kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 para Windows

Contenido

Avisos de marcas comerciales

Acerca de Kaspersky Endpoint Security 10 Service Pack 2 para Windows

En esta sección, se describen las funciones, los componentes y el kit de distribución de Kaspersky Endpoint Security, y se proporciona una lista de los requisitos de hardware y software de Kaspersky Endpoint Security.

Novedades

Kaspersky Endpoint Security 10 Service Pack 2 para Windows ofrece las siguientes características y mejoras:

1. Control de Inicio de las Aplicaciones:
   - Admite sistemas operativos de servidor:
   - Controla las descargas de módulos DLL y controladores.
   - Administra la lista de objetos en la tarea de inventario (módulos DLL y archivos de script).
   - Controla objetos en función de un criterio nuevo: por atributos de certificados de firmas digitales.
   - Genera un informe sobre inicios de pruebas de aplicaciones bloqueadas.
   - Admite dos modos de funcionamiento para el Control de Inicio de las Aplicaciones: "Lista negra" y "Lista blanca".
   - Usa el hash SHA256 para controlar e inventariar objetos.
   - Controla la ejecución de scripts del intérprete de PowerShell.
   - Hace uso de almacenamiento de certificados de sistema de confianza.
2. La administración de Microsoft BitLocker habilita el cifrado de discos duros con la ayuda de la tecnología BitLocker de Microsoft:
   - Administra el cifrado en forma remota.
   - Supervisa los dispositivos cifrados.
   - Crea informes de cifrado de dispositivos.
   - Restaura el acceso a dispositivos cifrados.
3. Cifrado de disco de Kaspersky:
   - Admite el ingreso de credenciales en el entorno previo al inicio del Agente de autenticación usando un teclado virtual.
   - Admite el modo de cifrado para solo cifrar el espacio ocupado en un dispositivo.
   - Compatible con el cifrado en tabletas (MS Surface versión 3 y versión 4).
4. Control de Privilegios de Aplicaciones:
   - Controla el acceso de las aplicaciones a los dispositivos de grabación de audio y video.

5. Control Web:

   - Configura reglas de acceso del recurso web para categorías adicionales de recursos web.

6. Control de dispositivos:

   - Registra eventos asociados con la eliminación y el guardado de archivos en dispositivos USB.
   - Genera una lista de redes Wi-Fi de confianza según la siguiente configuración: nombre, tipo de cifrado y tipo de autenticación.
   - Administra derechos de acceso del usuario para operaciones de lectura y escritura en archivos en discos CD/DVD.

7. Antivirus de correo electrónico:

   - Capaz de suprimir y renombrar tipos específicos de archivos dentro de archivos de almacenamiento para el análisis del Antivirus de correo electrónico.

8. Kaspersky Security Network:

   - Muestra KSN como un motivo de una decisión respecto del método de procesamiento del objeto en los informes de Kaspersky Endpoint Security y de Kaspersky Security Center.
   - Envía una pregunta a KSN respecto de la reputación de un archivo seleccionado.
   - Muestra el estado de disponibilidad de los servidores de KSN para equipos cliente con Kaspersky Endpoint Security instalado.

Kit de distribución

El kit de distribución de Kaspersky Endpoint Security contiene los siguientes archivos:

- Los archivos necesarios para instalar la aplicación con cualquier de los métodos disponibles:
- Los archivos del paquete de actualización que se utilizan durante la instalación de la aplicación.
- El archivo klcfginst.exe para instalar el complemento de administración de Kaspersky Endpoint Security a través de Kaspersky Security Center.
- El archivo ksn_<identificador del idioma>.txt, en el que se pueden ver las condiciones de participación en Kaspersky Security Network.
- El archivo license.txt, con el cual se puede ver el Contrato de licencia de usuario final.
- El archivo incompatible.txt que contiene una lista de software incompatible.
- El archivo installer.ini que contiene la configuración interna del kit de distribución.

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

Debe descomprimir el kit de distribución para acceder a los archivos.

Acerca de 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.

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.

El funcionamiento de los componentes de control está basado en las siguientes reglas:

- El Control de aplicaciones utiliza Reglas de control de aplicaciones.
- En el Control de dispositivos se utilizan las reglas de acceso a dispositivos y las reglas de acceso a los buses de conexión.
- En el Control Web se utilizan las reglas de acceso a recursos web.
- Control de anomalías adaptativo utiliza lasreglas del Control de anomalías adaptativo.

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 Mis 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 maliciosas 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. El componente filtra toda la actividad de red según reglas de dos clases: reglas de red para aplicaciones y reglas de paquetes de red.

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

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

Además de la protección en tiempo real que proporcionan los componentes de la aplicación, le recomendamos que *analice* periódicamente el equipo en busca de 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 mantener la protección del equipo actualizada, debe *actualizar* los módulos y las bases de datos que utiliza 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.

Administración remota mediante Kaspersky Security Center

Kaspersky Security Center hace posible iniciar y detener de forma remota Kaspersky Endpoint Security en un equipo cliente, administrar tareas, configurar los ajustes de la aplicación y realizar el cifrado de archivos y el cifrado completo del disco.

La funcionalidad de Cifrado de archivos permite cifrar archivos y carpetas almacenados en los discos locales del equipo. La funcionalidad de cifrado de disco completo permite cifrar discos duros y unidades extraíbles.

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.

La aplicación utiliza algoritmos especiales, desarrollados por los expertos de Kaspersky, para recibir información sobre errores recurrentes que le impiden seguir en funcionamiento. Esta información es necesaria para la recuperación de aplicación.

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 el disco duro
- Procesador con una velocidad de reloj de 1 GHz (compatible con el conjunto de instrucciones SSE2)
- RAM:
  - 1 GB para sistemas operativos de 32 bits
  - 2 GB para sistemas operativos de 64 bits

Sistemas operativos admitidos para computadoras personales:

- 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 / Education / Enterprise

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 para servidores de archivos:

- Windows Small Business Server 2008 Standard / Premium (64 bits)
- Windows Small Business Server 2011 Essentials / Standard (64 bits)
- Windows MultiPoint Server 2011 (64 bits)
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 o versiones posteriores
- 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

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.

Instalación y eliminación de la aplicación

En esta sección, se indican los pasos para instalar Kaspersky Endpoint Security en el equipo, completar la configuración inicial, actualizar una versión anterior de la aplicación y eliminar la aplicación del equipo.

Instalación de la aplicación

Esta sección describe cómo instalar Kaspersky Endpoint Security en el equipo y cómo realizar la configuración inicial de la aplicación.

Acerca de las formas de instalar la aplicación

Kaspersky Endpoint Security 10 para Windows puede instalarse de forma local (directamente en el equipo del usuario) o de forma remota desde la estación de trabajo del administrador.

La instalación local de Kaspersky Endpoint Security 10 para Windows puede llevarse a cabo de alguna de las siguientes maneras:

- En modo interactivo usando el Asistente de instalación de la aplicación.

  El modo interactivo requiere su participación en el proceso de instalación.

- En modo silencioso desde la línea de comandos.

  Una vez iniciada la instalación en modo silencioso, no es necesaria su participación en el proceso de instalación.

La aplicación puede instalarse en forma remota en equipos de red de las siguientes maneras:

- Con el conjunto de software de Kaspersky Security Center (consulte la *Guía de implementación de Kaspersky Security Center*).

- Con el Editor de directivas de grupo de Microsoft Windows (consulte los archivos de ayuda del sistema operativo).

- Con System Center Configuration Manager.

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

Instalación de la aplicación mediante el Asistente de instalación

La interfaz del Asistente de instalación de la aplicación consiste en una secuencia de ventanas correspondiente a los pasos de instalación de la aplicación. Puede desplazarse entre las páginas del Asistente de instalación mediante los botones **Atrás** y **Siguiente**. Para cerrar el Asistente de instalación después de que completó su tarea, haga clic en el botón **Finalizar**. Para interrumpir el Asistente de instalación en cualquier momento, haga clic en el botón **Cancelar**.

Para instalar la aplicación o actualizar la aplicación desde una versión anterior mediante el Asistente de instalación:

1. Ejecute el archivo setup.exe, que se incluye en el kit de distribución.

   Se inicia el Asistente de instalación.

