de nombre) pertinente en la Enciclopedia de Kaspersky y agréguelo a la zona de confianza. Por ejemplo, a menudo utiliza la aplicación Radmin para la administración remota de equipos. Kaspersky Endpoint Security considera esta actividad como sospechosa y puede bloquearla. Para evitar que la aplicación se bloquee, cree una exclusión de análisis con el nombre o la máscara de nombre que se indiquen en la Enciclopedia de Kaspersky.

Si una aplicación que recopila información y la envía para su proceso se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis si configura Kaspersky Endpoint Security tal como se describe en este documento.

Las exclusiones de escaneo pueden ser utilizadas por los siguientes componentes de aplicaciones y tareas configuradas por el administrador del sistema:

- Detección de comportamientos.
- Prevención de exploits.
- Prevención contra intrusos
- Protección contra amenazas de archivos.
- Protección contra amenazas web.
- Protección contra amenazas de correo.
- Tareas de análisis.

## Lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de archivos y de red (incluida la actividad maliciosa) y el acceso al registro del sistema no son supervisados por Kaspersky Endpoint Security. De manera predeterminada, Kaspersky Endpoint Security controla las acciones y el tráfico de red de todas las aplicaciones y analiza los objetos que abren, ejecutan o guardan los procesos asociados a las mismas. Sin embargo, Kaspersky Endpoint Security excluye de los análisis a una aplicación que se haya agregado a la lista de aplicaciones de confianza.

Por ejemplo, si considera que los objetos utilizados por la aplicación estándar Bloc de notas de Microsoft Windows son seguros sin análisis, es decir, que confía en esta aplicación, puede agregar el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza. De este modo, el análisis ignora objetos utilizados por esta aplicación.

Además, ciertas acciones clasificadas por Kaspersky Endpoint Security como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de una cantidad de aplicaciones. Por ejemplo, la intercepción del texto escrito con el teclado es un proceso de rutina para los conmutadores de disposición del teclado automática (como Punto Switcher). Para tener en cuenta las características de estas aplicaciones y no supervisarlas, se recomienda agregarlas a la lista de aplicaciones de confianza.

Al excluir del análisis las aplicaciones de confianza, se evitan problemas de compatibilidad de Kaspersky Endpoint Security con otros programas (por ejemplo, el doble análisis del tráfico de red en el equipo de un tercero realizado por Kaspersky Endpoint Security y otra aplicación antivirus) y además se mejora el rendimiento del equipo, lo que resulta crítico cuando se ejecutan aplicaciones del servidor.

Al mismo tiempo, el archivo ejecutable y los procesos de la aplicación de confianza seguirán siendo analizados en busca de virus y otras clases de malware. Una aplicación se puede excluir completamente del análisis de Kaspersky Endpoint Security mediante exclusiones de escaneo.

Configuración de exclusiones

| Parámetro | Descripción |
| --- | --- |
| **Tipos de objetos detectados** | Independientemente de la configuración de la aplicación ajustada, Kaspersky Endpoint Security siempre detecta y bloquea virus, gusanos y troyanos. Estos pueden ocasionar daños importantes al equipo.<br><br>• Virus y gusanos |

**Subcategoría**: virus y gusanos (Viruses_and_Worms)

**Nivel de amenaza**: alto

Los virus y gusanos tradicionales realizan acciones no autorizadas por el usuario. Pueden crear copias de sí mismos capaces de replicarse.

**Virus habitual**

Cuando un virus tradicional ingresa a un equipo, lo que hace es infectar un archivo, activarse, realizar acciones malintencionadas y agregar copias de sí mismo a otros archivos.

Los virus tradicionales solo se multiplican en los recursos locales del equipo; no pueden penetrar otros equipos por sí mismos. Solo pueden pasar a otro equipo si agregan una copia de sí mismos a un archivo almacenado en una carpeta compartida o en un CD dentro del equipo, o si el usuario reenvía un mensaje de correo con un archivo adjunto infectado.

El código de los virus tradicionales puede penetrar diversas áreas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de scripts* y *virus de macros*.

Los virus pueden infectar archivos mediante una variedad de técnicas. *Los virus de sobreescritura* escriben su código sobre el código del archivo infectado y borran el contenido de este. El archivo infectado deja de funcionar y no se puede restaurar. *Los virus parasitarios* modifican archivos y los dejan total o parcialmente funcionales. *Los virus de acompañamiento* no modifican archivos, sino que crean duplicados de ellos. Cuando se abre un archivo infectado, se inicia un duplicado de este (que, en realidad, es un virus). También es posible encontrarse con los siguientes tipos de virus: *virus de 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. Los gusanos reciben este nombre debido a su capacidad para "arrastrarse" de un equipo a otro y propagar copias de sí mismos sin el permiso del usuario mediante numerosos canales de datos.

La principal función que permite diferenciar los distintos tipos de gusanos es la forma de propagarse. La siguiente tabla proporciona un resumen de distintos tipos de gusanos, clasificados según la forma en que se propagan.

Formas de propagación

| Tipo | Nombre | Descripción |
|---|---|---|
| **Gusano de correo** | Gusano de correo | Se propagan mediante el correo. |

| | | |
|---|---|---|
| | | Un mensaje de correo infectado contiene un documento adjunto con una copia de un gusano o un vínculo a un archivo cargado en un sitio web que puede haber sufrido un ataque o haber sido creado exclusivamente con ese fin. Cuando se abre el documento adjunto, se activa el gusano. Cuando se hace clic en el vínculo, se descarga y se abre el archivo, y el gusano empieza a realizar acciones malintencionadas. Después de esto, empieza a distribuir copias de sí mismo. Para ello, busca otras direcciones de correo y les envía mensajes infectados. |
| **IM-Worm** | Clientes de MI | Se propagan a través de clientes de MI.<br>Por lo general, estos gusanos envían mensajes que incluyen un vínculo a un archivo con una copia del gusano ubicado en un sitio web y utilizan las listas de contactos del usuario. Cuando el usuario descarga el archivo y lo abre, se activa el gusano. |
| **IRC-Worm** | Gusanos de chat de Internet | Se propagan mediante Internet Relay Chats, sistemas de servicio que permiten comunicarse con otras personas a través de Internet en tiempo real.<br>Estos gusanos publican un archivo con una copia de sí mismos o un vínculo al archivo en un chat de Internet. Cuando el usuario descarga el archivo y lo abre, se activa el gusano. |
| **Gusano de red** | Gusanos de red | Estos gusanos se propagan a través de redes de equipos.<br>A diferencia de otros tipos de gusanos, un gusano de red típico se propaga sin la participación del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red (punto vulnerable) especialmente formado que contiene el código del gusano o una parte de él. Si en la red hay algún equipo "vulnerable", recibe este paquete de red. El gusano se activa una vez que penetra completamente en el equipo. |
| **P2P-Worm** | Gusanos de redes de uso compartido de archivos | Se propagan mediante redes punto a punto de uso compartido de archivos.<br>Para infiltrar una red P2P, el gusano se copia en una carpeta de uso compartido de archivos que, por lo general, está situada en el equipo del usuario. La red P2P muestra información sobre este archivo, de modo que el usuario pueda "encontrar" el archivo infectado en la red como a cualquier otro archivo, descargarlo y abrirlo.<br>Gusanos más sofisticados emulan el protocolo de red de una red P2P específica: devuelven respuestas positivas a solicitudes de búsqueda y ofrecen copias de sí mismo para su descarga. |
| **Gusano** | Otros tipos de gusanos | Otros tipos de gusanos incluyen los siguientes: |

| | | |
|---|---|---|
| | | • Gusanos que distribuyen copias de sí mismos por los recursos de red. Al utilizar las funciones del sistema operativo, buscan carpetas disponibles de red, se conectan a equipos conectados a Internet e intentan obtener acceso total a sus unidades de disco. A diferencia de los tipos de gusanos descritos anteriormente, otras clases de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano.<br><br>• Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono móvil a otro). |

- Troyanos

**Subcategoría**: Troyanos

**Nivel de amenaza**: alto

A diferencia de los gusanos y los virus, los troyanos no se autorreplican. Por ejemplo, penetran un equipo a través del correo o un navegador cuando el usuario visita una página web infectada. Los troyanos requieren la participación del usuario para iniciarse. Comienzan a realizar acciones malintencionadas inmediatamente después de iniciarse.

Los distintos troyanos se comportan de manera diferente en los equipos infectados. Las principales funciones de los troyanos consisten en bloquear, modificar o destruir información y en deshabilitar equipos o redes. Los troyanos también reciben o envían archivos, los ejecutan, muestran mensajes en pantalla, solicitan páginas web, descargan e instalan programas y reinician equipos.

Con frecuencia, los piratas usan "conjuntos" de varios troyanos.

Los tipos de comportamiento de los caballos de troya se describen en la siguiente tabla.

Tipos de comportamiento de caballos de troya en equipos infectados

| Tipo | Nombre | Descripción |
|---|---|---|
| **Trojan-ArcBomb** | Troyanos: "bombas en archivos de almacenamiento" | Cuando se descomprimen, estos archivos de almacenamiento aumentan de tamaño en una medida tal que afecta el funcionamiento del equipo.<br>Cuando el usuario intenta descomprimir un archivo de almacenamiento de esta clase, es posible que el equipo se ralentice o se bloquee, y el disco duro puede llenarse de datos "vacíos". Las "bombas en archivo de almacenamiento" son especialmente peligrosas para los servidores de correo y de archivos. Si el servidor utiliza un sistema automático para procesar la información entrante, una "bomba en archivo de almacenamiento" puede detener el servidor. |
| **Backdoor** | Troyanos de administración remota | Se considera que son los troyanos más peligrosos. Funcionan de manera bastante similar a las aplicaciones de administración remota instaladas en los equipos.<br>Estos programas se instalan en el equipo sin que el usuario los detecte, lo que permite al intruso administrarlo de forma remota. |
| **Caballo de troya** | Troyanos | En esta categoría se incluyen las siguientes aplicaciones |

| | | |
|---|---|---|
| | | malintencionadas:<br>• **Troyanos tradicionales**. Estos programas solo realizan las funciones principales de los troyanos: bloquear, modificar o destruir información y deshabilitar equipos o redes. A diferencia de los otros tipos de troyano descritos en la tabla, estos no tienen funciones avanzadas.<br>• **Troyanos versátiles**. Estos programas tienen funciones avanzadas típicas de diversos tipos de troyanos. |
| **Trojan-Ransom** | Ransom troyanos | Toman la información del usuario como "rehén", modificándola o bloqueándola, o afectan el funcionamiento del equipo, de modo que el usuario pierde la capacidad de utilizar la información. El intruso le exige al usuario un rescate a cambio de una aplicación que permita restaurar la información y la operatividad del equipo. |
| **Trojan-Clicker** | Trojan-Clicker | Acceden a páginas web desde el equipo del usuario, ya sea mediante el envío de comandos a un navegador por su cuenta o por medio de la modificación de las direcciones web especificadas en los archivos del sistema operativo.<br>Al utilizar estos programas, los intrusos realizan ataques de red e incrementan las visitas a sitios web, lo que aumenta la cantidad de anuncios publicitarios que se muestran. |
| **Trojan-Downloader** | Descargadores troyanos | Acceden a la página web del intruso para descargar de allí otra aplicación malintencionada e instalarla en el equipo del usuario. El nombre del archivo que se debe descargar puede venir establecido de antemano dentro del troyano o puede determinarse al acceder a la página del atacante. |
| **Trojan-Dropper** | Caballos de troya instaladores de software malintencionado | Contienen otros troyanos que descargan en el disco duro y luego instalan.<br>Los intrusos pueden utilizar programas de este tipo para cumplir los siguientes objetivos:<br>• Instalar una aplicación malintencionada sin que el usuario lo advierta: Los troyanos de esta |

| | | |
|---|---|---|
| | | clase no muestran ningún mensaje o, si lo hacen, dan información falsa (por ejemplo, pueden advertir sobre la existencia de un archivo dañado o sobre incompatibilidades en el sistema operativo).<br>• Impedir la detección de una aplicación malintencionada conocida. No todos los antivirus son capaces de detectar aplicaciones malintencionadas cuando vienen ocultas en troyanos de este tipo. |
| **Trojan-Notifier** | Caballos de troya notificadores | Le informan al atacante que puede introducirse en el sistema infectado y le envían información sobre el equipo: dirección IP, número de puerto abierto o dirección de correo electrónico. Se conectan con el intruso por medio de correo, FTP, ingreso a la página web del intruso o de otra manera.<br>Los troyanos notificadores suelen utilizarse en conjuntos conformados por varios troyanos. Informan al intruso que se han instalado correctamente otros troyanos en el equipo del usuario. |
| **Trojan-Proxy** | Caballos de troya proxy | Permiten al intruso acceder de forma anónima a páginas web mediante el equipo del usuario. Con frecuencia, se utilizan para enviar correo no deseado. |
| **Trojan-PSW** | Programas que roban contraseñas | Los programas que roban contraseñas son una clase de caballo de troya que roba cuentas de usuarios, tales como datos de registro de software. Estos troyanos encuentran datos confidenciales en archivos del sistema y en el Registro y se los envían a su "maestro" mediante correo, FTP, acceso a la página web del intruso o de otro modo.<br>Algunos de estos troyanos se categorizan en los distintos tipos descritos en esta tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan por Internet (Trojan-GameThief). |
| **Trojan-Spy** | Caballos de troya espías | Espían al usuario y reúnen información acerca de las acciones que este realiza cuando trabaja en el equipo. Pueden interceptar los datos |

| | | |
|---|---|---|
| | | introducidos por el usuario mediante el teclado, realizar capturas de pantalla o compilar listas de aplicaciones activas. Después de recibir la información, se la transfieren al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. |
| **Trojan-DDoS** | Caballos de troya atacantes de red | Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). Los piratas suelen infectar muchos equipos con estos programas de manera de utilizar los equipos para atacar a un único servidor simultáneamente.<br>Los programas DoS llevan a cabo un ataque desde un único equipo con el conocimiento del usuario. Los programas DDoS (DoS distribuida) llevan a cabo ataques distribuidos desde distintos equipos sin que lo advierta el usuario del equipo infectado. |
| **Trojan-IM** | Troyanos que roban información de usuarios de clientes de mensajería instantánea | Roban los números de cuenta y contraseñas de quienes usan clientes de mensajería instantánea. Transfieren los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. |
| **Rootkit** | RootKits | Enmascaran la existencia y las acciones de otras aplicaciones malintencionadas para ayudarlas a perdurar en el sistema operativo. También pueden ocultar archivos, claves del registro que se utilicen para ejecutar aplicaciones malintencionadas o procesos que se encuentren cargados en la memoria del equipo infectado. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones en el equipo del usuario y en otros equipos de la red. |
| **Trojan-SMS** | Troyanos en la forma de mensajes SMS | Infectan teléfonos móviles y envían mensajes SMS a números de teléfono con tarifas elevadas. |
| **Trojan-GameThief** | Troyanos que roban información de usuarios de juegos en línea | Roban credenciales de las cuentas de usuarios de juegos en línea, tras lo cual envían los datos al intruso mediante correo, FTP, acceso a la |

| | | |
|---|---|---|
| | | página web del intruso o de otro modo. |
| **Trojan-Banker** | Troyanos que roban cuentas bancarias | Roban datos de cuentas bancarias o de sistemas de dinero electrónico y luego envían la información al hacker por correo electrónico, por FTP, a través de una página creada por el atacante o usando otros medios. |
| **Trojan-Mailfinder** | Troyanos que reúnen direcciones de correo | Recopilan direcciones de correo almacenadas en un equipo y se las envían al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado. |