2. Siga las instrucciones del Asistente de instalación.

Cuando se inicia el archivo setup.exe, Kaspersky Endpoint Security comprueba el equipo para encontrar cualquier software incompatible. De forma predeterminada, al detectar software incompatible, el proceso de instalación se aborta y la lista de aplicaciones incompatibles con Kaspersky Endpoint Security aparece en la pantalla. Para continuar la instalación, elimine estas aplicaciones del equipo.

Paso 1. Comprobación de que el equipo cumple los requisitos de instalación

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

- Si el sistema operativo y el service pack cumplen con los requisitos de software para la instalación del producto.
- 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 11.1.1 para Windows, y la versión anterior de la aplicación se elimina automáticamente. Esto se aplica a las siguientes versiones de la aplicación:

- Kaspersky Endpoint Security 10 Service Pack 1 para Windows (versión 10.2.2.10535).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 para Windows (versión 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 para Windows (versión 10.2.5.3201)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 para Windows (versión 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 (versión 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 para Windows (versión 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 para Windows (compilación 10.3.3.275).
- Kaspersky Endpoint Security 11.0.0 para Windows (versión 11.0.0.6499)
- Kaspersky Endpoint Security para Windows 11.0.1 (versión 11.0.1.90).
- Kaspersky Endpoint Security para Windows 11.1.0 (versión 11.1.0.15919).

Paso 2. Página de bienvenida del procedimiento de instalación

Si se cumplen todos los requisitos de instalación de la aplicación, aparece una página de bienvenida después de iniciar el paquete de instalación. La página de bienvenida le notifica que se comenzará a instalar Kaspersky Endpoint Security en el equipo.

Para continuar con el Asistente de instalación, haga clic en el botón **Siguiente**.

Paso 3. Visualización del contrato de licencia y la directiva de privacidad

En este paso del Asistente de instalación, debe leer el Contrato de licencia de usuario final que se debe celebrar entre usted y Kaspersky, así como la Política de privacidad.

Lea detenidamente el Contrato de licencia de usuario final y la Política de privacidad. Si acepta todos los términos del Contrato de licencia de usuario final y la Política de privacidad, en la sección **Confirmo que he leído y comprendido la totalidad del texto, y que acepto lo siguiente**, seleccione las siguientes casillas de verificación:

- **los términos y las condiciones de este EULA**
- **la Política de privacidad que describe el manejo de los datos**

La Instalación de la aplicación en su dispositivo continuará después de que haya seleccionado ambas casillas.

Si no acepta el Contrato de licencia de usuario final y la Política de privacidad, detenga la instalación haciendo clic en el botón **Cancelar**.

Paso 4. Selección del tipo de instalación

En este paso, puede seleccionar el tipo más adecuado de instalación de Kaspersky Endpoint Security:

- **Instalación básica**. Si elige este tipo de la instalación, se instalan en el equipo todos los componentes de protección, excepto el componente Prevención de ataques BadUSB, con la configuración recomendada por expertos de Kaspersky.
- **Instalación estándar**. Si elige este tipo de la instalación, se instalan en el equipo todos los componentes de protección y control, excepto el componente Prevención de ataques BadUSB, con la configuración recomendada por expertos de Kaspersky.
- **Instalación personalizada**. Si selecciona este tipo de la instalación, el sistema le solicita que seleccione los componentes que se instalarán y que especifique la carpeta de destino para la aplicación.

  Este tipo de la instalación le permite instalar los componentes que no se incluyen en las instalaciones básica y estándar.

La instalación estándar está seleccionada de manera predeterminada.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para continuar con el Asistente de instalación, haga clic en el botón **Siguiente**. Para detener el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 5. Selección de los componentes de la aplicación a instalar

Este paso se realiza si selecciona la *Instalación personalizada* de la aplicación.

En este paso, puede seleccionar los componentes de Kaspersky Endpoint Security que desea instalar. El Antivirus de archivos es un componente obligatorio para la instalación. 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 unidades.
- Cifrado de archivos.
- Administrador de Microsoft BitLocker.
- KATA Sensor de punto final.

El *Administrador de Microsoft BitLocker* realiza las siguientes funciones:

- Administra el cifrado de BitLocker incorporado al sistema operativo Windows.
- Configura los parámetros de la directiva de cifrado y verifica su capacidad para ser aplicado al equipo administrado.
- Inicia procesos de cifrado y descifrado.
- Supervisa el estado del cifrado en el equipo administrado.
- Almacena claves de recuperación en forma centralizada en el Servidor de administración de Kaspersky Security Center.

KATA Sensor de punto final es un componente de la Plataforma antiataques dirigidos de Kaspersky. Esta solución está diseñada para detectar rápidamente amenazas como los ataques dirigidos. El componente supervisa continuamente procesos, conexiones de red activas y archivos que se modifican, y transmite esta información a la plataforma antiataques dirigidos de Kaspersky.

Para seleccionar un componente que quiera instalar, haga clic en el icono adyacente al nombre del componente para abrir el menú contextual y seleccione **Esta función se instalará en el disco duro local**. Para obtener más detalles acerca de las tareas que realiza el componente seleccionado y la cantidad de espacio en el disco que se necesita para instalarlo, consulte la parte inferior de la página actual del Asistente de instalación.

Para ver información detallada acerca del espacio disponible en los discos duros locales, haga clic en el botón **Volumen**. Esta información se muestra en la ventana **Espacio en disco disponible** que se abre.

Para cancelar la instalación del componente, seleccione la opción **Esta función no estará disponible** en el menú contextual.

Para volver a la lista de componentes instalados por defecto, haga clic en el botón **Restablecer**.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para continuar con el Asistente de instalación, haga clic en el botón **Siguiente**. Para detener el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 6. Selección de la carpeta de destino

Este paso está disponible si selecciona la *Instalación personalizada* de la aplicación.

En este paso, puede especificar la ruta de la carpeta de destino donde se instalará la aplicación. Para seleccionar la carpeta de destino para la aplicación, haga clic en el botón **Examinar**.

Para ver información acerca del espacio disponible en los discos duros locales, haga clic en el botón **Volumen**. Esta información se muestra en la ventana **Requisitos de espacio en disco** que se abre.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para continuar con el Asistente de instalación, haga clic en el botón **Siguiente**. Para detener el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 7. Adición de exclusiones de análisis

Este paso está disponible si selecciona la *Instalación personalizada* de la aplicación.

En este paso, puede especificar qué exclusiones del análisis desea agregar a la configuración de la aplicación.

Las casillas **Excluir áreas recomendadas por Microsoft del alcance del análisis** / **Excluir áreas recomendadas por Kaspersky del alcance del análisis** excluyen áreas recomendadas por Microsoft o Kaspersky de la zona de confianza, o bien, las incluyen.

Si una de estas casillas está seleccionada, Kaspersky Endpoint Security incluye, respectivamente, las áreas que Microsoft o Kaspersky recomiendan en la zona de confianza. Kaspersky Endpoint Security no analiza dichas áreas en busca de virus u otras amenazas.

La casilla **Excluir áreas recomendadas por Microsoft del alcance del análisis** está disponible si Kaspersky Endpoint Security se instala en un equipo que se ejecuta en Microsoft Windows para servidores de archivos.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para continuar con el Asistente de instalación, haga clic en el botón **Siguiente**. Para detener el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 8. Preparación para la instalación de la aplicación

Se recomienda proteger el proceso de instalación porque su equipo se puede infectar por programas maliciosos que podrían interferir con la instalación de Kaspersky Endpoint Security 10 para Windows.

La protección del proceso de instalación está habilitada por defecto.

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. Si es así, interrumpa la instalación y vuelva a iniciar el Asistente de instalación de la aplicación. En el paso "Preparación para la instalación de la aplicación", desactive la casilla **Proteger el proceso de instalación**.

La casilla **Garantizar la compatibilidad con Citrix PVS** activa/desactiva la función que instala controladores en el modo de compatibilidad con Citrix PVS.

Seleccione esta casilla solo si está trabajando con Citrix Provisioning Services.

La casilla **Agregar la ruta del archivo avp.com a la variable del sistema %PATH%** habilita o deshabilita la opción que agrega la ruta del archivo avp.com a la variable del sistema %PATH%.

Si se selecciona esta casilla, el inicio de Kaspersky Endpoint Security o de cualquiera de sus tareas desde la línea de comandos no requiere introducir la ruta del archivo ejecutable. Es suficiente ingresar el nombre del archivo ejecutable y el comando para iniciar la tarea en particular.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para instalar el programa, haga clic en el botón **Instalar**. Para detener el Asistente de instalación, haga clic en el botón **Cancelar**.

Es posible que se interrumpan las conexiones de red actuales mientras se instala la aplicación en el equipo. La mayor parte de las conexiones de red canceladas se restaura una vez finalizada la instalación de la aplicación.

Paso 9. Instalación de la aplicación

La instalación de la aplicación puede demorar unos minutos. Espere hasta que se complete.

Si está actualizando una versión anterior de la aplicación, este paso también incluye la migración de la configuración y la eliminación de la versión anterior de la aplicación.

Una vez finalizada la instalación de Kaspersky Endpoint Security, se inicia al Asistente de configuración inicial.

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`.

Para instalar la aplicación o actualizarla a una versión nueva:

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|0] [/pADDLOCAL=<componente>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/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|0] [ADDLOCAL=<componente>] [SKIPPRODUCTCHECK=1|0]
[SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<nombre de usuario> KLPASSWD=<contraseña>
KLPASSWDAREA=<alcance de la contraseña>] [ENABLETRACES=1|0 TRACESLEVEL=<nivel de
seguimiento>] /qn
```

`EULA`	Aceptar o rechazar los términos del Contrato de licencia de usuario final. Valores disponibles: • `1`: aceptar los términos del Contrato de licencia de usuario final. • `0`: rechazar los términos del Contrato de licencia de usuario final. El texto del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Es necesario aceptar los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar su versión.
`PRIVACYPOLICY`	Aceptar o rechazar la Política de privacidad. Valores disponibles: • `1`: aceptar la Política de privacidad. • `0`: rechazar la Política de privacidad. El texto de la Política de privacidad se incluye en el kit de distribución de Kaspersky Endpoint Security. Para instalar la aplicación o actualizar la versión de la aplicación, deberá aceptar la 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: • `1`: participar en KSN. • `0`: negarse a participar en KSN (valor predeterminado). El paquete de distribución de Kaspersky Endpoint Security está optimizado para ser utilizado con Kaspersky Security Network. Si opta por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que se haya completado la instalación.
`ALLOWREBOOT`	Permitir que el equipo se reinicie automáticamente, de ser necesario, cuando la aplicación termine de instalarse o actualizarse. Valores disponibles: • `1`: reiniciar el equipo automáticamente si es necesario. • `0`: no permitir que el equipo se reinicie automáticamente (valor predeterminado). 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.
`ADDLOCAL`	Seleccione componentes adicionales para la 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 y KATA Sensor de punto final. Valores disponibles: • `MSBitLockerFeature`. Se instala el componente Administrador de BitLocker. • `AntiAPTFeature`. Se instala el componente KATA Sensor de punto final.
`SKIPPRODUCTCHECK`	Búsqueda de software incompatible. La lista de software incompatible se encuentra en el archivo incompatible.txt, que forma parte del kit de distribución. Valores disponibles: • `1`: habilitar la búsqueda de software incompatible (valor predeterminado). • `0`: deshabilitar la búsqueda de software incompatible.
`SKIPPRODUCTUNINSTALL`	Eliminación automática del software incompatible detectado. Valores disponibles: • `1`: Kaspersky Endpoint Security intentará eliminar el software incompatible detectado (valor predeterminado). • `0`: el software incompatible no se eliminará de forma automática.
`KLLOGIN`	Permite definir el nombre de usuario con el que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (componente de Protección con contraseña). El nombre de usuario se configura a la par de los parámetros `KLPASSWD` y `KLPASSWDAREA`. El nombre de usuario predeterminado es KLAdmin.
`KLPASSWD`	Permite definir la contraseña con la que se accederá a las funciones y a las opciones de configuración de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros `KLLOGIN` y `KLPASSWDAREA`). Si especifica una contraseña, pero no un nombre de usuario con el parámetro `KLLOGIN`, se utilizará de 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: • `SET`: modificar la configuración de la aplicación. • `EXIT`: cerrar la aplicación. • `DISPROTECT`: deshabilitar los componentes de protección y detener las tareas de análisis. • `DISPOLICY`: deshabilitar la directiva de Kaspersky Security Center. • `UNINST`: eliminar la aplicación del equipo. • `DISCTRL`: deshabilitar los componentes de control. • `REMOVELIC`: eliminar la clave.

	• `REPORTS`: acceder a los informes.
`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. Valores disponibles: • `1`: La función de seguimiento de la aplicación está habilitada. • `0`: No realizar un seguimiento (valor predeterminado).
`TRACESLEVEL`	Nivel de detalle de los archivos de seguimiento. Valores disponibles: • `100` (crítico). Solo los mensajes de errores críticos. • `200` (alto). Mensajes sobre todos los errores, incluidos los graves. • `300` (diagnóstico). Mensajes sobre todos los errores y una selección de mensajes que contengan advertencias. • `400` (importante). Todos los mensajes y las advertencias sobre errores críticos y comunes, además de una selección de mensajes que contienen información adicional. • `500` (normal). Todos los mensajes y las advertencias sobre errores críticos y comunes, además de mensajes con información detallada sobre el funcionamiento de la aplicación en modo normal (valor predeterminado). • `600` (bajo). Todos los mensajes posibles.

Ejemplo:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

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

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

Cuando concluya la instalación, Kaspersky Endpoint Security activará la licencia de prueba a menos que se 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 activar una licencia comercial.

Al instalar la aplicación o actualizar su versión en modo silencioso, se admite el uso de los siguientes archivos:

- setup.ini: los ajustes de configuración general de la aplicación;
- Install.cfg:: configuración local de Kaspersky Endpoint Security;
- setup.reg: claves del Registro.

Para que las claves del archivo setup.reg se graben en el Registro, el parámetro `SetupReg` del archivo setup.ini debe tener el valor `setup.reg`. 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.

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.

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.

- `[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`	Aceptar o rechazar los términos del Contrato de licencia de usuario final. Valores disponibles: • `1`: aceptar los términos del Contrato de licencia de usuario final. • `0`: rechazar los términos del Contrato de licencia de usuario final. El texto del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Es necesario aceptar los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar su versión.
	`PrivacyPolicy`	Aceptar o rechazar la Política de privacidad. Valores disponibles: • `1`: aceptar la Política de privacidad. • `0`: rechazar la Política de privacidad. El texto de la Política de privacidad se incluye en el kit de distribución de Kaspersky Endpoint Security. Para instalar la aplicación o actualizar la versión de la aplicación, deberá aceptar la 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: • `1`: participar en KSN. • `0`: negarse a participar en KSN (valor predeterminado).

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

		• `0`: deshabilitar el mecanismo para proteger la instalación. Puede deshabilitar la protección de la instalación. La protección de la instalación incluye la protección contra el reemplazo del paquete de distribución con programas maliciosos, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso a la sección del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, 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. No es necesario reiniciar al instalar Kaspersky Endpoint Security. El reinicio es necesario solo si tiene que eliminar aplicaciones incompatibles antes de la instalación. El reinicio también puede ser necesario al actualizar la versión de la aplicación.