- Herramientas maliciosas

**Subcategoría**: Herramientas maliciosas

**Nivel de peligrosidad**: medio

A diferencia de otros tipos de software malware, las herramientas maliciosas no realizan acciones inmediatamente después de iniciarse. Pueden almacenarse de manera segura e iniciarse en el equipo del usuario. A menudo, los intrusos utilizan las funciones de estos programas para crear virus, gusanos y troyanos, perpetrar ataques de red en servidores remotos, atacar equipos o llevar a cabo otras acciones malintencionadas.

Varias funciones de las herramientas maliciosas se agrupan en los tipos descritos en la siguiente tabla.

Funciones de herramientas maliciosas

| Tipo | Nombre | Descripción |
|---|---|---|
| **Constructor** | Constructores | Permiten crear nuevos virus, gusanos y troyanos. Algunos constructores ofrecen una interfaz estándar, con ventanas para elegir el tipo de aplicación malintencionada que se va a crear, los métodos que se usarán para contrarrestar los depuradores y otras características. |
| **Dos** | Ataque de red | Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). |
| **Exploit** | Exploits | Los puntos vulnerables son conjuntos de datos o un código de programa que se sirve de las vulnerabilidades de la aplicación en la que se procesa para realizar una acción malintencionada en un equipo. Por ejemplo, un punto vulnerable puede escribir o leer archivos o solicitar páginas web "infectadas". |

| | | |
|---|---|---|
| | | Distintos puntos vulnerables se sirven de las vulnerabilidades de diversos servicios de red o aplicaciones. Disfrazados como paquete de red, los puntos vulnerables se transfieren a través de la red a numerosos equipos y buscan equipos con servicios de red vulnerables. Un punto vulnerable en un archivo DOC se sirve de las vulnerabilidades de un editor de texto. Puede comenzar a realizar las acciones preprogramadas por el pirata cuando el usuario abre el archivo infectado. Un punto vulnerable incrustado en un mensaje de correo busca vulnerabilidades en cualquier cliente de correo. Puede empezar a realizar una acción malintencionada apenas el usuario abre el mensaje infectado en dicho cliente.<br>Los gusanos de red se propagan por las redes mediante los puntos vulnerables. Los puntos vulnerables *Nuker* son paquetes de red que deshabilitan equipos. |
| **FileCryptor** | Cifradores | Se utilizan para cifrar otras aplicaciones malintencionadas y evitar, con ello, que las aplicaciones antivirus las detecten. |
| **Flooder** | Programas para "contaminar" redes | Envían numerosos mensajes a través de canales de red. Este tipo de herramienta incluye, por ejemplo, programas que contaminan Internet Relay Chats.<br>Las herramientas de tipo "flooder" no incluyen programas que "contaminan" los canales usados por el correo, los clientes de mensajería instantánea y los sistemas de comunicaciones móviles. Estos programas se describen de manera individual en la tabla (flooder de correo, IM-Flooder y flooder de SMS). |
| **HackTool** | Herramientas de piratería | Permiten los ataques a los equipos en los que están instalados o atacan otro equipo (por ejemplo, mediante la adición de nuevas cuentas de sistema sin el permiso del usuario o la eliminación de registros del sistema para ocultar rastros de su presencia en el sistema operativo). Este tipo de herramienta incluye algunos analizadores de protocolos que ofrecen funciones malintencionadas, como la interceptación de contraseñas. Los analizadores de |

| | | |
|---|---|---|
| | | protocolos son programas que permiten ver el tráfico de red. |
| **Hoax** | Hoax | Alarman al usuario con mensajes similares a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario de que se dio formato a un disco, cuando esto no sucedió en realidad. |
| **Spoofer** | Herramientas de falsificación | Envían mensajes y solicitudes de red con una dirección falsa del remitente. Los intrusos utilizan herramientas de falsificación para hacerse pasar por los verdaderos remitentes de los mensajes, por ejemplo. |
| **VirTool** | Herramientas que pueden ingresar modificaciones en las aplicaciones malintencionadas | Permiten la modificación de otros programas de software malware y los ocultan de las aplicaciones antivirus. |
| **Email-Flooder** | Programas que "contaminan" las direcciones de correo | Envían numerosos mensajes a varias direcciones de correo electrónico y, de este modo, las contaminan. Un gran volumen de mensajes entrantes impide que los usuarios vean mensajes deseados en sus buzones. |
| **IM-Flooder** | Programas que "contaminan" el tráfico de los clientes de MI | "Inundan" a los usuarios de clientes de MI con mensajes. Un gran volumen de mensajes impide a los usuarios visualizar mensajes entrantes deseados. |
| **SMS-Flooder** | Programas que "contaminan" el tráfico con mensajes SMS | Envían numerosos mensajes de SMS a teléfonos móviles. |

- Adware

  **Subcategoría**: software de publicidad (Adware);

  **Nivel de amenaza**: medio

  El adware muestra información publicitaria al usuario. Los programas de adware muestran anuncios publicitarios en las interfaces de otros programas y redireccionan las solicitudes de búsqueda a páginas web publicitarias. Algunos reúnen información de marketing acerca del usuario y la envían a su desarrollador. Esta información puede incluir los nombres de los sitios web visitados por el usuario o el contenido de sus solicitudes de búsqueda. A diferencia de los caballos de troya espías, el adware envía esta información al desarrollador con el permiso del usuario.

- Marcadores automáticos

**Subcategoría**: software legal que los delincuentes pueden usar para dañar el equipo o sus datos personales

**Nivel de peligrosidad**: medio

La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP, y Telnet.

Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

| Tipo | Nombre | Descripción |
|---|---|---|
| **Client-IRC** | Clientes de chat de Internet | Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware. |
| **Dialer** | Marcadores automáticos | Pueden establecer conexiones telefónicas a través de un módem en modo oculto. |
| **Downloader** | Programas para realizar descargas | Pueden descargar archivos de páginas web en modo oculto. |
| **Monitor** | Programas para supervisar | Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos). |
| **PSWTool** | Restauradores de contraseñas | Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito. |
| **RemoteAdmin** | Programas de administración remota | Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos. |

| | | |
|---|---|---|
| | | Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo. |
| **Server-FTP** | Servidores FTP | Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP. |
| **Server-Proxy** | Servidores proxy | Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **Server-Telnet** | Servidores Telnet | Funcionan como servidores Telnet. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de Telnet. |
| **Server-Web** | Servidores web | Funcionan como servidores web. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP. |
| **RiskTool** | Herramientas para trabajar en un equipo local | Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos. |
| **NetTool** | Herramientas de red | Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos. |
| **Client-P2P** | Clientes de red P2P | Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware. |
| **Client-SMTP** | Clientes SMTP | Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **WebToolbar** | Barras de herramientas web | Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda. |
| | | |

| | | |
|---|---|---|
| **FraudTool** | Pseudoprogramas | Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada. |

- Detectar otras clases de software que los criminales puedan usar para dañar el equipo o sus datos personales.

**Subcategoría**: software legal que los delincuentes pueden usar para dañar el equipo o sus datos personales

**Nivel de peligrosidad**: medio

La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP, y Telnet.

Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

| Tipo | Nombre | Descripción |
|---|---|---|
| **Client-IRC** | Clientes de chat de Internet | Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware. |
| **Dialer** | Marcadores automáticos | Pueden establecer conexiones telefónicas a través de un módem en modo oculto. |
| **Downloader** | Programas para realizar descargas | Pueden descargar archivos de páginas web en modo oculto. |
| **Monitor** | Programas para supervisar | Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos). |
| **PSWTool** | Restauradores de contraseñas | Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito. |
| **RemoteAdmin** | Programas de administración remota | Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos. |

| | | |
|---|---|---|
| | | Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo. |
| **Server-FTP** | Servidores FTP | Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP. |
| **Server-Proxy** | Servidores proxy | Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **Server-Telnet** | Servidores Telnet | Funcionan como servidores Telnet. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de Telnet. |
| **Server-Web** | Servidores web | Funcionan como servidores web. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP. |
| **RiskTool** | Herramientas para trabajar en un equipo local | Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos. |
| **NetTool** | Herramientas de red | Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos. |
| **Client-P2P** | Clientes de red P2P | Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware. |
| **Client-SMTP** | Clientes SMTP | Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario. |
| **WebToolbar** | Barras de herramientas web | Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda. |
| | | |

| | | |
|---|---|---|
| **FraudTool** | Pseudoprogramas | Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada. |

- **Ejecutables comprimidos que puedan tener código malicioso oculto**

  Kaspersky Internet Security analiza objetos comprimidos y el módulo descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

  Para ocultar los programas peligrosos de las aplicaciones antivirus, los intrusos los comprimen mediante compresores especiales o crean archivos de empaquetado múltiple.

  Los analistas de virus de Kaspersky han identificado los compresores más utilizados por los piratas.

  Cuando Kaspersky Endpoint Security detecta uno de estos compresores en un archivo, puede darse casi por seguro que el archivo contiene una aplicación malintencionada o una aplicación que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario.

  Kaspersky Endpoint Security distingue los siguientes tipos de programas:

  - *Archivos comprimidos potencialmente peligrosos*: se usan para comprimir software malware, como virus, gusanos y troyanos.
  - *Archivos comprimidos varias veces* (nivel de amenaza medio): el objeto se comprimió tres veces con un compresor o varios.

- **Archivos de empaquetado múltiple**

Kaspersky Internet Security analiza objetos comprimidos y el módulo descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

Para ocultar los programas peligrosos de las aplicaciones antivirus, los intrusos los comprimen mediante compresores especiales o crean archivos de empaquetado múltiple.

Los analistas de virus de Kaspersky han identificado los compresores más utilizados por los piratas.

Cuando Kaspersky Endpoint Security detecta uno de estos compresores en un archivo, puede darse casi por seguro que el archivo contiene una aplicación malintencionada o una aplicación que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario.

Kaspersky Endpoint Security distingue los siguientes tipos de programas:

- *Archivos comprimidos potencialmente peligrosos*: se usan para comprimir software malware, como virus, gusanos y troyanos.
- *Archivos comprimidos varias veces* (nivel de amenaza medio): el objeto se comprimió tres veces con un compresor o varios.

**Exclusiones**

Esta tabla contiene información acerca de las exclusiones de análisis.

Para excluir objetos de los análisis, puede usar los siguientes métodos:

- Especifique la ruta al archivo o a la carpeta.
- Especifique el hash del objeto.
- Usar máscaras:
  - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
  - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\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) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\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.

| | |
|---|---|
| | • Escriba el nombre que se le da al tipo de objeto en la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`). Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Cliente*`, Kaspersky Endpoint Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis. |
| **Aplicaciones de confianza** | En esta tabla, se enumeran las aplicaciones de confianza cuya actividad no supervisa Kaspersky Endpoint Security durante su funcionamiento.<br>El componente Control de aplicaciones regula el inicio de cada una de las aplicaciones sin tener en cuenta si la aplicación se incluye en la tabla de aplicaciones de confianza. |
| **Combinar valores al heredar**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Esto fusiona la lista de exclusiones de análisis y aplicaciones de confianza en las directivas principales y secundarias de Kaspersky Security Center. Para fusionar listas, la directiva secundaria debe configurarse para heredar la configuración de la directiva principal de Kaspersky Security Center.<br>Si la casilla está seleccionada, los elementos de la lista de la directiva principal de Kaspersky Security Center se mostrarán en las directivas secundarias. Así puede, por ejemplo, crear una lista consolidada de aplicaciones de confianza para toda la organización.<br>Los elementos de lista heredados de una directiva secundaria no se pueden eliminar ni editar. Los elementos de la lista de exclusiones de análisis y la lista de aplicaciones de confianza que se fusionan durante la herencia se pueden eliminar y editar solo en la directiva principal. Si lo necesita, podrá agregar, editar y eliminar elementos de la lista en directivas de menor jerarquía.<br>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.<br>Si esta casilla no está seleccionada, los elementos de las listas no se fusionarán cuando una directiva de Kaspersky Security Center herede la configuración de otra. |
| **Permitir el uso de exclusiones locales/Permitir el uso de aplicaciones de confianza locales**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | *Exclusiones locales y aplicaciones de confianza locales (zona de confianza local)*: lista definida por el usuario de objetos y aplicaciones en Kaspersky Endpoint Security para un equipo específico. Kaspersky Endpoint Security no supervisa objetos y aplicaciones de la zona de confianza local. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza además de la zona de confianza general en una directiva.<br>Si la casilla está seleccionada, un usuario puede crear una lista local de exclusiones de análisis y una lista local de aplicaciones de confianza. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.<br>Si la casilla no está seleccionada, un usuario puede acceder solo a las listas generales de exclusiones de análisis y aplicaciones de confianza generadas en la directiva. Si se generaron listas locales, después de deshabilitar esta funcionalidad, Kaspersky Endpoint Security continúa excluyendo los objetos enumerados de los análisis. |
| **Almacén de confianza de certificados del sistema** | Si se selecciona uno de los almacenes de certificados de sistema de confianza, Kaspersky Endpoint Security excluye de los análisis las aplicaciones firmadas con una firma digital de confianza. Kaspersky Endpoint Security asigna automáticamente dichas aplicaciones al grupo *De confianza*.<br>Si se selecciona **No usar**, Kaspersky Endpoint Security analiza las aplicaciones independientemente de si tienen o no una firma digital. Para definir el grupo de confianza de una aplicación, Kaspersky Endpoint Security tiene en cuenta lo peligrosa que puede resultar para el equipo. |