	`AddEnvironment`	Agregar a la variable del sistema %PATH% la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security. Valores disponibles: • `1`: la variable del sistema %PATH% se complementará con la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security. • `0`: la variable del sistema %PATH% no se complementará con la ruta de acceso a los archivos ejecutables incluidos en la carpeta de instalación de Kaspersky Endpoint Security.
	`AMPPL`	Habilitar o deshabilitar el uso de la tecnología AM-PPL (Anti-Malware Protected Process Light) para proteger el servicio de Kaspersky Endpoint Security. Valores disponibles: • `1`: el servicio de Kaspersky Endpoint Security se protegerá con la tecnología AM-PPL. • `0`: el servicio de Kaspersky Endpoint Security no se protegerá 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 de la

		instalación del programa. Los archivos de seguimiento de Kaspersky Endpoint Security se guardan en la carpeta %ProgramData%/Kaspersky Lab. Valores disponibles: • `1`: realizar un seguimiento de la instalación. • `0`: no realizar un seguimiento de la instalación (valor predeterminado).
	`TracesLevel`	Nivel de detalle de los archivos de seguimiento. Valores disponibles: • `100` (crítico). Solo mensajes sobre errores graves. • `200` (alto). Mensajes sobre todos los errores, incluidos los graves. • `300` (diagnóstico). Mensajes sobre todos los errores y una selección de mensajes que contengan advertencias. • `400` (importante). Todos los mensajes y las advertencias sobre errores críticos y comunes, además de una selección de mensajes que contienen información adicional. • `500` (normal). Todos los mensajes y las advertencias sobre errores críticos y comunes, además de mensajes con información detallada sobre el funcionamiento de la aplicación en modo normal (valor predeterminado). • `600` (bajo). Todos los mensajes posibles.
`[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.
	`MailAntiVirus`	Antivirus de correo electrónico.
	`IMAntiVirus`	Antivirus Ml.
	`WebAntiVirus`	Antivirus de Internet.
	`ApplicationPrivilegeControl`	Control de Privilegios de Aplicaciones.
	`SystemWatcher`	System Watcher.
	`Firewall`	Firewall.
	`NetworkAttackBlocker`	Bloqueador de ataques de red.
	`WebControl`	Control web.
	`DeviceControl`	Control de dispositivos.
	`ApplicationStartupControl`	Control de Inicio de las Aplicaciones.

	`FileEncryption`	Bibliotecas de cifrado de archivos.
	`DiskEncryption`	Bibliotecas de cifrado de disco completo.
	`VulnerabilityAssessment`	Monitor de vulnerabilidades.
	`KeyboardAuthorization`	Prevención de ataques BadUSB
	`AntiAPT`	KATA Sensor de Endpoint.
	`MSBitLocker`	Administrador de Microsoft BitLocker.
	`AdminKitConnector`	Conector del Agente de red para administrar la aplicación en forma remota mediante Kaspersky Security Center. Valores disponibles: • `1`: instalar el Conector del Agente de red. • `0`: no instalar el Conector del Agente de red.
`[Tasks]`	`ScanMyComputer`	Tarea de Análisis completo. Valores disponibles: • `1`: incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0`: no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.
	`ScanCritical`	Tarea de Análisis de áreas críticas. Valores disponibles: • `1`: incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0`: no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.
	`Updater`	Tarea de actualización. Valores disponibles: • `1`: incluir la tarea en la lista de tareas de Kaspersky Endpoint Security. • `0`: no incluir la tarea en la lista de tareas de Kaspersky Endpoint Security.

Asistente de configuración inicial

El Asistente de configuración inicial de Kaspersky Endpoint Security se inicia al final del procedimiento de instalación de la aplicación. El Asistente de configuración inicial le permite activar la aplicación y recopila información sobre las aplicaciones que están incluidas en el sistema operativo. Estas aplicaciones se agregan a la lista de aplicaciones de confianza cuyas acciones dentro del sistema operativo no están sujetas a restricciones.

La interfaz del Asistente de configuración inicial consta de una secuencia de páginas (pasos). Puede desplazarse por las páginas del Asistente de configuración inicial mediante los botones **Atrás** y **Siguiente**. Para completar el procedimiento del Asistente de configuración inicial, haga clic en el botón **Finalizar**. Para detener el procedimiento del Asistente de configuración inicial en cualquier etapa, haga clic en **Cancelar**.

Si el Asistente de configuración inicial se interrumpe por algún motivo, no se guardan las configuraciones ya especificadas. La próxima vez que intente usar la aplicación, el Asistente de configuración inicial comenzará de nuevo y tendrá que establecer la configuración desde el comienzo.

Activación de la aplicación

Se debe activar la aplicación en un equipo con la fecha y hora del sistema actual. Si la fecha y hora del sistema se modifican tras la activación de la aplicación, la clave se torna inoperativa. La aplicación cambia a un modo de operación sin actualizaciones y Kaspersky Security Network no está disponible. La clave se puede volver operativa nuevamente solo mediante la reinstalación del sistema operativo.

En este paso, seleccione una de las siguientes opciones de activación de Kaspersky Endpoint Security:

- **Activar mediante un código de activación**. Para activar la aplicación con un código de activación, seleccione esta opción e ingrese un código de activación.
- **Activar mediante un archivo de clave**. Seleccione esta opción para activar la aplicación con un archivo de clave.
- **Activar la versión de prueba**. Seleccione esta opción para activar la versión de prueba de la aplicación. El usuario podrá utilizar la versión totalmente funcional de la aplicación durante el plazo de vigencia de la licencia de la versión de prueba. Después de que venza la licencia, la funcionalidad de la aplicación se bloquea y no puede activar la versión de prueba nuevamente.
- **Activar más tarde**. Seleccione esta opción si desea omitir la etapa de activación de Kaspersky Endpoint Security. El usuario solo podrá usar los componentes Antivirus de archivos y Firewall. Después de la instalación, el usuario podrá actualizar las bases de datos antivirus y los módulos de Kaspersky Endpoint Security solo una vez. La opción **Activar más tarde** solo está disponible la primera vez que inicia el Asistente de configuración inicial, inmediatamente después de instalar la aplicación.

Necesita estar conectado a Internet para activar la versión de prueba de la aplicación o para activar la aplicación con un código de activación.

Para continuar con el Asistente de configuración inicial, seleccione una opción de activación y, luego, el botón **Siguiente**. Para detener el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Paso 2. Activación con un código de activación

Este paso solo está disponible cuando activa la aplicación con un código de activación. Cuando activa la versión de prueba de la aplicación o la activa con un archivo de clave, este paso se omite.

Durante este paso, Kaspersky Endpoint Security envía datos al servidor de activación para verificar el código de activación introducido.

- Si es correcta la verificación del código de activación, el Asistente de configuración inicial pasa automáticamente a la siguiente ventana.

- Si la verificación del código de activación es errónea, se muestra el mensaje correspondiente. En ese caso, debe solicitar asistencia al proveedor de software que le vendió la licencia de Kaspersky Endpoint Security.
- Si se excedió la cantidad de activaciones para el código de activación, se muestra la notificación correspondiente. El Asistente de configuración inicial se interrumpe, y la aplicación sugiere que se contacte al Servicio de soporte técnico de Kaspersky.

Para volver al paso anterior del Asistente de configuración inicial, haga clic en el botón **Atrás**. Para detener el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Activación con un archivo de clave

Este paso solo está disponible cuando activa la aplicación con un archivo de clave.

En este paso, especifique la ruta del archivo de clave. Para ello, haga clic en el botón **Examinar** y seleccione un archivo de clave con formato `<Id. de archivo>.key`.

Luego de seleccionar un archivo de clave, la siguiente información se muestra en la parte inferior de la ventana:

- Clave
- El tipo de licencia (comercial o de prueba) y la cantidad de equipos que cubre esta licencia
- Fecha de activación de la aplicación en el equipo
- Fecha de caducidad de la licencia
- Funcionalidad de la aplicación disponible de acuerdo con la licencia.
- Notificaciones sobre problemas con la clave en caso de que haya. Por ejemplo, *La lista negra de claves está dañada*

Para volver al paso anterior del Asistente de configuración inicial, haga clic en el botón **Atrás**. Para continuar con el Asistente de configuración inicial, haga clic en el botón **Siguiente**. Para detener el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Selección de las funciones que se activarán

Este paso solo está disponible cuando activa la versión de prueba de la aplicación.