# Configuración de la aplicación

Puede configurar la siguiente configuración general de la aplicación:

- Modo de funcionamiento
- Autoprotección
- Rendimiento
- Información para depuración
- Estado del equipo cuando se aplique la configuración

Configuración de la aplicación

| Parámetro | Descripción |
| --- | --- |
| **Ejecutar Kaspersky Endpoint Security al iniciarse el equipo** | Cuando se selecciona esta casilla, Kaspersky Endpoint Security se inicia después de cargado el sistema operativo y protege al equipo durante toda la sesión.<br>Cuando se desactiva esta casilla, Kaspersky Endpoint Security no se inicia después de cargado el sistema operativo, sino cuando el usuario lo inicia manualmente. La protección del equipo está desactivada y los datos del usuario pueden estar expuestos a amenazas. |
| **Habilitar la tecnología de desinfección avanzada** | Cuando la casilla está seleccionada y se detecta actividad maliciosa en el sistema operativo, aparece una notificación emergente en la pantalla. En la notificación, Kaspersky Endpoint Security ofrece al usuario realizar una desinfección avanzada del equipo. Cuando el usuario aprueba este procedimiento, Kaspersky Endpoint Security neutraliza la amenaza. Una vez completado el procedimiento de desinfección avanzada, Kaspersky Endpoint Security reinicia el equipo. La tecnología de desinfección avanzada utiliza una cantidad considerable de recursos del equipo, lo que puede ralentizar otras aplicaciones.<br>Si Kaspersky Endpoint Security está instalado en un equipo con Windows for Servers, Kaspersky Endpoint Security no mostrará la notificación. Por lo tanto, el usuario no podrá seleccionar una acción para desinfectar una amenaza activa. Para desinfectar una amenaza, debe habilitar la tecnología de Desinfección avanzada en la configuración de la aplicación y ejecutar la Desinfección avanzada de inmediato en la configuración de la tarea *Análisis antivirus*. A continuación, debe iniciar la tarea *Análisis antivirus*. |
| **Usar Kaspersky Security Center como servidor proxy para la activación**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Si se selecciona esta casilla, el Servidor de administración de Kaspersky Security Center se usa como servidor proxy al activar la aplicación. |

| | |
|---|---|
| **Habilitar Autoprotección** | Cuando se selecciona esta casilla, Kaspersky Endpoint Security impide la alteración y la eliminación de archivos de aplicaciones en el disco duro, procesos de memoria y entradas en el registro del sistema. |
| **Permitir que la configuración de Kaspersky Endpoint Security se administre a través de aplicaciones de control remoto** | Si la casilla está seleccionada, las aplicaciones de administración remota de confianza (como TeamViewer, LogMeIn Pro y Remotely Anywhere) pueden modificar la configuración de Kaspersky Endpoint Security.<br>Las aplicaciones de administración remota que no son de confianza tienen prohibido modificar la configuración de Kaspersky Endpoint Security incluso cuando esta casilla está seleccionada. |
| **Habilitar el control de servicios externos** | Si se selecciona esta casilla, Kaspersky Endpoint Security permite la administración de servicios de la aplicación desde un equipo remoto. Cuando se intenta administrar los servicios de la aplicación de forma remota, aparece una notificación en la barra de tareas de Microsoft Windows, por encima del icono de la aplicación (a menos que el usuario haya desactivado el servicio de notificaciones). |
| **Posponer las tareas programadas cuando el equipo funciona con carga de batería** | Si se selecciona la casilla, se habilita el modo de ahorro de energía. Kaspersky Endpoint Security pospone las tareas programadas. Las tareas de análisis y actualización podrán iniciarse manualmente cuando sea necesario. |
| **Conceder recursos a otras aplicaciones** | Cuando Kaspersky Endpoint Security ejecuta las tareas programadas, esto puede ocasionar una mayor carga de trabajo en la CPU y los subsistemas de disco, lo que ralentiza el rendimiento de otras aplicaciones.<br>Cuando se selecciona esta casilla, Kaspersky Endpoint Security suspende las tareas programadas cuando detecta una mayor carga y libera recursos del sistema operativo para las aplicaciones del usuario. |
| **Habilitar escritura en archivos de volcado** | Si se selecciona la casilla, Kaspersky Endpoint Security escribe en los archivos de volcado cuando se cierra inesperadamente.<br>Si se desactiva la casilla, Kaspersky Endpoint Security no escribe en los archivos de volcado. La aplicación también elimina los archivos de volcado actuales del disco duro del equipo. |
| **Habilitar la protección de los archivos de volcado y de seguimiento** | Si se activa esta casilla, podrán acceder a los archivos de volcado el administrador del sistema, el administrador local y el usuario que haya habilitado la creación de dichos archivos. Solo los administradores del sistema y locales pueden acceder a archivos de seguimiento.<br>Si la casilla se desactiva, todos los usuarios podrán acceder a los archivos de volcado y de seguimiento. |
| **Estado del equipo cuando se aplique la configuración**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Opciones para mostrar, en Web Console, los estados de los equipos cliente con Kaspersky Endpoint Security instalado cuando ocurran errores al aplicar una directiva o ejecutar una tarea. Los estados disponibles son *Sin inconvenientes*, *Advertencia* y *Crítico*. |

# Informes y repositorios

## Informes

La información sobre el funcionamiento de cada componente de Kaspersky Endpoint Security, los eventos de cifrado de datos, la ejecución de cada tarea de análisis, la tarea de actualización y la tarea de comprobación de integridad y el funcionamiento general de la aplicación se registra en informes.

Los Informes se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES\Report`.

## Copias de seguridad

El depósito *Copia de seguridad* contiene copias de respaldo de los archivos que se modifican o eliminan cuando se realiza una desinfección. Una *copia de seguridad* es una copia del archivo creada antes de desinfectar o eliminar el archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

Las copias de seguridad de los archivos se almacenan en la carpeta `C:\ProgramData\Kaspersky Lab\KES\QB`.

Los usuarios del grupo Administradores tienen acceso completo a esta carpeta. Se conceden accesos limitados a esta carpeta al usuario cuya cuenta se utilizó para instalar Kaspersky Endpoint Security.

Kaspersky Endpoint Security no brinda la capacidad de configurar permisos de acceso de usuario a copias de seguridad de archivos.

Configuración de informes y repositorios

| Parámetro | Descripción |
|---|---|
| **Conservar informes no más de N días** | Si la casilla está seleccionada, los informes se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de informes es de 30 días. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe. |
| **Limitar el tamaño del archivo de informe a N MB** | Si esta casilla está seleccionada, el tamaño del archivo de informes nunca superará el valor definido. Por defecto, el tamaño máximo del archivo es de 1024 MB. Para evitar que se exceda el tamaño máximo del archivo del informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas de este archivo cuando alcanza el tamaño máximo. |
| **Conservar objetos no más de N días** | Si la casilla está seleccionada, los archivos se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de archivos es de 30 días. Al caducar el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos de Copia de seguridad. |
| **Limitar el tamaño de Copia de seguridad a N MB** | Si la casilla está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo es de 100 MB. Cuando se alcanza el valor definido, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos para evitar que el límite se exceda. |
| **Transferencia de datos al** | Categorías de eventos de los equipos cliente cuya información debe transmitirse al Servidor de administración. |

| | |
|---|---|
| **Servidor de administración**<br>*(disponible solo en Kaspersky Security Center)* | |

## Configuración de red

Puede definir los ajustes del servidor proxy que se utiliza para conectarse a Internet y actualizar las bases de datos antivirus, seleccionar el modo de vigilancia para los puertos de red y configurar la función de análisis de conexiones cifradas.

Opciones de red

| Parámetro | Descripción |
|---|---|
| **Limitar el tráfico de las conexiones de uso medido** | Si esta casilla está seleccionada, la aplicación limita su propio tráfico de red cuando la conexión a Internet está limitada. Kaspersky Endpoint Security identifica las conexiones de Internet móviles de alta velocidad como limitadas, y las conexiones Wi-Fi como ilimitadas.<br>Redes basadas en costos funciona en equipos con Windows 8 o posterior. |
| **Inyectar el script en el tráfico web para interactuar con páginas web** | Si la casilla de verificación está seleccionada, Kaspersky Endpoint Security inyecta un script de interacción de la página web en el tráfico web. Esta secuencia de comandos garantiza que el componente Control web pueda funcionar correctamente. El script permite registrar eventos de Control web. Sin este script, no puede habilitar la supervisión de la actividad de Internet del usuario.<br>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. |
| **Servidor proxy** | La configuración del servidor proxy utilizado para el acceso a Internet de los usuarios de los equipos cliente. Kaspersky Endpoint Security utiliza estas opciones de configuración para ciertos componentes de protección, inclusive para la actualización de bases de datos y módulos de aplicación.<br>Para la configuración automática de un servidor proxy, Kaspersky Endpoint Security usa el protocolo WPAD (protocolo de detección automática de proxy web). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, Kaspersky Endpoint Security usa la dirección especificada en la configuración del navegador Microsoft Internet Explorer. |
| **No usar el servidor proxy para las direcciones locales** | Si la casilla está seleccionada, Kaspersky Endpoint Security no utiliza un servidor proxy cuando realiza una actualización desde una carpeta compartida. |
| **Puertos supervisados** | **Supervisar todos los puertos de red**. En este modo de supervisión de puertos de red, los componentes de protección (protección contra archivos peligrosos, protección contra amenazas web y protección contra amenazas de correo) controlan los flujos de datos que se transmiten a través de cualquier puerto de red abierto del equipo. |

| | |
|---|---|
| | **Vigilar solo los puertos de red seleccionados**. Cuando se selecciona este modo, los componentes de protección vigilan los puertos de red seleccionados y la actividad de red de las aplicaciones seleccionadas. La lista de puertos de red que normalmente se utilizan para transmitir correo electrónico y otras clases de tráfico se configura siguiendo las recomendaciones de los expertos de Kaspersky.<br><br>**Vigilar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky**. En este modo, se utiliza una lista predefinida con las aplicaciones a las que están asociados los puertos que Kaspersky Endpoint Security vigilará. La lista incluye aplicaciones como Google Chrome, Adobe Reader y Java.<br><br>**Vigilar todos los puertos de las aplicaciones especificadas**. En este modo, se utiliza una lista de aplicaciones asociadas a los puertos que Kaspersky Endpoint Security deberá vigilar. |
| **Análisis de conexiones cifradas** | Kaspersky Endpoint Security analiza el tráfico de red cifrado que se transmite a través de los protocolos siguientes:<br><br>• SSL 3.0<br><br>• TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.<br><br>Kaspersky Endpoint Security es compatible con los siguientes modos de análisis de conexiones cifradas:<br><br>• **No analizar las conexiones cifradas** Kaspersky Endpoint Security no tendrá acceso al contenido de los sitios web cuyas direcciones comienzan con `https://`.<br><br>• **Analizar las conexiones cifradas si lo solicitan los componentes de protección**. Kaspersky Endpoint Security escaneará solo el tráfico cifrado cuando lo soliciten los componentes Protección contra archivos peligrosos, Protección contra amenazas de correo y Control Web.<br><br>• **Analizar siempre las conexiones cifradas** Kaspersky Endpoint Security analizará el tráfico de red cifrado aunque los componentes de protección estén deshabilitados.<br><br>Kaspersky Endpoint Security no analiza las conexiones cifradas que fueron establecidas por aplicaciones de confianza para las que el análisis de tráfico está desactivado. Kaspersky Endpoint Security no analiza las conexiones cifradas de la lista predefinida de sitios web de confianza. Los expertos de Kaspersky crean la lista predefinida de sitios web de confianza. Esta lista se actualiza con las bases de datos antivirus de la aplicación. Puede ver la lista predefinida de sitios web de confianza únicamente en la interfaz de Kaspersky Endpoint Security. No puede verla en la Consola de Kaspersky Security Center. |
| **Cuando se visite un dominio cuyo certificado no sea de confianza** | • **Permitir**. 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.<br><br>Cuando el usuario utilice un navegador para acceder a un dominio cuyo certificado no sea de confianza, Kaspersky Endpoint Security le mostrará una página HTML para advertirle que acceder a ese dominio en particular no es recomendable e indicarle por qué. La página contendrá un vínculo para obtener acceso al recurso web solicitado. Una vez que el usuario hace clic en el vínculo, dispone de una hora para visitar otros recursos alojados en el mismo dominio sin que Kaspersky Endpoint Security le advierta sobre la falta de confianza en el certificado. |

| | |
|---|---|
| | • **Bloquear conexión**. 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.<br><br>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. |
| **Si se presentan errores al analizar una conexión cifrada** | • **Bloquear conexión**. Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security bloquea la conexión de red.<br><br>• **Agregar el dominio a las exclusiones**. Cuando se elige esta opción y ocurre un error al analizar una conexión cifrada, Kaspersky Endpoint Security agrega 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 solo puede consultarse a través de la interfaz local de la aplicación. Para borrar el contenido de la lista, deberá seleccionar **Bloquear conexión**. |
| **Bloquear las conexiones SSL 2.0** | Cuando la casilla está activada, Kaspersky Endpoint Security bloquea las conexiones de red que se establecen con el protocolo SSL 2.0.<br><br>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. |
| **Descifrar conexiones cifradas a sitios web con certificado de EV** | 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.<br><br>Cuando esta casilla está activada, Kaspersky Endpoint Security descifra y controla las conexiones cifradas que se establecen con sitios web que utilizan certificados de EV.<br><br>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 basándose en la dirección del sitio web (por ejemplo, `https://facebook.com`).<br><br>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. |
| **Direcciones de confianza** | Para esta función, se utiliza una lista de direcciones web que Kaspersky Endpoint Security excluye del análisis de conexiones. Puede ingresar un nombre de dominio o una dirección IP. Kaspersky Endpoint Security admite el carácter `*` al ingresar una máscara de nombre de dominio.<br><br>Kaspersky Endpoint Security no admite máscaras para direcciones IP.<br><br>Ejemplos:<br>• `dominio.com`: esta entrada incluye las direcciones `https://dominio.com`, `https://www.dominio.com` y `https://dominio.com/pagina123`. Esta entrada no incluye subdominios (por ejemplo, `subdominio.dominio.com`).<br><br>• `subdominio.dominio.com`: esta entrada incluye las direcciones `https://subdominio.dominio.com` y |

| | |
|---|---|
| | `https://subdominio.dominio.com/pagina123`. Esta entrada no incluye el dominio `dominio.com`.<br><br>• `*.dominio.com`: esta entrada incluye las direcciones `https://peliculas.dominio.com` y `https://imagenes.dominio.com/pagina123`. Esta entrada no incluye el dominio `dominio.com`. |
| **Aplicaciones de confianza** | En esta lista, se enumeran las aplicaciones de confianza cuya actividad no supervisa Kaspersky Endpoint Security durante su funcionamiento. Puede seleccionar los tipos de actividades que Kaspersky Endpoint Security no supervisará (por ejemplo, puede indicarle a la aplicación que no analice el tráfico de red). Kaspersky Endpoint Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara. |
| **Analizar el tráfico seguro en las aplicaciones de Mozilla**<br>*(disponible solo en la interfaz de Kaspersky Endpoint Security)* | Si esta casilla 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.<br><br>Para analizar el tráfico en el navegador Mozilla Firefox y el cliente de correo Thunderbird, debe habilitar el Análisis de conexiones cifradas. Si el análisis de conexiones cifradas está deshabilitado, Kaspersky Endpoint Security no analiza el tráfico del navegador Mozilla Firefox ni el cliente de correo Thunderbird.<br><br>Kaspersky Endpoint Security utiliza el certificado raíz de Kaspersky para descifrar y analizar el tráfico cifrado. Puede seleccionar el almacén de certificados que contendrá el certificado raíz de Kaspersky.<br>• **Usar almacén de certificados de Windows**. El certificado raíz de Kaspersky se agrega a esta tienda durante la instalación de Kaspersky Endpoint Security.<br>• **Usar almacén de certificados de Mozilla**. Mozilla Firefox y Thunderbird utilizan sus propios almacenes de certificados. Si se selecciona el almacén de certificados de Mozilla, debe agregar manualmente el certificado raíz de Kaspersky a este almacén a través de las propiedades del navegador. |

## Interfaz

Puede configurar los ajustes de la interfaz de la aplicación.

Configuración de la interfaz

| Parámetro | Descripción |
|---|---|
| **Interacción con el usuario**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | **Con 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.<br><br>**Con interfaz completa**. La ventana principal de Kaspersky Endpoint Security y el icono ubicado en el área de notificación de Windows estarán disponibles en el equipo cliente. El usuario podrá interactuar con Kaspersky Endpoint Security a través del menú contextual del icono. Kaspersky Endpoint Security también mostrará notificaciones por encima del icono. |

| | |
|---|---|
| | **Ninguna 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. |
| **Configuración de notificaciones** | Tabla con la configuración de notificaciones de eventos de diferentes niveles de importancia que pueden producirse durante el funcionamiento de un componente o tarea, o de la aplicación completa. Kaspersky Endpoint Security muestra notificaciones sobre estos eventos en la pantalla, los envía por correo electrónico o los registra. |
| **Parámetros de notificaciones por correo electrónico.** | Parámetros del servidor SMTP con el que se enviarán las notificaciones de los eventos registrados mientras la aplicación esté en funcionamiento. |
| **Mostrar el estado de la aplicación en el área de notificaciones** | Categorías de eventos de la aplicación que provocan un cambio ( o ) en el icono de Kaspersky Endpoint Security ubicado en el área de notificación de la barra de tareas de Microsoft Windows. Dichos eventos también dan lugar a una notificación emergente. |
| **Notificaciones sobre el estado de las bases de datos antivirus locales** | Configuración de notificaciones sobre bases de datos antivirus obsoletas utilizadas por la aplicación. |
| **Protección con contraseña** | Cuando este interruptor está activado y el usuario intenta realizar una acción alcanzada por la función de protección con contraseña, Kaspersky Endpoint Security solicita la contraseña en cuestión. El alcance de la protección con contraseña se compone de las acciones que se han prohibido (por ejemplo, la desactivación de los componentes de protección) y las cuentas de usuario para las que se han prohibido tales acciones.<br><br>Cuando habilite la protección con contraseña, Kaspersky Endpoint Security le pedirá que establezca la contraseña que se necesitará para realizar operaciones. |
| **Recursos web de soporte técnico**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Lista de vínculos a recursos web que contienen información sobre asistencia técnica para Kaspersky Endpoint Security. Los vínculos agregados se mostrarán en la ventana **Soporte** de la interfaz local de Kaspersky Endpoint Security en lugar de los vínculos estándar. |
| **Mensaje para el usuario**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Mensaje que se muestra en la ventana **Soporte** de la interfaz local de Kaspersky Endpoint Security. |

## Administrar configuración

Puede guardar la configuración actual de Kaspersky Endpoint Security en un archivo y usarla para configurar rápidamente la aplicación en otro equipo. También puede utilizar un archivo de configuración al implementar la aplicación a través de Kaspersky Security Center 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.

Parámetros de administración de la configuración de la aplicación

| Configuración | Descripción |
|---|---|
| **Importar** | Extraiga la configuración de la aplicación de un archivo en formato CFG y aplíquela. |
| **Exportar** | Guarde la configuración actual de la aplicación en un archivo en formato CFG. |
| **Restaurar** | Puede restaurar la configuración recomendada por Kaspersky for Endpoint Security en cualquier momento. Después de restaurar la configuración, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección. |

## Administración de tareas

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

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

Puede crear cuantas tareas locales, de grupo y para selecciones de equipos necesite. Para más información sobre cómo trabajar con grupos de administración y selecciones de equipos, *consulte la Ayuda en línea de Kaspersky Security Center*.

Configuración de Administración de tareas

| Parámetro | Descripción |
|---|---|
| **Permitir el uso de tareas locales** | Si se selecciona la casilla, las tareas locales se muestran en la interfaz local de Kaspersky Endpoint Security. Cuando no haya restricciones adicionales de la directiva, el usuario puede configurar y ejecutar tareas. Sin embargo, la configuración del programa de ejecución de tareas no está disponible para el usuario. El usuario puede ejecutar tareas solo manualmente.<br>Si la casilla de verificación se desactiva, el uso de tareas locales se detiene. En este modo, las tareas locales no se ejecutan según la programación. Las tareas no pueden iniciarse o configurarse en la interfaz local de Kaspersky Endpoint Security, o al funcionar con la línea de comandos.<br>Un usuario puede iniciar un análisis antivirus de un archivo o carpeta al seleccionar la opción **Buscar virus** en el menú contextual del archivo o carpeta. La tarea de análisis se inicia con los valores predeterminados de configuración para la tarea de análisis personalizado. |
| **Permitir que se muestren las tareas de grupo** | Si se selecciona la casilla, las tareas de grupo se muestran en la interfaz local de Kaspersky Endpoint Security. El usuario podrá ver la lista de tareas completa a través de la interfaz de la aplicación. |

| | |
|---|---|
| | Si se desactiva esta casilla, Kaspersky Endpoint Security mostrará una lista de tareas vacía. |
| **Permitir la administración de tareas de grupo** | Si se selecciona esta casilla, los usuarios podrán iniciar y detener las tareas de grupo que se creen en Kaspersky Security Center. Podrán para ello usar cualquiera de las dos interfaces de la aplicación (completa o simplificada).<br><br>Si se desactiva esta casilla, Kaspersky Endpoint Security iniciará las tareas programadas automáticamente. El administrador también podrá iniciar estas tareas manualmente a través de Kaspersky Security Center. |

# Análisis del equipo

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

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

## Análisis completo

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

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

Los especialistas de Kaspersky recomiendan no modificar el alcance de la tarea *Análisis completo*.

Para reducir el impacto en los recursos del equipo, recomendamos realizar un análisis en segundo plano en lugar de un análisis completo. El nivel de seguridad del equipo no se verá afectado.

## Análisis de áreas críticas

De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del kernel, los procesos en ejecución y los sectores de inicio del disco.

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

## Análisis personalizado

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

- Memoria del kernel
- Objetos cargados al iniciar el sistema operativo
- Copia de seguridad del sistema operativo
- el buzón de correo de Outlook
- los discos duros, las unidades extraíbles y las 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 inicio, la memoria del sistema y la partición del sistema.

## Comprobación de integridad

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

Configuración del análisis

| Parámetro | Descripción |
| --- | --- |
| **Nivel de seguridad** | Kaspersky Endpoint Security puede usar diferentes grupos de configuraciones para ejecutar un análisis. Estos grupos de configuraciones que se almacenan en la aplicación se denominan *niveles de seguridad*.<br>• **Alto**. Kaspersky Endpoint Security analiza todos los tipos de archivos. Al analizar archivos compuestos, Kaspersky Endpoint Security también analiza archivos en formato de correo.<br>• **Recomendado**. Kaspersky Endpoint Security analiza solamente los formatos de archivo especificados en todos los discos duros, las unidades de red, los medios de almacenamiento extraíbles del equipo y los objetos OLE integrados. Kaspersky Endpoint Security no analiza los archivos de almacenamiento ni los paquetes de instalación.<br>• **Bajo**. Kaspersky Endpoint Security analiza solamente los archivos nuevos o modificados con las extensiones especificadas en todos los discos duros, las unidades extraíbles y las unidades de red del equipo. Kaspersky Endpoint Security no analiza los archivos compuestos. |
| **Acción al detectar una amenaza** | **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos. |

| | |
|---|---|
| | **Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.<br>**Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos.<br>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 si se puede desinfectar en el futuro. |
| **Alcance de la protección** | Lista de objetos que analiza Kaspersky Endpoint Security cuando realiza una tarea de análisis. Los objetos dentro del alcance del análisis pueden incluir la memoria Kernel, procesos en ejecución, sectores de arranque, almacenamiento de copias de seguridad del sistema, bases de datos de correo electrónico, discos duros, unidades extraíbles o unidades de red, una carpeta o un archivo. |
| **Programa de análisis** | **Manual**. Modo de ejecución en el que puede iniciar el análisis manualmente en el momento que sea conveniente para usted.<br>**Programado**. En este modo de ejecución de la tarea de análisis, Kaspersky Endpoint Security inicia la tarea de análisis de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de análisis, también puede iniciar manualmente la tarea de análisis. |
| **Ejecutar tareas omitidas**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea de análisis omitida tan pronto como sea posible. La tarea de análisis puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea.<br>Si la casilla no está seleccionada, Kaspersky Endpoint Security no ejecuta las tareas de análisis omitidas. En lugar de eso, ejecuta la siguiente tarea de análisis según la programación actual. |
| **Ejecutar solo cuando el equipo está inactivo** | Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. |
| **Ejecutar análisis como** | De forma predeterminada, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. El alcance de la protección puede incluir unidades de red u otros objetos que requieren derechos especiales para acceder. Puede especificar un usuario que posea los derechos requeridos en la configuración de Kaspersky Endpoint Security y ejecutar la tarea de análisis con la cuenta de este usuario. |
| **Tipos de archivos** | Kaspersky Endpoint Security considera los archivos sin extensión como ejecutables. Kaspersky Endpoint Security siempre analiza los archivos ejecutables, independientemente de los tipos de archivo que seleccione para analizar.<br>**Todos los archivos**. Si esta configuración está habilitada, Kaspersky Endpoint Security revisa todos los archivos sin excepción (todos los formatos y las extensiones). |

| | |
|---|---|
| | **Archivos analizados según su formato**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. Antes de analizar un archivo en busca de código malintencionado, se analiza el encabezado interno del archivo para determinar el formato del archivo (por ejemplo, .txt, .doc o .exe). El análisis también busca archivos con extensiones de archivo particulares.<br>**Archivos analizados según su extensión**. Si esta configuración está habilitada, Kaspersky Endpoint Security analiza únicamente los archivos que se pueden infectar. El formato de archivo se determina según su extensión. |
| **Analizar solo archivos nuevos y modificados** | Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como compuestos. |
| **Omitir archivos que se analicen por más de N segundos** | Limita la duración del análisis de un solo objeto. Luego de un período especificado de tiempo, Kaspersky Endpoint Security detiene el análisis de un archivo. Esto ayuda a reducir la duración del análisis. |
| **Analizar archivos de almacenamiento** | Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE. |
| **Analizar paquetes de distribución** | Use esta casilla para habilitar/deshabilitar el análisis de paquetes de distribución de terceros. |
| **Analizar archivos de Microsoft Office** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **Analizar formatos de correo electrónico** | La casilla habilita o deshabilita la opción para que Kaspersky Endpoint Security analice los archivos en formatos de correo electrónico y bases de datos de correo.<br>La aplicación analiza completamente solo los formatos de archivo de correo MS Outlook, Windows Mail/Outlook Express y EML, y solo si el equipo tiene el cliente de correo MS Outlook x86.<br>Si la casilla está seleccionada, Kaspersky Endpoint Security divide el archivo de formato de correo en sus componentes (encabezado, cuerpo, archivos adjuntos) y lo analiza en busca de amenazas.<br>Si se desactiva la casilla, Kaspersky Endpoint Security analiza el archivo de formato de correo como si fuera un único archivo. |
| **Analizar archivos de almacenamiento protegidos por contraseña** | Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los archivos de almacenamiento protegidos por contraseña. Para analizar los archivos de un archivo de almacenamiento, se le solicitará que escriba la contraseña.<br>Si se desactiva la casilla, Kaspersky Endpoint Security ignorará el análisis de los archivos de almacenamiento protegidos por contraseña. |
| **No desempaquetar archivos compuestos grandes** | Si esta casilla está seleccionada, Kaspersky Endpoint Security no analiza los archivos compuestos si su tamaño excede el valor.<br>Si esta casilla está desactivada, Kaspersky Endpoint Security analiza los archivos compuestos de todos los tamaños.<br>Kaspersky Endpoint Security analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla está marcada o no. |
| **Aprendizaje automático y análisis de firmas** | El método aprendizaje automático y análisis de firmas usa las bases de datos de Kaspersky Endpoint Security que contienen descripciones de las amenazas conocidas y |

| | |
|---|---|
| | las formas para neutralizarlas. La protección que usa este método proporciona el nivel de seguridad mínimo aceptable.<br>Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado. |
| **Análisis heurístico** | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br>Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Tecnología iSwift** | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS. |
| **Tecnología iChecker** | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |

## 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 inicio, la memoria del sistema y la partición del sistema. La aplicación inicia un análisis en segundo plano en los siguientes casos:

- después de que se actualizan las bases de datos antivirus;
- cuando Kaspersky Endpoint Security se ha estado ejecutando por treinta minutos;
- cada seis horas;
- Cuando el equipo está inactivo durante cinco minutos o más (el equipo está bloqueado o el protector de pantalla está encendido).