En este paso, puede seleccionar la funcionalidad que se hará disponible después de la activación de la aplicación:

- **Instalación básica**. Si se selecciona esta opción, después de la activación de la aplicación, solo estarán disponibles los componentes de protección, el de Control de Privilegios de Aplicaciones y el del Monitor de vulnerabilidades.
- **Instalación estándar**. Si se selecciona esta opción, después de la activación, solo estarán disponibles los componentes de protección y control de la aplicación.

- **Instalación completa**. Si se selecciona esta opción, después de la activación de la aplicación, estarán disponibles todos los componentes de la aplicación instalados, incluida la funcionalidad de cifrado de datos.

Si seleccionó más componentes de los que permite la licencia adquirida durante la instalación, después de la activación de la aplicación se instalarán los componentes que no están disponibles según la licencia, pero no podrá usarlos. Si la licencia adquirida le permite utilizar más componentes que los instalados, una vez activada la aplicación se muestran en la sección **Licencia** los componentes que no han sido instalados.

La instalación estándar está seleccionada de manera predeterminada.

Para volver al paso anterior del Asistente de configuración inicial, haga clic en el botón **Atrás**. Para continuar con el Asistente de configuración inicial, haga clic en el botón **Siguiente**. Para detener el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Fin de la activación

En este paso, el Asistente de configuración inicial le informa que Kaspersky Endpoint Security se activó correctamente. Se proporciona la siguiente información sobre la licencia:

- El tipo de licencia (comercial o de prueba) y la cantidad de equipos que cubre esta licencia
- Fecha de caducidad de la licencia
- Funcionalidad de la aplicación disponible de acuerdo con la licencia.

Para continuar con el Asistente de configuración inicial, haga clic en el botón **Siguiente**. Para detener el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Análisis del sistema operativo

En este paso, se reúne información acerca de las aplicaciones incluidas en el sistema operativo. Estas aplicaciones se agregan a la lista de aplicaciones de confianza cuyas acciones dentro del sistema operativo no están sujetas a restricciones.

Las demás aplicaciones se analizan la primera vez que se inician después de la instalación de Kaspersky Endpoint Security.

Para detener el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Finalización de la configuración inicial de la aplicación

La ventana de finalización del Asistente de configuración inicial contiene información acerca de la finalización del proceso de instalación de Kaspersky Endpoint Security.

Si desea iniciar Kaspersky Endpoint Security, haga clic en el botón **Finalizar**.

Si desea salir del Asistente de configuración inicial sin iniciar Kaspersky Endpoint Security, desactive la casilla **Iniciar Kaspersky Endpoint Security 10 para Windows** y haga clic en **Finalizar**.

Declaración de Kaspersky Security Network

En este paso, se lo invita a participar en Kaspersky Security Network.

Revise la Declaración de Kaspersky Security Network:

- Si acepta todos sus términos, seleccione la opción **Acepto las condiciones de participación en Kaspersky Security Network** en la ventana del Asistente de Configuración Inicial.
- Si no acepta las condiciones de participación en Kaspersky Security Network, seleccione la opción **No acepto las condiciones de participación en Kaspersky Security Network** en la ventana del Asistente de Configuración Inicial.

Para proseguir con el Asistente de Configuración Inicial, haga clic en **Aceptar**.

Acerca de las formas de actualizar una versión anterior de la aplicación

Para actualizar una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, descifre todos los discos duros cifrados.

Puede actualizar las siguientes aplicaciones a Kaspersky Endpoint Security 10 Service Pack 2 para Windows:

- Kaspersky Anti-Virus 6.0 para Windows Workstations MP4 CF1 (compilación 6.0.4.1424) / MP4 CF2 (compilación 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 para Windows Servers MP4 (compilación 6.0.4.1424) / MP4 CF2 (compilación 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 para Windows (compilación 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 para Windows (compilación 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 para Windows (versión 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 para Windows (compilación 10.2.5.3201).

Cuando se actualice cualquiera de las aplicaciones enumeradas anteriormente a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, no se transferirán los contenidos de Cuarentena y Copia de seguridad.

Puede actualizar la versión anterior de la aplicación de las siguientes maneras:

- Localmente, en modo interactivo, usando el Asistente de instalación de la aplicación.
- En forma local y en modo no interactivo, desde la línea de comandos
- De forma remota, con el conjunto de software de Kaspersky Security Center (consulte la *Guía de implementación de Kaspersky Security Center*).

- De forma remota, a través del Editor de directivas de grupo de Microsoft Windows (consulte los archivos de ayuda del sistema operativo)

Cuando esté actualizando una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, no es necesario que elimine la versión anterior de la aplicación. Se recomienda salir de todas las aplicaciones activas antes de actualizar una versión anterior de la aplicación.

Eliminación de la aplicación

Esta sección describe cómo se puede quitar Kaspersky Endpoint Security del equipo.

Acerca de las formas de quitar 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 eliminar del equipo de varias maneras:

- En forma local y en modo interactivo, con el Asistente de instalación
- En forma local y en modo no interactivo, desde la línea de comandos
- De forma remota, con el conjunto de software de Kaspersky Security Center (consulte la *Guía de implementación de Kaspersky Security Center* para conocer los detalles)
- De forma remota, a través del Editor de directivas de grupo de Microsoft Windows (consulte los archivos de ayuda del sistema operativo)

Eliminación de la aplicación mediante el Asistente de instalación

Para eliminar Kaspersky Endpoint Security mediante el Asistente de instalación:

1. En el menú **Inicio**, seleccione **Aplicaciones → Kaspersky Endpoint Security 10 para Windows → Modificar, Reparar o Quitar**.

   Se inicia el Asistente de instalación.

2. En la ventana **Modificar, Reparar o Quitar aplicación** del Asistente de instalación, haga clic en el botón **Quitar**.

3. Siga las instrucciones del Asistente de instalación.

Paso 1. Almacenamiento de datos de la aplicación para futuros usos.

Durante este paso, puede especificar cuáles de los datos que utiliza la aplicación quiere mantener para seguir usándolos durante la siguiente instalación de la aplicación (por ejemplo: al instalar una versión más reciente). Si no especifica ningún dato, la aplicación se elimina completamente.

Para guardar datos de la aplicación para futuros usos,

seleccione las casillas adyacentes a los tipos de datos que quiera guardar:

- **Datos de activación**: datos que eliminan la necesidad de activar la aplicación que se instale en el futuro. Se activa automáticamente con la licencia actual, siempre y cuando esta no haya caducado al momento de la instalación.
- Los **archivos de Copias de seguridad** son archivos analizados por la aplicación y puestos en la Copia 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, debe restaurar dichos objetos de su almacenamiento antes de eliminar la aplicación. 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**: valores de configuración de la aplicación seleccionados durante la configuración.
- **Almacenamiento local de las claves de cifrado**: datos que proporcionan acceso directo a archivos y dispositivos que se cifraron antes de eliminar la aplicación. Se puede acceder a archivos y unidades cifrados directamente después de la reinstalación de la aplicación con la funcionalidad de cifrado.

  Esta casilla está seleccionada por defecto.

Para continuar con el Asistente de instalación, haga clic en el botón **Siguiente**. Para detener el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 2. Confirmación de la eliminación de la aplicación.

Debido a que la eliminación de la aplicación pone en peligro la seguridad del equipo, se le solicita que confirme que desea eliminar la aplicación. Para ello, haga clic en el botón **Eliminar**.

Para detener la eliminación de la aplicación en cualquier momento, puede cancelar la operación haciendo clic en el botón **Cancelar**.

Paso 3. Eliminación de la aplicación. Fin de la eliminación

En este paso, el Asistente de instalación elimina la aplicación del equipo. Espere a que se complete la eliminación de la aplicación.