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

- el equipo pasa al modo activo;

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

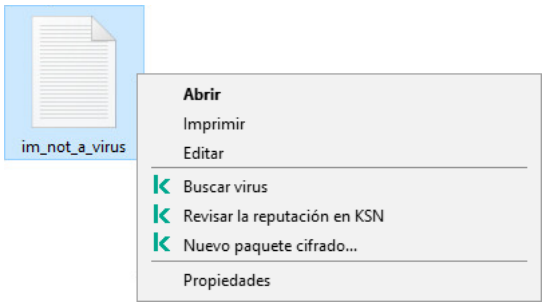
- el equipo (portátil) comienza a funcionar con batería.

Cuando se realiza un análisis en segundo plano, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.

## Análisis desde el menú contextual

Kaspersky Endpoint Security permite analizar archivos individuales en busca de virus y otras clases de malware desde el menú contextual (vea la siguiente imagen).

Cuando se realiza un análisis desde el menú contextual, Kaspersky Endpoint Security no analiza los archivos cuyo contenido está almacenado en la nube de OneDrive.




Análisis desde el menú contextual

Analizar desde la configuración de tareas del menú contextual

| Parámetro | Descripción |
|---|---|
| **Acción al detectar una amenaza** | **Desinfectar; eliminar si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si falla la desinfección, Kaspersky Endpoint Security elimina los archivos.<br>**Desinfectar; bloquear si falla la desinfección**. Si esta opción está seleccionada, Kaspersky Endpoint Security automáticamente intenta desinfectar todos los archivos infectados que detecta. Si la desinfección no es posible, Kaspersky Endpoint Security agrega la información sobre los archivos infectados que se detectan a la lista de amenazas activas.<br>**Informar**. Si esta opción se selecciona, Kaspersky Endpoint Security agrega la información sobre archivos infectados a la lista de amenazas activas en la detección de estos archivos. |
| **Analizar solo archivos nuevos y modificados** | Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como compuestos. |
| **Omitir archivos que se analicen por más de N seg** | Limita la duración del análisis de un solo objeto. Luego de un período especificado de tiempo, Kaspersky Endpoint Security detiene el análisis de un archivo. Esto ayuda a reducir la duración del análisis. |

| | |
|---|---|
| **Analizar archivos de almacenamiento** | Analiza archivos en los siguientes formatos: RAR, ARJ, ZIP, CAB, LHA, JAR e ICE. |
| **Analizar paquetes de distribución** | La casilla habilita o deshabilita el análisis de los paquetes de distribución. |
| **Analizar archivos de Microsoft Office** | Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. |
| **No desempaquetar archivos compuestos grandes** | Si esta casilla está seleccionada, Kaspersky Endpoint Security no analiza los archivos compuestos si su tamaño excede el valor. |
| **Aprendizaje automático y análisis de firmas** | El método aprendizaje automático y análisis de firmas usa las bases de datos de Kaspersky Endpoint Security que contienen descripciones de las amenazas conocidas y las formas para neutralizarlas. La protección que usa este método proporciona el nivel de seguridad mínimo aceptable.<br>Según las recomendaciones de los expertos de Kaspersky, el aprendizaje automático y análisis de firmas está siempre habilitado. |
| **Análisis heurístico** | Esta tecnología se desarrolló para detectar amenazas que no pueden detectarse mediante el uso de la versión actual de las bases de datos de la aplicación de Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de un virus conocido.<br><br>Al analizar archivos en busca de código malintencionado, el analizador heurístico ejecuta instrucciones en los archivos ejecutables. La cantidad de instrucciones que ejecuta el analizador heurístico depende del nivel especificado para el analizador heurístico. El nivel del análisis heurístico garantiza un equilibrio entre la profundidad del análisis de nuevas amenazas, la carga sobre los recursos del sistema operativo y la duración del análisis heurístico. |
| **Tecnología iSwift** | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de publicación de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. La tecnología iSwift es un avance de la tecnología iChecker para el sistema de archivos NTFS. |
| **Tecnología iChecker** | Esta tecnología permite aumentar la velocidad del análisis al excluir ciertos archivos del análisis. Los archivos se excluyen del análisis mediante un algoritmo especial que tiene en cuenta la fecha de lanzamiento de las bases de datos de Kaspersky Endpoint Security, la fecha en que se analizó por última vez el archivo y cualquier modificación que se haya realizado a la configuración de análisis. Existen limitaciones en el uso de la tecnología iChecker: no funciona con archivos de gran tamaño y solamente se implementa en los archivos con una estructura reconocida por la aplicación (por ejemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |

## Análisis de unidades extraíbles

Kaspersky Endpoint Security le permite analizar los unidades extraíbles en busca de virus y otras clases de malware cuando se conectan al equipo.

| Parámetro | Descripción |
|---|---|
| **Acción cuando se conecte una unidad extraíble** | • **No analizar**.<br>• **Análisis detallado** Si se selecciona esta opción, después de que se conecta un disco extraíble, Kaspersky Endpoint Security analiza todos los archivos localizados en el disco extraíble, incluidos los archivos dentro de objetos compuestos.<br>• **Análisis rápido**. Si se selecciona esta opción, cuando se conecte una unidad extraíble, Kaspersky Endpoint Security analizará solo los archivos que sean de algunos formatos específicos, por ser los más propensos a estar infectados. Los objetos compuestos no se desempaquetarán. |
| **Tamaño máximo de la unidad extraíble** | Si se selecciona esta casilla, Kaspersky Endpoint Security realiza la acción seleccionada en la lista desplegable **Acción cuando se conecte una unidad extraíble** en los unidades extraíbles cuyo tamaño no excede el tamaño máximo especificado.<br>Si se desactiva la casilla, Kaspersky Endpoint Security realiza la acción seleccionada en la lista desplegable **Acción cuando se conecte una unidad extraíble** en los unidades extraíbles de cualquier tamaño. |
| **Mostrar el progreso del análisis** | Si se selecciona la casilla, Kaspersky Endpoint Security muestra el progreso de análisis de las unidades extraíbles en una ventana independiente y en la ventana **Tareas**.<br>Si la casilla se desactiva, Kaspersky Endpoint Security realiza los análisis de las unidades extraíbles en segundo plano. |
| **No permitir que se detenga la tarea de análisis** | Si se selecciona esta casilla, el botón **Detener** no estará disponible ni en la ventana **Tareas** ni en la ventana **Análisis antivirus** de la interfaz local de Kaspersky Endpoint Security. |

## Comprobación de integridad

Kaspersky Endpoint Security verifica si los archivos almacenados en la carpeta de instalación del programa presentan daños 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.

Para crear la tarea *Comprobación de integridad*, deberá usar la Consola de administración de Kaspersky Security Center 12 o Kaspersky Security Center 12 Web Console. No es posible crear esta tarea con Kaspersky Security Center Cloud Console.

Las siguientes situaciones pueden comprometer la integridad de la aplicación:

- Un objeto malicioso modifica los archivos de Kaspersky Endpoint Security. Ante esta situación, siga el procedimiento para restaurar Kaspersky Endpoint Security con las herramientas del sistema operativo. Cuando concluya la restauración, realice un análisis completo del equipo y ejecute nuevamente la comprobación de integridad.
- La firma digital llega a su fecha de caducidad. Ante esta situación, actualice Kaspersky Endpoint Security.

| Parámetro | Descripción |
| --- | --- |
| **Programa de análisis** | **Manual**. Modo de ejecución en el que puede iniciar el análisis manualmente en el momento que sea conveniente para usted.<br>**Programado**. En este modo de ejecución de la tarea de análisis, Kaspersky Endpoint Security inicia la tarea de análisis de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de análisis, también puede iniciar manualmente la tarea de análisis. |
| **Ejecutar tareas omitidas** | Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea de análisis omitida tan pronto como sea posible. La tarea de análisis puede omitirse, por ejemplo, si el equipo estaba apagado a la hora de inicio programada de dicha tarea.<br>Si la casilla no está seleccionada, Kaspersky Endpoint Security no ejecuta las tareas de análisis omitidas. En lugar de eso, ejecuta la siguiente tarea de análisis según la programación actual. |
| **Ejecutar solo cuando el equipo está inactivo** | Inicio pospuesto de la tarea de análisis cuando los recursos del equipo están ocupados. Kaspersky Endpoint Security inicia la tarea de análisis si el equipo está bloqueado o el protector de pantalla está activado. |
| **Ejecutar como**<br>*(disponible solo en la Consola de Kaspersky Security Center)* | De forma predeterminada, la tarea de análisis se ejecuta en nombre del usuario con cuyos derechos está registrado en el sistema operativo. Es posible que se requieran permisos especiales para acceder a la carpeta de instalación de la aplicación. Puede especificar un usuario que posea los derechos requeridos en la configuración de Kaspersky Endpoint Security y ejecutar la tarea de análisis con la cuenta de este usuario. |

## Actualización de bases de datos y módulos de software de la aplicación

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Endpoint Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

Las actualizaciones regulares requieren una licencia en vigencia. Si no hay una licencia actual, se podrá realizar una única actualización.

La principal fuente de actualizaciones de Kaspersky Endpoint Security son los servidores de actualizaciones de Kaspersky.

Su equipo debe estar conectado a Internet para descargar correctamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. Por defecto, la configuración de la conexión a Internet se determina automáticamente. Si utiliza un servidor proxy, debe definir su configuración.

Las actualizaciones se descargan usando el protocolo HTTPS. No obstante, cuando es la única opción posible, la descarga también puede realizarse con el protocolo HTTP.

Al realizar una actualización, se descargan e instalan en el equipo los siguientes objetos:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se brinda con bases de datos que contienen firmas de virus y otras amenazas e información sobre maneras de neutralizarlas. Los componentes de protección utilizan esta información al realizar búsquedas de archivos infectados en el equipo y neutralizarlos. Las bases de datos se actualizan constantemente con registros de amenazas nuevas y métodos para contrarrestarlas. Por lo tanto, le recomendamos actualizar las bases de datos con regularidad.

  Además de las bases de datos de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de la aplicación interceptar el tráfico de la red.

- Módulos de la aplicación. Además de las bases de datos de Kaspersky Endpoint Security, también se pueden actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación repara vulnerabilidades en Kaspersky Endpoint Security y agrega funciones nuevas o mejora funciones existentes.

Durante la actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con la versión actualizada en el origen de actualizaciones. Si las bases de datos y los módulos de la aplicación actuales difieren de las respectivas versiones actualizadas, la parte faltante de las actualizaciones se instala en el equipo.

Los archivos de ayuda contextual se pueden actualizar junto con las actualizaciones de los módulos de la aplicación.

Si las bases de datos están obsoletas, es posible que el tamaño del paquete de actualización sea considerable, lo que puede ocasionar un mayor tráfico web (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en la sección **Actualización** en la ventana **Tareas**.

La información sobre los resultados de la actualización y sobre todos los eventos que ocurren durante la ejecución de la tarea de actualización se registra en el informe de Kaspersky Endpoint Security.