Cuando elimine la aplicación, es posible que sea necesario reiniciar el equipo. Si decide no reiniciar el equipo inmediatamente, el fin del procedimiento de la eliminación de la aplicación se pospone hasta que se reinicie el sistema operativo o hasta que el equipo se apague y se vuelva a encender.

Eliminación de la aplicación desde la línea de comandos

Puede iniciar el proceso de desinstalación de la aplicación desde la línea del comandos. La desinstalación se lleva a cabo en modo interactivo o silencioso (sin iniciar el Asistente de instalación de la aplicación).

Para iniciar el proceso de desinstalación de la aplicación en modo interactivo,

en la línea de comandos, escriba `setup.exe /x` o `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

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

Para iniciar el proceso de desinstalación de la aplicación en modo silencioso,

en la línea de comandos, escriba `setup.exe /s /x` o `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

De esta manera se inicia el proceso de la desinstalación de la aplicación en modo silencioso (sin iniciar el Asistente de instalación).

Si la operación de desinstalación de la aplicación está protegida con contraseña, se debe ingresar tanto el nombre de usuario como la contraseña correspondiente en la línea de comandos.

Para eliminar la aplicación desde la línea de comandos en modo interactivo cuando se definen el nombre de usuario y la contraseña para la autenticación de la eliminación, modificación o reparación de Kaspersky Endpoint Security:

En la línea de comandos, escriba `setup.exe /pKLLOGIN=<Nombre de usuario> /pKLPASSWD=***** /x` o

`msiexec.exe KLLOGIN=<Nombre de usuario> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}.`

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

Para eliminar la aplicación desde la línea de comandos en modo silencioso cuando se definen el nombre de usuario y la contraseña para la autenticación de la eliminación, modificación o reparación de Kaspersky Endpoint Security:

En la línea de comandos, escriba `setup.exe /pKLLOGIN=<Nombre de usuario> /pKLPASSWD=***** /s /x` o

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Nombre de usuario> KLPASSWD=***** /qn.`

Eliminación de objetos y datos restantes después de la operación de prueba 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 dos maneras:

- Con la directiva de Kaspersky Security Center.
- Con la Utilidad de Restauración.

Para usar una directiva de Kaspersky Security Center para eliminar objetos y datos restantes después de la operación de prueba del Agente de autenticación:

1. Aplique al equipo una directiva de Kaspersky Security Center con parámetros configurados para descifrar todos los discos duros del equipo.
2. Inicie Kaspersky Endpoint Security.

Para usar la Utilidad de Restauración para eliminar objetos y datos restantes después de la operación de prueba del Agente de autenticación:

1. Inicie la Utilidad de restauración; para ello, ejecute el archivo ejecutable fdert.exe que se creó con Kaspersky Endpoint Security en el equipo con el disco duro del sistema conectado en el cual quedan objetos y datos después de la operación de prueba del Agente de autenticación.
2. En la lista desplegable **Seleccionar dispositivo** de la ventana de la Utilidad de Restauración, seleccione el disco duro del sistema con los objetos y datos para eliminar.
3. Haga clic en el botón **Analizar**.
4. Haga clic en el botón **Eliminar objetos y datos de AA**.

   De esta forma se inicia el proceso de quitar objetos y datos restantes después de la operación de prueba del Agente de autenticación.

Después de quitar los objetos y datos restantes luego de la operación de prueba del Agente de autenticación, es posible que también sea necesario quitar información sobre la incompatibilidad de aplicaciones con el Agente de autenticación.

Para quitar información sobre incompatibilidad de aplicaciones con el Agente de autenticación,

escriba el comando `avp pbatestreset` en la línea de comandos.

Los componentes de cifrado deben estar instalados para poder ejecutar el comando `avp pbatestreset`.

Interfaz de la aplicación

En esta sección, se describen los elementos principales de la interfaz de la aplicación.

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.

Indicación de la actividad de la aplicación

El icono de la aplicación sirve como indicador de la actividad de la aplicación:

- El icono protection enabled significa que están habilitados todos los componentes de protección de la aplicación.
- El icono reinicio necesario significa que ocurrieron eventos importantes durante el funcionamiento de Kaspersky Endpoint Security a los que debería prestarse atención. Por ejemplo, el componente Protección contra amenazas de archivos está deshabilitado y las bases de datos de la aplicación están desactualizadas.
- El icono error occurred significa que ocurrieron eventos críticos durante el funcionamiento de Kaspersky Endpoint Security. Por ejemplo: un error en el funcionamiento de un componente, o daños de las bases de datos de la aplicación.

Menú contextual del icono de la aplicación

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

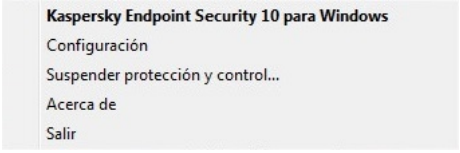
- **Kaspersky Endpoint Security para Windows**. Se abre la ventana principal de la aplicación. En esta ventana, puede ajustar el funcionamiento de las tareas y los componentes de la aplicación, además de mostrar las estadísticas de los archivos procesados y las amenazas detectadas.
- **Configuración**. Se abre la ventana **Configuración**. La ficha **Configuración** permite cambiar la configuración predeterminada de la aplicación.
- **Suspender protección y control**/**Reanudar protección y control**. Suspende o reanuda temporalmente el funcionamiento de los componentes de protección y control. Este elemento del menú contextual no afecta a la tareas de actualización ni de análisis, y solo está disponible cuando se deshabilita la directiva de Kaspersky Security Center.

  Kaspersky Endpoint Security utiliza Kaspersky Security Network independientemente de si se ha pausado o reiniciado la operación de los componentes de protección y control.

- **Deshabilitar directiva** / **Habilitar directiva**. Desactiva o activa la directiva de Kaspersky Security Center. Este elemento del menú contextual está disponible si se ha aplicado una directiva a un equipo en la que esté instalado Kaspersky Endpoint Security y se ha establecido una contraseña para deshabilitar la directiva de Kaspersky Security Center.

- **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

Para abrir el menú contextual del icono de la aplicación, apoye el puntero sobre el icono de la aplicación en el área de notificación de la barra de tareas de Microsoft Windows y haga clic con el botón derecho del mouse.

Ventana principal de la aplicación

La ventana principal de Kaspersky Endpoint Security incluye los elementos de la interfaz que brindan acceso a las funciones principales de la aplicación.

La ventana principal de la aplicación contiene los elementos siguientes:

- Vínculo a **Kaspersky Endpoint Security para Windows**. Si se hace clic en este vínculo, se abre la ventana **Acerca de**, que contiene información sobre la versión de la aplicación.

- Botón Icono de ayuda. Al hacer clic en este botón, se lo llevará al sistema de ayuda de Kaspersky Endpoint Security.

- Ventana **Tecnologías de detección de amenazas**. Esta sección contiene la siguiente información:

  - La parte izquierda de la sección muestra una lista de tecnologías de detección de amenazas. El número de amenazas que se detectaron usando la tecnología específica aparece a la derecha del nombre de cada tecnología de detección de amenazas.

  - Según la presencia de amenazas activas, el centro de la sección muestra una de las leyendas siguientes:

    - **No hay amenazas**. Si se muestra esta leyenda, al hacer clic en la sección **Tecnologías de detección de amenazas**, se abre la ventana **Tecnologías de detección de amenazas**, que contiene breves descripciones de las tecnologías de detección de amenazas, así como el estado y las estadísticas globales de la infraestructura del servicio en la nube de Kaspersky Security Network.

    - **N amenazas activas**. Si se muestra esta leyenda, al hacer clic en la sección **Tecnologías de detección de amenazas**, se abre la ventana **Amenazas activas**, que muestra una lista de los eventos asociados con archivos infectados que no se procesaron por algún motivo.

- Sección **Componentes de protección**. Al hacer clic en esta sección, se abre la ventana **Componentes de protección**. En esta ventana, puede ver el estado de funcionamiento de los componentes instalados. Desde esta ventana, también puede abrir una subsección en la ventana **Configuración** que contiene la configuración de cualquier componente instalado, excepto los componentes del cifrado.

- Sección **Tareas**. Al hacer clic en esta sección, se abre la ventana **Tareas**. En esta ventana, puede administrar el funcionamiento de las tareas de Kaspersky Endpoint Security que se utilizan para actualizar módulos y bases de datos de la aplicación, analizar archivos en busca de virus y otro malware, y ejecutar una comprobación de integridad.