Configuración de actualización de las bases de datos y los módulos de la aplicación

| Parámetro | Descripción |
| --- | --- |
| **Modo de ejecución** | **Automático**. En este modo, Kaspersky Endpoint Security comprueba el origen de las actualizaciones en busca de nuevos paquetes de actualizaciones con una cierta frecuencia. La frecuencia de las comprobaciones para detectar paquetes de actualizaciones aumenta durante las epidemias de virus y disminuye cuando no hay epidemias. Después de detectar un paquete de actualizaciones nuevo, Kaspersky Endpoint Security lo descarga e instala las actualizaciones en el equipo.<br>**Manual**. Este modo de ejecución de la tarea de actualización permite iniciar manualmente la tarea de actualización.<br>**Programado**. En este modo de ejecución de la tarea de actualización, Kaspersky Endpoint Security ejecuta la tarea de actualización de acuerdo con la programación especificada por el usuario. Si se selecciona este modo de ejecución de la tarea de actualización, también se puede iniciar manualmente la tarea de actualización de Kaspersky Endpoint Security. |
| **Ejecutar tareas omitidas** | Si la casilla está seleccionada, Kaspersky Endpoint Security inicia la tarea de actualización ignorada tan pronto como es posible. La tarea de actualización puede ignorarse, por ejemplo, si el equipo se apagó a la hora de inicio de dicha tarea. |

| | |
|---|---|
| | Si la casilla está desactivada, Kaspersky Endpoint Security no inicia las tareas de actualización ignoradas. En lugar de eso, ejecuta la siguiente tarea de actualización según la programación actual. |
| **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.<br><br>Como origen de actualizaciones, puede utilizar el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky o una carpeta local o de red dispuesta para tal fin.<br><br>La lista por defecto de orígenes de actualizaciones incluye a los servidores de actualización de Kaspersky Security Center y de Kaspersky. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las actualizaciones.<br><br>Kaspersky Endpoint Security no admite actualizaciones que provengan de servidores HTTPS, a menos que sean servidores de actualización de Kaspersky.<br><br>Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno tras otro, comenzando por el principio de la lista, y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible. |
| **Ejecutar la tarea como** | Por defecto, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta ha usado para iniciar sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security puede actualizarse desde un origen de actualizaciones al cual el usuario que inició sesión no puede acceder debido a la falta de permisos exigidos (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o una fuente de actualización para la cual no se ha configurado la autenticación del servidor proxy. En la configuración de Kaspersky Endpoint Security, puede especificar un usuario que tenga dichos permisos y comenzar la tarea de actualización de Kaspersky Endpoint Security según dicha cuenta de usuario. |
| **Descargar actualizaciones de módulos de la aplicación** | Esta casilla activa o desactiva la descarga de actualizaciones de los módulos de la aplicación y las bases de datos antivirus.<br><br>Si está seleccionada la casilla, Kaspersky Endpoint Security notifica al usuario sobre actualizaciones de módulos de aplicación disponibles e incluye las actualizaciones de los módulos de aplicación en el paquete de actualización mientras se ejecuta la tarea de actualización. La forma en la que se aplican las actualizaciones de los módulos de la aplicación está determinada por la siguiente configuración:<br><br>• **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.<br><br>• **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Endpoint Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. Esta opción está seleccionada por defecto. |

| | |
|---|---|
| | Si está desmarcada la casilla, Kaspersky Endpoint Security no notifica al usuario sobre actualizaciones de módulos de aplicación disponibles y no incluye las actualizaciones de los módulos de aplicación en el paquete de actualización mientras se ejecuta la tarea de actualización.<br><br>Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final.<br><br>Esta casilla está seleccionada por defecto. |
| **Copiar las actualizaciones en la carpeta** | Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security copia el paquete de actualizaciones a la carpeta compartida especificada bajo la casilla de verificación. A continuación, otros equipos en la LAN pueden recibir el paquete de actualización desde esta carpeta compartida. Esto reduce el tráfico de Internet debido a que el paquete de actualización sólo puede descargarse una vez. La carpeta especificada por defecto es `C:\ProgramData\Kaspersky Lab\KES\Update distribution\`. |
| **Servidor proxy para actualizaciones**<br>*(disponible solo en la interfaz de Kaspersky Endpoint Security)* | Configuración del servidor proxy para el acceso a Internet de los usuarios de equipos cliente para actualizar los módulos de la aplicación y las bases de datos.<br><br>Para la configuración automática de un servidor proxy, Kaspersky Endpoint Security usa el protocolo WPAD (protocolo de detección automática de proxy web). Si la dirección IP del servidor proxy no se puede determinar a través de este protocolo, Kaspersky Endpoint Security usa la dirección especificada en la configuración del navegador Microsoft Internet Explorer. |
| **No usar el servidor proxy para las direcciones locales**<br>*(disponible solo en la interfaz de Kaspersky Endpoint Security)* | Si la casilla está seleccionada, Kaspersky Endpoint Security no utiliza un servidor proxy cuando realiza una actualización desde una carpeta compartida. |

# Apéndice 2. Grupos de confianza de aplicaciones

Kaspersky Endpoint Security categoriza todas las aplicaciones que se inician en el equipo en grupos de confianza. Se categorizan según el nivel de peligrosidad que las aplicaciones suponen para el sistema operativo.

Los grupos de confianza se organizan del siguiente modo:

- **De confianza**. Este grupo incluye las aplicaciones para las que se cumplen una o más de las siguientes condiciones:
  - las aplicaciones tienen la firma digital de un proveedor de confianza;
  - las aplicaciones están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;

- las aplicaciones han sido colocadas por el usuario en el grupo De confianza.

No hay ninguna operación prohibida para estas aplicaciones.

- **Restricción mínima**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - las aplicaciones no tienen la firma digital de un proveedor de confianza;
  - las aplicaciones no están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - las aplicaciones han sido colocadas por el usuario en el grupo Restricción mínima.

  Estas aplicaciones están sujetas a restricciones mínimas para el acceso a los recursos del sistema operativo.
- **Restricción máxima**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - las aplicaciones no tienen la firma digital de un proveedor de confianza;
  - las aplicaciones no están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - las aplicaciones han sido colocadas por el usuario en el grupo Restricción máxima.

  Estas aplicaciones están sujetas a restricciones máximas para el acceso a los recursos del sistema operativo.
- **No confiables**. Este grupo incluye aplicaciones para las que se cumplen las siguientes condiciones:
  - las aplicaciones no tienen la firma digital de un proveedor de confianza;
  - las aplicaciones no están registradas en la base de datos de aplicaciones de confianza de Kaspersky Security Network;
  - las aplicaciones han sido colocadas por el usuario en el grupo No confiables.

  Estas aplicaciones no tienen permitido realizar ninguna operación.

# Apéndice 3. Extensiones de archivo para el análisis rápido de unidades extraíbles

com: archivo ejecutable de una aplicación que no supera los 64 KB

exe: archivo ejecutable o archivo autoextraíble

sys: archivo de sistema de Microsoft Windows

prg – texto de programas para dBase™, Clipper o Microsoft FoxPro Visual®, o un programa WAVmaker

bin: archivo binario

bat: archivo de lote

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para el DOS), OS/2

dpl: biblioteca Borland Delphi comprimida

dll: biblioteca de vínculos dinámicos

scr: pantalla inicial de Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto de Microsoft OLE (Object Linking and Embedding)

tsp: programa que se ejecuta en modo de tiempo dividido

drv: controlador de dispositivos

vxd: controlador de dispositivos virtuales de Microsoft Windows

pif: archivo de información del programa

lnk: archivo de vínculos de Microsoft Windows

reg: archivo de claves del registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de la configuración para Microsoft Windows, Windows NT y algunas aplicaciones

cla: clase de Java

vbs – script de Visual Basic®

vbe: extensión de video del BIOS

js, jse: texto fuente de JavaScript

htm: documento del hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta – programa de hipertexto para Microsoft Internet Explorer®

asp: script de Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script que se integra en archivos HTML

wsh: archivo de Microsoft Windows Script Host

wsf: script de Microsoft Windows

the: archivo del tapiz de escritorio de Microsoft Windows 95

hlp: archivo de ayuda de Windows

eml: mensaje de correo electrónico de Microsoft Outlook Express

nws: nuevo mensaje de correo electrónico de Microsoft Outlook Express

msg: mensaje de correo electrónico de Microsoft Mail

plg: mensaje de correo electrónico

mbx: mensaje de correo electrónico guardado de Microsoft Office Outlook

doc*: documentos de Microsoft Office Word, por ejemplo: doc para documentos de Microsoft Office Word, docx para documentos de Microsoft Office Word 2007 compatibles con XML, y docm para documentos de Microsoft Office Word 2007 compatibles con macros

dot*: plantillas de documentos de Microsoft Office Word, por ejemplo: dot para plantillas de documentos de Microsoft Office Word, dotx para plantillas documentos de Microsoft Office Word 2007 y dotm para plantillas de documentos de Microsoft Office Word 2007 compatibles con macros

fpm: programa de base de datos, archivo de inicio de Microsoft Visual FoxPro

rtf: documento con formato de texto enriquecido

shs: fragmento del manipulador de objetos de desecho de la Shell de Windows

dwg – base de datos de planos de AutoCAD®

msi: paquete de Microsoft Windows Installer

otm: proyecto de VBA para Microsoft Office Outlook

pdf: documento de Adobe Acrobat

swf – objeto del paquete de Shockwave® Flash

jpg, jpeg: formato de gráfico de imagen comprimida

emf: archivo con formato de metarchivo mejorado

ico: archivo de icono de objeto

ov? - archivos ejecutables de Microsoft Office Word

xl*: documentos y archivos de Microsoft Office Excel, por ejemplo: xls, la extensión correspondiente a Microsoft Office Excel, xlc para diagramas, xlt para plantillas de documentos, xlsx para libros de Microsoft Office Excel 2007, xltm para libros de Microsoft Office Excel 2007 compatibles con macros, xlsb para libros de Microsoft Office Excel 2007 en formato binario (no XML), xltx para plantillas de Microsoft Office Excel 2007, xlsm para plantillas de Microsoft Office Excel 2007 compatibles con macros y xlam para complementos de Microsoft Office Excel 2007 compatibles con macros

pp* – documentos y archivos de Microsoft Office PowerPoint®, por ejemplo: pps para diapositivas de Microsoft Office PowerPoint, ppt para presentaciones, pptx para presentaciones de Microsoft Office PowerPoint 2007, pptm para presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, potx para plantillas de presentaciones de Microsoft Office PowerPoint 2007, potm para plantillas de presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007, ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 compatibles con macros y ppam para complementos de Microsoft Office PowerPoint 2007 compatibles con macros

md* – documentos y archivos de Microsoft Office Access®, por ejemplo: mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: una diapositiva de Microsoft PowerPoint 2007

sldm: una diapositiva de Microsoft PowerPoint 2007 compatible con macros

thmx: un tema de Microsoft Office 2007

# Apéndice 4. Tipos de archivo para el filtro de adjuntos de Protección contra amenazas de correo

Tenga en cuenta que el formato real de un archivo puede no coincidir con la extensión de su nombre de archivo.

Si habilita el filtrado de objetos adjuntos a mensajes de correo electrónico, el componente Protección contra amenazas de correo puede renombrar o eliminar archivos con las extensiones siguientes:

com: archivo ejecutable de una aplicación que no supera los 64 KB

exe: archivo ejecutable o archivo autoextraíble

sys: archivo de sistema de Microsoft Windows

prg – texto de programas para dBase™, Clipper o Microsoft FoxPro Visual®, o un programa WAVmaker

bin: archivo binario

bat: archivo de lote

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para el DOS), OS/2

dpl: biblioteca Borland Delphi comprimida

dll: biblioteca de vínculos dinámicos

scr: pantalla inicial de Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto de Microsoft OLE (Object Linking and Embedding)

tsp: programa que se ejecuta en modo de tiempo dividido

drv: controlador de dispositivos

vxd: controlador de dispositivos virtuales de Microsoft Windows

pif: archivo de información del programa

lnk: archivo de vínculos de Microsoft Windows

reg: archivo de claves del registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de la configuración para Microsoft Windows, Windows NT y algunas aplicaciones

cla: clase de Java

vbs – script de Visual Basic®

vbe: extensión de video del BIOS

js, jse: texto fuente de JavaScript

htm: documento del hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta – programa de hipertexto para Microsoft Internet Explorer®

asp: script de Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script que se integra en archivos HTML

wsh: archivo de Microsoft Windows Script Host

wsf: script de Microsoft Windows

the: archivo del tapiz de escritorio de Microsoft Windows 95

hlp: archivo de ayuda de Windows

eml: mensaje de correo electrónico de Microsoft Outlook Express

nws: nuevo mensaje de correo electrónico de Microsoft Outlook Express

msg: mensaje de correo electrónico de Microsoft Mail

plg: mensaje de correo electrónico

mbx: mensaje de correo electrónico guardado de Microsoft Office Outlook

doc*: documentos de Microsoft Office Word, por ejemplo: doc para documentos de Microsoft Office Word, docx para documentos de Microsoft Office Word 2007 compatibles con XML, y docm para documentos de Microsoft Office Word 2007 compatibles con macros

dot*: plantillas de documentos de Microsoft Office Word, por ejemplo: dot para plantillas de documentos de Microsoft Office Word, dotx para plantillas documentos de Microsoft Office Word 2007 y dotm para plantillas de documentos de Microsoft Office Word 2007 compatibles con macros

fpm: programa de base de datos, archivo de inicio de Microsoft Visual FoxPro

rtf: documento con formato de texto enriquecido

shs: fragmento del manipulador de objetos de desecho de la Shell de Windows

dwg – base de datos de planos de AutoCAD®

msi: paquete de Microsoft Windows Installer

otm: proyecto de VBA para Microsoft Office Outlook

pdf: documento de Adobe Acrobat

swf – objeto del paquete de Shockwave® Flash

jpg, jpeg: formato de gráfico de imagen comprimida

emf: archivo con formato de metarchivo mejorado

ico: archivo de icono de objeto

ov? - archivos ejecutables de Microsoft Office Word

xl*: documentos y archivos de Microsoft Office Excel, por ejemplo: xls, la extensión correspondiente a Microsoft Office Excel, xlc para diagramas, xlt para plantillas de documentos, xlsx para libros de Microsoft Office Excel 2007, xltm para libros de Microsoft Office Excel 2007 compatibles con macros, xlsb para libros de Microsoft Office Excel 2007 en formato binario (no XML), xltx para plantillas de Microsoft Office Excel 2007, xlsm para plantillas de Microsoft Office Excel 2007 compatibles con macros y xlam para complementos de Microsoft Office Excel 2007 compatibles con macros

pp* – documentos y archivos de Microsoft Office PowerPoint®, por ejemplo: pps para diapositivas de Microsoft Office PowerPoint, ppt para presentaciones, pptx para presentaciones de Microsoft Office PowerPoint 2007, pptm para presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, potx para plantillas de presentaciones de Microsoft Office PowerPoint 2007, potm para plantillas de presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007, ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 compatibles con macros y ppam para complementos de Microsoft Office PowerPoint 2007 compatibles con macros

md* – documentos y archivos de Microsoft Office Access®, por ejemplo: mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: una diapositiva de Microsoft PowerPoint 2007

sldm: una diapositiva de Microsoft PowerPoint 2007 compatible con macros

thmx: un tema de Microsoft Office 2007

# Apéndice 5. Configuración de red para la interacción con servicios externos

Kaspersky Endpoint Security utiliza la siguiente configuración de red para interactuar con servicios externos.

Configuración de red

| Dirección | Descripción |
| --- | --- |
| `activation-v2.kaspersky.com/activationservice/activationservice.svc`<br>Protocolo: `HTTPS`<br>Puerto: `443` | Activación de la aplicación |
| `s00.upd.kaspersky.com`<br>`s01.upd.kaspersky.com`<br>`s02.upd.kaspersky.com`<br>`s03.upd.kaspersky.com`<br>`s04.upd.kaspersky.com`<br>`s05.upd.kaspersky.com`<br>`s06.upd.kaspersky.com`<br>`s07.upd.kaspersky.com`<br>`s08.upd.kaspersky.com`<br>`s09.upd.kaspersky.com`<br>`s10.upd.kaspersky.com`<br>`s11.upd.kaspersky.com`<br>`s12.upd.kaspersky.com`<br>`s13.upd.kaspersky.com`<br>`s14.upd.kaspersky.com`<br>`s15.upd.kaspersky.com`<br>`s16.upd.kaspersky.com`<br>`s17.upd.kaspersky.com`<br>`s18.upd.kaspersky.com`<br>`s19.upd.kaspersky.com`<br>`cm.k.kaspersky-labs.com`<br>Protocolo: `HTTPS`<br>Puerto: `443` | Actualizar las bases de datos y los módulos de la aplicación |
| `downloads.upd.kaspersky.com`<br>Protocolo: `HTTPS`<br>Puerto: `443` | • Actualizar las bases de datos y los módulos de la aplicación<br>• Verificar si se puede acceder a los servidores de Kaspersky. Si el acceso a los servidores mediante el DNS del sistema no es posible, la aplicación utiliza el DNS público. Esto es |

| | |
|---|---|
| | necesario para asegurarse de que las bases de datos antivirus estén actualizadas y se mantenga el nivel de seguridad del equipo. Kaspersky Endpoint Security utiliza la siguiente lista de servidores DNS públicos en el siguiente orden:<br>1. Google Public DNS (8.8.8.8).<br>2. Cloudflare DNS (1.1.1.1).<br>3. Alibaba Cloud DNS (223.6.6.6).<br>4. Quad9 DNS (9.9.9.9).<br>5. CleanBrowsing (185.228.168.168).<br>Las solicitudes emitidas por la aplicación pueden contener direcciones de dominios y la dirección IP pública del usuario, ya que la aplicación establece una conexión TCP/UDP con el servidor DNS. Esta información es necesaria, por ejemplo, para validar el certificado de un recurso web cuando se utiliza HTTPS. Si Kaspersky Endpoint Security utiliza un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio correspondiente. Si desea evitar que Kaspersky Endpoint Security utilice un servidor DNS público, comuníquese con el Servicio de soporte técnico para obtener un parche privado. |
| `touch.kaspersky.com`<br>Protocolo: `HTTP` | • Recibiendo el tiempo de confianza para revisar el periodo de validez del certificado (conexión TLS). |

| | |
|---|---|
| | • Advertencia sobre la denegación de acceso a un recurso web en el navegador (Protección contra amenazas web y Control web) |
| `p00.upd.kaspersky.com`<br>`p01.upd.kaspersky.com`<br>`p02.upd.kaspersky.com`<br>`p03.upd.kaspersky.com`<br>`p04.upd.kaspersky.com`<br>`p05.upd.kaspersky.com`<br>`p06.upd.kaspersky.com`<br>`p07.upd.kaspersky.com`<br>`p08.upd.kaspersky.com`<br>`p09.upd.kaspersky.com`<br>`p10.upd.kaspersky.com`<br>`p11.upd.kaspersky.com`<br>`p12.upd.kaspersky.com`<br>`p13.upd.kaspersky.com`<br>`p14.upd.kaspersky.com`<br>`p15.upd.kaspersky.com`<br>`p16.upd.kaspersky.com`<br>`p17.upd.kaspersky.com`<br>`p18.upd.kaspersky.com`<br>`p19.upd.kaspersky.com`<br>`downloads.kaspersky-labs.com`<br>`cm.k.kaspersky-labs.com`<br>Protocolo: `HTTP`<br>Puerto: `80` | Actualizar las bases de datos y los módulos de la aplicación |
| `ds.kaspersky.com`<br>Protocolo: `HTTPS`<br>Puerto: `443` | Uso de Kaspersky Security Network |
| `ksn-a-stat-geo.kaspersky-labs.com`<br>`ksn-file-geo.kaspersky-labs.com`<br>`ksn-verdict-geo.kaspersky-labs.com`<br>`ksn-url-geo.kaspersky-labs.com`<br>`ksn-a-p2p-geo.kaspersky-labs.com`<br>`ksn-info-geo.kaspersky-labs.com`<br>`ksn-cinfo-geo.kaspersky-labs.com`<br>Protocolo: `Cualquier`<br>Puerto: `443`, `1443` | Uso de Kaspersky Security Network |
| | |

| | |
|---|---|
| `click.kaspersky.com`<br>`redirect.kaspersky.com`<br>Protocolo: `HTTPS` | Haga clic en los vínculos de la interfaz |
| `crl.kaspersky.com`<br>`ocsp.kaspersky.com`<br>Protocolo: `HTTP`<br>Puerto: `80` | Infraestructura de clave pública (PKI) |

# Apéndice 6. Eventos de la aplicación en el registro de eventos de Windows

Kaspersky Endpoint Security utiliza el registro de eventos de Windows para guardar información sobre el funcionamiento de sus componentes, sobre los eventos de cifrado de datos, sobre la ejecución de las tareas de análisis, actualización y comprobación de integridad, y sobre las operaciones que realiza en general.

**Auditoría del sistema**

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 201 | Contrato de licencia de usuario final infringido | ✓ |
| 203 | Licencia a punto de caducar | – |
| 204 | La licencia está por caducar | – |
| 206 | Faltan las bases de datos o están dañadas | – |
| 207 | Las bases de datos son obsoletas | – |
| 208 | Las bases de datos están desactualizadas | – |
| 209 | La ejecución automática de la aplicación está deshabilitada | – |
| 210 | Actualizaciones automáticas deshabilitadas | – |
| 211 | Autoprotección deshabilitada | – |
| 212 | La tarea no se puede ejecutar | – |
| 213 | Autoprotección bloquea la operación con recursos de la aplicación | – |
| 214 | Componentes de protección deshabilitados | – |
| 215 | El equipo se ejecuta en modo seguro | – |
| 216 | Hay archivos sin procesar | – |
| 217 | Informe borrado | ✓ |
| 218 | Configuración de la aplicación cambiada | ✓ |
| 219 | Directiva de grupo aplicada | ✓ |
| 220 | Directiva de grupo deshabilitada | – |
| 221 | Tarea iniciada | – |
| 222 | Tarea detenida | – |
| 223 | Tarea completada | – |
| 224 | Reinicie la aplicación para completar la actualización | – |
| 225 | Es necesario reiniciar el equipo | ✓ |
| 226 | La licencia permite usar componentes que no se han instalado | – |
| 227 | Los componentes instalados coinciden con la licencia | – |
| 229 | Error de activación | ✓ |
| 230 | Código de activación de reserva incorrecto | – |
| 231 | Se debe iniciar la desinfección avanzada de una amenaza activa detectada | – |
| 232 | Desinfección avanzada iniciada | – |
| 233 | Desinfección avanzada completada | – |
| 235 | Aplicación iniciada | ✓ |
| 236 | Aplicación detenida | ✓ |

| | | |
|---|---|---|
| 237 | La aplicación se cerró en forma forzosa durante una sesión anterior | ✓ |
| 240 | La licencia está por caducar | ✓ |
| 238 | Se modificaron los parámetros de la suscripción | ✓ |
| 239 | Se ha renovado la suscripción | ✓ |
| 335 | Objeto restaurado del Depósito de copias de seguridad | ✓ |
| 336 | No se puede restaurar el objeto del Depósito de copias de seguridad | ✓ |
| 245 | El procesamiento de algunas funciones del SO está deshabilitado | ✓ |
| 250 | Conexión cifrada terminada | ✓ |
| 708 | Configuración de tarea aplicada correctamente | – |
| 335 | Objeto restaurado del Depósito de copias de seguridad | ✓ |
| 2000 | Usar un nombre de usuario y contraseña | – |
| 2001 | Actividad de red sospechosa detectada | – |
| 2020 | La participación en KSN está habilitada | – |
| 2021 | La participación en KSN está deshabilitada | – |
| 2022 | Servidores de KSN disponibles | – |
| 2023 | Servidores de KSN no disponibles | – |
| 2024 | La aplicación funciona y procesa los datos conforme a las leyes pertinentes y utiliza la infraestructura adecuada | ✓ |
| 227 | Todos los componentes de la aplicación definidos por la licencia se instalaron y se ejecutan en modo normal | – |

Detección de comportamientos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo o sus datos personales | – |
| 307 | Objeto eliminado | – |
| 308 | Se creó una copia de seguridad del objeto | – |
| 311 | No se puede crear una copia de seguridad | – |
| 313 | No se puede eliminar | – |
| 323 | El objeto se eliminará al reiniciar | – |
| 329 | Nombre del objeto cambiado | – |
| 331 | Bloqueado | – |
| 452 | Proceso finalizado | – |
| 453 | No se puede finalizar el proceso | – |
| 455 | Reversión completada | – |
| 458 | Valor del registro restaurado | – |
| 459 | Valor del registro eliminado | – |
| 453 | Ejecución de archivo/código bloqueada | – |

## Prevención de exploits

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 302 | Se detectó un objeto malicioso | – |
| 331 | Bloqueado | – |
| 455 | Reversión completada | – |
| 323 | El objeto se eliminará al reiniciar | – |
| 307 | Objeto eliminado | – |
| 329 | Nombre del objeto cambiado | – |
| 457 | Archivo restaurado | – |
| 458 | Valor del registro restaurado | – |
| 459 | Valor del registro eliminado | – |

## Prevención contra intrusos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 301 | Objeto procesado | – |
| 302 | Se detectó un objeto malicioso | – |
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo o sus datos personales | – |
| 306 | Objeto desinfectado | – |
| 307 | Objeto eliminado | – |
| 308 | Se creó una copia de seguridad del objeto | – |
| 310 | No se puede crear una copia de seguridad | – |
| 312 | No se puede desinfectar | – |
| 313 | No se puede eliminar | – |
| 314 | Objeto no procesado | – |
| 315 | Objeto omitido | – |
| 317 | Error de procesamiento | ✓ |
| 318 | Archivo de almacenamiento detectado | – |
| 319 | Objeto empaquetado detectado | – |
| 320 | Objeto cifrado | – |
| 321 | Objeto dañado | – |
| 322 | Archivo de almacenamiento protegido por contraseña detectado | – |
| 323 | El objeto se eliminará al reiniciar | – |
| 324 | El objeto se desinfectará al reiniciar | – |
| 327 | Sobrescrito con una copia desinfectada anteriormente | – |
| 332 | Información sobre el objeto detectado | – |
| 335 | Objeto restaurado del Depósito de copias de seguridad | – |
| 336 | No se puede restaurar el objeto del Depósito de copias de seguridad | ✓ |
| 340 | El objeto está en la lista de admitidos de KSN Privada | ✓ |
| 401 | Aplicación puesta en el grupo de confianza | – |
| 402 | Aplicación puesta en un grupo restringido | – |
| 403 | Prevención de intrusiones en el host accionada | – |
| 452 | Proceso finalizado | – |
| 453 | No se puede finalizar el proceso | – |

Protección contra amenazas de archivos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 302 | Se detectó un objeto malicioso | ✓ |
| 317 | Error de procesamiento | ✓ |
| 336 | No se puede restaurar el objeto del Depósito de copias de seguridad | ✓ |
| 340 | El objeto está en la lista de admitidos de KSN Privada | ✓ |
| 301 | Objeto procesado | – |
| 306 | Objeto desinfectado | – |
| 307 | Objeto eliminado | – |
| 308 | Se creó una copia de seguridad del objeto | – |
| 310 | No se puede crear una copia de seguridad | – |
| 312 | No se puede desinfectar | – |
| 313 | No se puede eliminar | – |
| 314 | Objeto no procesado | – |
| 315 | Objeto omitido | – |
| 318 | Archivo de almacenamiento detectado | – |
| 319 | Objeto empaquetado detectado | – |
| 320 | Objeto cifrado | – |
| 321 | Objeto dañado | – |
| 322 | Archivo de almacenamiento protegido por contraseña detectado | – |
| 323 | El objeto se eliminará al reiniciar | – |
| 324 | El objeto se desinfectará al reiniciar | – |
| 325 | Sobrescrito con una copia desinfectada anteriormente | – |
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo o sus datos personales | – |
| 329 | Nombre del objeto cambiado | – |
| 335 | Objeto restaurado del Depósito de copias de seguridad | – |
| 452 | Proceso finalizado | – |
| 453 | No se puede finalizar el proceso | – |
| 332 | Información sobre el objeto detectado | – |

Protección contra amenazas web

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 301 | Objeto procesado | – |
| 302 | Se detectó un objeto malicioso | ✓ |
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo o sus datos personales | – |
| 317 | Error de procesamiento | ✓ |
| 318 | Archivo de almacenamiento detectado | – |
| 319 | Objeto empaquetado detectado | – |
| 321 | Objeto dañado | – |
| 322 | Archivo de almacenamiento protegido por contraseña detectado | – |
| 329 | Nombre del objeto cambiado | – |
| 362 | Vínculo peligroso bloqueado | ✓ |
| 1201 | Se detectó un vínculo peligroso que ya se había abierto | ✓ |
| 1211 | Se detectó un vínculo malintencionado que ya se había abierto | ✓ |
| 363 | Vínculo peligroso abierto | ✓ |
| 341 | Se bloqueó la descarga del objeto | – |
| 370 | El vínculo está en la lista de admitidos de KSN Privada | ✓ |
| 370 | El objeto está en la lista de admitidos de KSN Privada | ✓ |
| 332 | Información sobre el objeto detectado | – |