- Botón **Informes**. Al hacer clic en este botón, se abre la ventana **Informes**, que contiene información sobre los eventos que tuvieron lugar durante el funcionamiento de la aplicación en general o de alguno de sus componentes en particular, o bien durante la realización de las tareas.

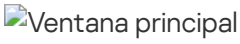
- Botón **Repositorios**. Al hacer clic en este botón, se abre la ventana **Copias de seguridad**. En esta ventana, puede ver una lista de las copias de los archivos infectados eliminados por la aplicación.

- Botón **Soporte**. Al hacer clic en este botón, se abre la ventana **Soporte**, que contiene información sobre el sistema operativo, la versión actual de Kaspersky Endpoint Security y vínculos a recursos de información de Kaspersky.

- Botón **Configuración**. Al hacer clic en este botón, se abre la ventana **Configuración**, en la cual puede modificar la configuración predeterminada de la aplicación.

- Botón / / . Al hacer clic en este botón abre la ventana **Eventos**, que contiene información sobre las actualizaciones disponibles, así como solicitudes de acceso a archivos y equipos cifrados.

- Vínculo **Licencia**. Si se hace clic en este vínculo, se abre la ventana **Licencia**, que contiene información sobre la licencia actual.


Ventana principal

Ventana principal de la aplicación

Puede abrir la ventana principal de Kaspersky Endpoint Security de las siguientes maneras:

- Haga clic en el icono de la aplicación en el área de notificación de la barra de tareas de Microsoft Windows.

- Seleccione **Kaspersky Endpoint Security para Windows** en el menú contextual del icono de la aplicación.

Ventana Configuración de la aplicación

La ventana de configuración de Kaspersky Endpoint Security le permite configurar los parámetros generales de la aplicación, los componentes individuales, los informes y depósitos, las tareas de análisis, las tareas de actualización y la comunicación con los servidores de Kaspersky Security Network.

La ventana está dividida en dos partes (vea la siguiente imagen):

- La parte izquierda contiene los componentes de la aplicación, las tareas y una sección de configuración avanzada compuesta por varias subsecciones.

- La parte derecha contiene los elementos de control que puede usar para configurar los parámetros del componente o de la tarea que se seleccionó en la parte izquierda de la ventana, además de opciones de configuración avanzadas.


Configuración

Ventana Configuración de la aplicación

Para abrir la ventana de configuración de la aplicación, realice una de las siguientes acciones:

- En la ventana principal de la aplicación, seleccione la ficha **Configuración**.
- En el menú contextual del icono de la aplicación, seleccione **Configuración**.

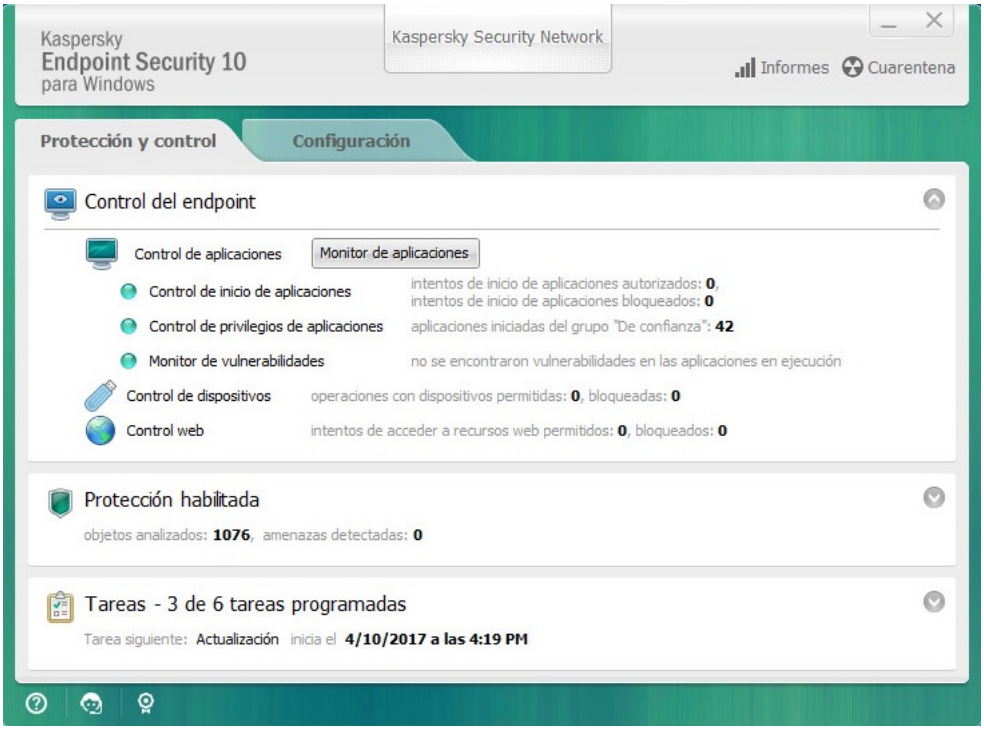
Ficha Protección y control de la aplicación

La ficha Protección y control de Kaspersky Endpoint Security está diseñada para proporcionar información general sobre la ejecución de todas las tareas y el funcionamiento de todos los componentes de la aplicación. En esta ficha, también puede regular el funcionamiento de los componentes y la ejecución de las tareas.

La ficha Protección y control de la aplicación está compuesta por tres partes (ver a la figura a continuación):

- La sección **Control del endpoint** contiene una lista de componentes de control.
- La sección **Administrar protección** contiene una lista de componentes de la protección antivirus.
- La sección **Tareas** contiene una lista de tareas locales que se ejecutan en el equipo.

Cada sección contiene elementos de control que puede usar para activar o desactivar el funcionamiento de un componente, dirigirse a la configuración correspondiente al componente o la tarea seleccionado, y ver estadísticas de funcionamiento correspondientes al componente o a la tarea seleccionado.



Ficha Protección y control de la aplicación

Para abrir la ficha Protección y control de la aplicación, realice una de las siguientes acciones:

- En la ventana principal de la aplicación, seleccione la ficha **Protección y control**.
- Haga clic en el icono de la aplicación en el área de notificación de la barra de tareas de Microsoft Windows.
- Seleccione **Kaspersky Endpoint Security 10 para Windows** en el menú contextual del icono de la aplicación.

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:

- Al instalar Kaspersky Endpoint Security en modo interactivo.
- Cuando se lee el archivo license.txt. Este documento se incluye en el kit de distribución de la aplicación.

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:

- Número de pedido
- Detalles del usuario al que se otorgó la licencia
- Detalles de la aplicación que se puede activar usando la licencia
- La limitación del número de unidades con licencia (por ejemplo, el número de dispositivos en los cuales se puede usar la aplicación con la licencia)
- Fecha de inicio del plazo de licencia
- Fecha de caducidad de la licencia o plazo de licencia
- Tipo de licencia

Acerca de la suscripción

La suscripción para Kaspersky Endpoint Security es una orden de compra para la aplicación con parámetros específicos (fecha de caducidad de la suscripción, 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. Puede administrar su suscripción en el sitio web del proveedor de servicios.

La suscripción puede ser limitada (por un año, por ejemplo) o ilimitada (sin fecha de caducidad). Para mantener Kaspersky Endpoint Security activo tras la caducidad del período de suscripción limitada, debe renovar la suscripción. La suscripción ilimitada se renueva en forma automática si los servicios del proveedor se han pagados por adelantado a tiempo.

En el caso de una suscripción limitada, una vez que caduca la suscripción se le puede ofrecer un período de gracia para la renovación de la suscripción, durante el cual la aplicación mantiene su funcionalidad. El proveedor de servicios decide si otorga el período de gracia y, de hacerlo, determina la duración de dicho período.

Para utilizar Kaspersky Endpoint Security con suscripción, debe aplicar el código de activación que recibió por parte del proveedor de servicios. Una vez que se aplica el código de activación, se instala la clave activa. La clave activa define la licencia para la utilización de la aplicación con suscripción. Se puede instalar una clave adicional solamente utilizando un código de activación y no se puede instalar utilizando un archivo de clave o bajo suscripción.

La funcionalidad de la aplicación disponible con suscripción puede corresponder a la funcionalidad de la aplicación para los siguientes tipos de licencias comerciales: estándar, Kaspersky Business Space Security y Kaspersky Enterprise Space Security. Las licencias de estos tipos están diseñadas para proteger los servidores de archivos, las estaciones de trabajo y los dispositivos móviles, y admite el uso de componentes de control en estaciones de trabajo y dispositivos móviles.

Las opciones de administración de suscripción posibles pueden variar con cada proveedor de servicios. El proveedor de servicios puede no ofrecer un período de gracia para la renovación de la suscripción, durante el que la aplicación mantendrá su funcionalidad.

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

Acerca del código de activación

Un *código de activación* es una secuencia alfanumérica única de veinte números y letras latinas que usted recibe al adquirir una licencia comercial de 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.

Cuando se activa la aplicación utilizando un código de activación, se instala la clave activa. Se puede instalar una clave adicional solamente utilizando un código de activación y no se puede instalar utilizando un archivo de clave o bajo suscripción.

Si perdió un código de activación después activar la aplicación, puede restaurarlo. Puede necesitar un código de activación, por ejemplo, para registrar una cuenta Kaspersky CompanyAccount. Para restaurar un código de activación, se debe poner en contacto con el Servicio de soporte técnico de Kaspersky.

Acerca de la clave

Una *clave* es una secuencia alfanumérica única. Una clave le permite usar la aplicación de acuerdo con los términos indicados en el Certificado (tipo de licencia, período de validez de la licencia, restricciones de la licencia).

No se provee un certificado de licencia para una clave instalada por suscripción.

Se puede agregar una clave a la aplicación utilizando un código de activación o un archivo de clave.

Puede agregar, editar o eliminar claves. Kaspersky puede bloquear la clave si se infringe el Contrato de licencia de usuario final. Si la clave se ha incluido en la lista negra, es necesario agregar una clave diferente para continuar utilizando la aplicación.