Protección contra amenazas de correo

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 301 | Objeto procesado | – |
| 306 | Objeto desinfectado | – |
| 302 | Se detectó un objeto malicioso | ✓ |
| 317 | Error de procesamiento | ✓ |
| 340 | El objeto está en la lista de admitidos de KSN Privada | ✓ |
| 307 | Objeto eliminado | – |
| 308 | Se creó una copia de seguridad del objeto | – |
| 312 | No se puede desinfectar | – |
| 314 | Objeto no procesado | – |
| 318 | Archivo de almacenamiento detectado | – |
| 319 | Objeto empaquetado detectado | – |
| 321 | Objeto dañado | – |
| 322 | Archivo de almacenamiento protegido por contraseña detectado | – |
| 329 | Nombre del objeto cambiado | – |
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo | – |
| 332 | Información sobre el objeto detectado | – |

## Firewall

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 601 | Actividad de red autorizada | – |
| 602 | Actividad de red bloqueada | – |

## Protección contra amenazas de red

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 651 | Ataque de red detectado | – |

## Prevención de ataques BadUSB

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 2050 | Teclado autorizado | – |
| 2051 | Teclado no autorizado | ✓ |
| 2052 | Error de autorización de teclado | ✓ |

## Protección vía AMSI

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 301 | Objeto procesado | – |
| 302 | Se detectó un objeto malicioso | ✓ |
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo o sus datos personales | – |
| 314 | Objeto no procesado | – |
| 315 | Objeto omitido | – |
| 317 | Error de procesamiento | ✓ |
| 318 | Archivo de almacenamiento detectado | – |
| 319 | Objeto empaquetado detectado | – |
| 320 | Objeto cifrado | – |
| 321 | Objeto dañado | – |
| 322 | Archivo de almacenamiento protegido por contraseña detectado | – |
| 1512 | El resultado del análisis del objeto se envió a una aplicación de otro desarrollador | – |
| 329 | Nombre del objeto cambiado | – |
| 332 | Información sobre el objeto detectado | – |
| 340 | El objeto está en la lista de admitidos de KSN Privada | ✓ |
| 2200 | La solicitud de AMSI se bloqueó | ✓ |

## Control de aplicaciones

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 701 | Inicio de aplicación autorizado | – |
| 702 | Inicio de aplicación prohibido | – |
| 703 | Inicio de aplicación prohibido en el modo de prueba | – |
| 704 | Inicio de aplicación autorizado en el modo de prueba | – |
| 707 | Error en la configuración de la tarea. No se aplicó la configuración de la tarea | – |
| 710 | Se inició un proceso prohibido antes del inicio de Kaspersky Endpoint Security para Windows | – |
| 708 | Configuración de tarea aplicada correctamente | – |

## Control de dispositivos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 801 | Operación con el dispositivo autorizada | – |
| 802 | Operación con el dispositivo prohibida | – |
| 803 | Acceso temporal al dispositivo activado | ✓ |
| 808 | Se realizó una operación en un archivo | – |
| 809 | Conexión de red bloqueada | – |

## Control Web

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 751 | Acceso autorizado | – |
| 752 | Acceso bloqueado | – |
| 753 | Advertencia acerca de contenido indeseado | – |
| 754 | Se accedió a contenido indeseado tras una advertencia | – |
| 751 | Se abrió una página permitida | – |

## Control de anomalías adaptativo

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 501 | Queja de actividad de la aplicación bloqueada | – |
| 2201 | Acción del proceso omitida | – |
| 2200 | Acción del proceso bloqueada | ✓ |

## Cifrado de datos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 904 | Error al implementar las reglas de cifrado o descifrado de archivos | ✓ |
| 912 | Error de cifrado o descifrado de archivos | ✓ |
| 1305 | Error de cifrado o descifrado del dispositivo | ✓ |
| 931 | Error al crear el paquete cifrado | ✓ |
| 951 | Error al habilitar el modo portátil | ✓ |
| 953 | Error al deshabilitar el modo portátil | ✓ |
| 1311 | No se pudo cargar el módulo de cifrado | ✓ |
| 1340 | La tarea de administración de cuentas del Agente de autenticación finalizó con un error | ✓ |
| 1312 | No se puede aplicar la directiva | ✓ |
| 1342 | No se pudo realizar la actualización de FDE | ✓ |
| 1343 | La reversión de la actualización de FDE se realizó correctamente | ✓ |
| 1345 | Error al instalar o actualizar los controladores de Cifrado de disco de Kaspersky en la imagen de WinRE | ✓ |
| 1346 | Error al eliminar los controladores de Cifrado de disco de Kaspersky de la imagen de WinRE | ✓ |
| 1370 | Se cambió la clave de recuperación de BitLocker | ✓ |
| 901 | Se inició la implementación de las reglas de cifrado o descifrado de archivos | – |
| 902 | Se completó la implementación de las reglas de cifrado o descifrado de archivos | – |
| 903 | Se interrumpió la implementación de las reglas de cifrado o descifrado de archivos | – |
| 905 | Se reanudó la implementación de las reglas de cifrado o descifrado de archivos | – |
| 910 | Cifrado o descifrado de archivos iniciado | – |
| 911 | Cifrado o descifrado de archivos completado | – |
| 913 | El archivo no se cifró porque es una exclusión | – |
| 914 | Cifrado o descifrado de archivos interrumpido | – |
| 1301 | Cifrado o descifrado del dispositivo iniciado | – |
| 1302 | Cifrado o descifrado del dispositivo completado | – |
| 1307 | Dispositivo sin cifrar | – |
| 1303 | Cifrado o descifrado del dispositivo interrumpido | – |
| 1304 | Cifrado o descifrado del dispositivo reanudado | – |
| 1309 | El proceso de cifrado o descifrado de la unidad se cambió al modo pasivo | – |

| | | |
|---|---|---|
| 1308 | El proceso de cifrado o descifrado de dispositivos se cambió al modo activo | – |
| 1306 | El usuario optó por no implementar la directiva de cifrado | – |
| 940 | Acceso al archivo bloqueado | ✓ |
| 950 | Modo portátil habilitado | – |
| 952 | Modo portátil deshabilitado | – |
| 1330 | Nueva cuenta del Agente de autenticación creada | – |
| 1337 | Cuenta no agregada. Esta cuenta ya existe | – |
| 1338 | Cuenta no modificada. Esta cuenta no existe | – |
| 1339 | Cuenta no eliminada. Esta cuenta no existe | – |
| 1331 | Cuenta del agente de autenticación eliminada | – |
| 1332 | Contraseña de la cuenta del Agente de autenticación cambiada | – |
| 1334 | Intento de inicio de sesión del Agente de autenticación fallido | – |
| 1333 | Inicio de sesión del Agente de autenticación correcto | – |
| 1335 | Se accedió al disco duro con el procedimiento de solicitud de acceso a dispositivos cifrados | – |
| 1336 | Intento fallido de acceder al disco duro con el procedimiento de solicitud de acceso a dispositivos cifrados | – |
| 1310 | Se cargó el módulo de cifrado | – |
| 1344 | La reversión de la actualización de Cifrado de disco completo se completó con un error | ✓ |
| 1341 | La actualización de FDE se realizó correctamente | ✓ |
| 1332 | Contraseña de la cuenta del Agente de autenticación cambiada | – |

Sensor de Endpoint

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 2100 | Servidor de Kaspersky Anti Targeted Attack Platform no disponible | – |
| 2105 | Se bloqueó el inicio de la aplicación | ✓ |
| 2106 | Se bloqueó la apertura del documento | ✓ |
| 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 Sensor de Endpoint se conectó al servidor | – |
| 2102 | Se recuperó la conexión con el servidor de Kaspersky Anti Targeted Attack Platform | – |
| 2112 | Se finalizaron todos los procesos iniciados desde una imagen de archivo o secuencia | ✓ |
| 2113 | Aplicación iniciada | ✓ |
| 2111 | El administrador del servidor de Kaspersky Anti Targeted Attack Platform eliminó el archivo o flujo | ✓ |
| 2110 | El administrador restauró el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform | ✓ |
| 2109 | El administrador colocó el archivo en la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform | ✓ |
| 2107 | La actividad de red de las aplicaciones de terceros se ha bloqueado | ✓ |
| 2108 | No se bloquea la actividad de red de las aplicaciones de terceros | ✓ |

Análisis del equipo

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 302 | Se detectó un objeto malicioso | ✓ |
| 335 | Objeto restaurado del Depósito de copias de seguridad | ✓ |
| 336 | No se puede restaurar el objeto del Depósito de copias de seguridad | ✓ |
| 340 | El objeto está en la lista de admitidos de KSN Privada | ✓ |
| 301 | Objeto procesado | – |
| 329 | Nombre del objeto cambiado | – |
| 306 | Objeto desinfectado | – |
| 307 | Objeto eliminado | – |
| 308 | Se creó una copia de seguridad del objeto | – |
| 310 | No se puede crear una copia de seguridad | – |
| 312 | No se puede desinfectar | – |
| 313 | No se puede eliminar | – |
| 314 | Objeto no procesado | – |
| 315 | Objeto omitido | – |
| 317 | Error de procesamiento | – |
| 318 | Archivo de almacenamiento detectado | – |
| 319 | Objeto empaquetado detectado | – |
| 320 | Objeto cifrado | – |
| 321 | Objeto dañado | – |
| 322 | Archivo de almacenamiento protegido por contraseña detectado | – |
| 323 | El objeto se eliminará al reiniciar | – |
| 324 | El objeto se desinfectará al reiniciar | – |
| 327 | Sobrescrito con una copia desinfectada anteriormente | – |
| 303 | Clases de software legítimo detectadas que los intrusos puedan usar para dañar el equipo o sus datos personales | – |

## Comprobación de integridad

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 2002 | Error al comprobar la firma del módulo del sistema | – |

## Actualización de bases de datos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 101 | Ocurrió un error interno | ✓ |
| 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 a causa de un error de actualización | – |
| 1008 | Actualizando archivos | – |
| 1009 | Distribuyendo actualizaciones | – |
| 1010 | Revertiendo archivos | – |
| 1011 | Error al actualizar un componente | – |
| 1012 | Error al distribuir las actualizaciones de componentes | – |
| 1013 | Creando la lista de archivos para descargar | – |
| 1014 | Error de actualización local | – |
| 1016 | Operación cancelada por el usuario | – |
| 1017 | No se pueden iniciar dos tareas al mismo tiempo | – |
| 1018 | Error al comprobar las bases de datos y los módulos de la aplicación | – |
| 1019 | Error de interacción con Kaspersky Security Center | – |
| 1020 | No hay actualizaciones disponibles | – |
| 1021 | No se actualizaron todos los componentes | – |
| 1022 | Distribución de actualizaciones completada correctamente | – |
| 1023 | Actualización terminada con éxito, error de distribución de actualizaciones | – |
| 2153 | No se pudo instalar el parche | – |
| 2156 | No se pudo revertir el parche | – |
| 2150 | Descargando parches | – |
| 2151 | Instalando parches | – |
| 2152 | Parche instalado | – |
| 2154 | Revirtiendo el parche | – |
| 2155 | Parche revertido | – |

## Eliminación de datos

Código de los eventos

| Id. del evento | Descripción | Habilitado de forma predeterminada |
|---|---|---|
| 223 | Tarea completada | – |
| 221 | Tarea iniciada | – |
| 222 | Tarea detenida | – |
| 2252 | El objeto no se puede eliminar | – |
| 2253 | Estadísticas de la tarea de eliminación | – |
| 2251 | Objeto eliminado | – |

# Información sobre código de terceros

La información sobre código de terceros se incluye en el archivo legal_notices.txt, que está almacenado en la carpeta de instalación de la aplicación.

# Avisos de marcas comerciales

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, iTunes y Safari son marcas comerciales de Apple Inc., registradas en los Estados Unidos y en otros países.

AutoCAD es una marca comercial o una marca registrada de Autodesk, Inc. y/o sus filiales y/o sus empresas vinculadas en los Estados Unidos y/o en otros países.

La palabra Bluetooth y la marca y los logotipos asociados son propiedad de Bluetooth SIG, Inc.

Borland es una marca comercial o una marca registrada de Borland Software Corporation.

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. Dichas marcas pueden estar registradas en la Oficina de Patentes y Marcas de los Estados Unidos y en otros países.

Dell es una marca comercial de Dell, Inc. o de sus filiales.

dBase es una marca comercial de dataBased Intelligence, Inc.

EMC es una marca comercial o marca comercial registrada de EMC Corporation en los Estados Unidos y en otros países.

Radmin es una marca registrada de Famatech.

IBM es una marca comercial de International Business Machines Corporation, registrada en muchas jurisdicciones del mundo.

ICQ es una marca registrada y/o una marca de servicio de ICQ LLC.

Intel es una marca comercial de Intel Corporation en los Estados Unidos y/o en otros países.

IOS es una marca comercial registrada de Cisco Systems, Inc. y/o sus filiales en los Estados Unidos y otros países.

Lenovo y ThinkPad son marcas comerciales de Lenovo en los Estados Unidos y/o en otros sitios.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca registrada o una marca comercial de Logitech en los Estados Unidos y/o en otros países.

LogMeIn Pro y Remotely Anywhere son marcas registradas de LogMeIn, Inc.

Mail.ru es una marca comercial registrada de Mail.Ru, LLC.

McAfee es una marca comercial o marca comercial registrada de McAfee, Inc. en los Estados Unidos y en 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 y 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 Corporation y/o de sus empresas vinculadas.

VERISIGN es una marca comercial registrada en los Estados Unidos y en otros países o una marca comercial no registrada de VeriSign, Inc. y sus subsidiarias.

VMware 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 marca comercial registrada de Symantec Corporation o de sus empresas vinculadas en los Estados Unidos y en otros países.

SAMSUNG es una marca comercial de SAMSUNG en los Estados Unidos y en otros países.