Si se ha eliminado una clave correspondiente a una licencia caducada, la funcionalidad de la aplicación no estará disponible. No puede agregar una clave igual después de que se ha eliminado.

Hay dos tipos de claves: activa y adicional.

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 adicional* es una clave que le permite al usuario usar la aplicación, pero que no está en uso en estos momentos. Cuando la clave activa caduque, la clave adicional se activará automáticamente. Se puede agregar una clave adicional solamente si la clave activa está disponible.

Solo se puede agregar una clave para una licencia de prueba como una clave activa. No se puede agregar como clave adicional. Una clave de licencia de prueba no puede reemplazar a la clave activa de una licencia comercial.

Si una clave queda en una lista negra, la funcionalidad de la aplicación definida por la licencia con la que se activó la aplicación continúa disponible durante ocho días. Kaspersky Security Network y las actualizaciones de módulos de aplicación y bases de datos están disponibles sin restricciones. La aplicación le notifica al usuario que la clave se ha ingresado en la lista negra. Luego de ocho días, la funcionalidad de la aplicación se vuelve limitada al nivel de funcionalidad que está disponible una vez que caduca la licencia: la aplicación se ejecuta sin actualizaciones y Kaspersky Security Network no está disponible.

Acerca del archivo de clave

Un *archivo de clave* es el archivo de extensión .key que usted recibe de parte de Kaspersky después de adquirir Kaspersky Endpoint Security. El propósito del archivo de clave es añadir una clave que active la aplicación.

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.

Sobre la provisión de datos

Si se aplica un código de activación para activar Kaspersky Endpoint Security, acepta transmitir periódicamente la siguiente información de modo automático con el objetivo de verificar el uso correcto de la aplicación:

- Tipo, versión y localización de Kaspersky Endpoint Security
- Versiones de actualizaciones instaladas para Kaspersky Endpoint Security
- ID del equipo e ID de la instalación de Kaspersky Endpoint Security específica en el equipo
- El número de serie del certificado y el identificador de la clave activa

- Tipo, versión y velocidad binaria del sistema operativo y nombre del entorno virtual (si Kaspersky Endpoint Security está instalado en un entorno virtual)
- ID de los componentes de Kaspersky Endpoint Security que están activos cuando se transmite la información

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

Al utilizar un código de activación, acepta transmitir automáticamente los datos enumerados anteriormente. Si no acepta transmitir esta información a Kaspersky, debería usar 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 exclusivo del inicio de la tarea de la actualización
  - ID exclusivo de la instalación de Kaspersky Endpoint Security
- Al utilizar enlaces desde la interfaz de Kaspersky Endpoint Security:
  - Versión de Kaspersky Endpoint Security
  - Versión del sistema operativo
  - Fecha de activación de Kaspersky Endpoint Security
  - Fecha de caducidad de la licencia
  - Fecha de creación de la clave
  - Fecha de instalación de Kaspersky Endpoint Security
  - ID de Kaspersky Endpoint Security
  - ID de la vulnerabilidad detectada en el sistema operativo
  - ID de la última actualización instalada de Kaspersky Endpoint Security
  - Hash del archivo detectado como amenaza y el nombre de esta amenaza según la clasificación de Kaspersky
  - Categoría del error de activación de Kaspersky Endpoint Security
  - Código del error de activación de Kaspersky Endpoint Security
  - Número de días hasta el vencimiento de la clave

- Número de días transcurridos desde que se agregó la clave
- Número de días transcurridos desde que caducó la licencia
- Número de equipos en los cuales se ha aplicado la licencia activa
- Clave activa
- Plazo de la licencia de Kaspersky Endpoint Security
- Estado actual de la licencia
- Tipo de licencia activa
- Tipo de aplicación
- ID exclusivo del inicio de la tarea de la actualización
- ID exclusivo de la instalación de Kaspersky Endpoint Security
- ID exclusivo de instalación del software 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.

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.

Visualización de la información de la licencia

Para ver información sobre la licencia:

Haga clic en main_license / license_expired 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).


KES11_License_info

Ventana Licencia

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

- **Estado de la clave**. Puede almacenar más de una clave en el equipo. Hay dos tipos de claves: activa y adicional. La aplicación no puede tener más de una clave activa. La clave adicional puede activarse solo si la clave activa ha caducado o si se la elimina con el botón component_malfunction.
- **Clave**. Una *clave* es una secuencia alfanumérica irrepetible que se genera a partir de un código de activación o de un archivo de clave.

- **Tipo de licencia**. Los siguientes tipos de licencias están disponibles: de prueba y comercial.
- **Nombre de la aplicación**. Nombre completo del producto de Kaspersky adquirido.
- **Características**. Funciones de la aplicación que la licencia permite utilizar. Entre las funciones se encuentran Protección, Controles de seguridad, Cifrado de datos y Sensor de Endpoint. La lista de funciones disponibles también puede consultarse 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. El Asistente de activación de la aplicación le permitirá agregar una clave activa y un máximo de una clave adicional.

Adquisición de una licencia

Puede comprar una licencia después de instalar la aplicación. Cuando adquiere una licencia, recibe 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 main_license / license_expired.

   Se abre la ventana **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 licencia

Cuando se acerca la fecha de vencimiento de la licencia, puede renovarla. Esto garantiza que el equipo permanecerá protegido después de que venza la licencia actual y hasta que active la aplicación con una nueva licencia.

Para renovar una licencia:

1. Reciba un código de activación de la aplicación o archivo de clave nuevo.
2. Agregue una clave adicional con el código de activación o el archivo de clave que ha recibido.

Se agrega una clave adicional como resultado. Se activa cuando caduca la licencia.

La actualización de la clave de adicional a activa puede llevar algún tiempo, debido a la distribución de la carga a través de los servidores de activación de Kaspersky.

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 para 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.

Puede renovar la suscripción en el sitio web del 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 que ha caducado el período de gracia y la aplicación no ha actualizado el estado de la suscripción en forma automática.

Visitar el sitio web del proveedor de servicios

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

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

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

Acerca de los métodos de 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. El proceso de activación de la aplicación implica agregar una clave.

Puede activar la aplicación de las siguientes maneras:

- Al instalar la aplicación usando el asistente de configuración Inicial. Puede agregar la clave activa de esta forma.
- En forma local desde la interfaz de aplicación, utilizando el Asistente de activación. Puede agregar tanto la clave activa como la adicional de esta manera.
- En forma remota con el conjunto de software de Kaspersky Security Center al crear y luego iniciar una tarea para agregar una clave. Puede agregar la clave activa y la clave adicional de esta forma.
- De forma remota mediante la distribución de claves y códigos de activación almacenados en el almacenamiento de claves del Servidor de administración de Kaspersky Security Center a equipos de clientes (consulte la ayuda de Kaspersky Security Center para obtener más información al respecto). Puede agregar la clave activa y la clave adicional de esta forma.

  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.

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 main_license / license_expired que se encuentra en la parte inferior de la ventana principal de la aplicación.

   Se abre la ventana **Licencia**.

2. En la ventana **Licencia**, haga clic en el botón **Activar la aplicación con una licencia nueva**.

   Se inicia el Asistente de activación de la aplicación.

3. Siga las instrucciones del Asistente de activación.

Para obtener más información sobre el procedimiento de activación de la aplicación, consulte la sección sobre el Asistente de configuración inicial.

Activación de la aplicación desde la línea de comandos

Para activar la aplicación desde la línea de comandos,

escriba `avp.com license /add <código de activación o archivo de clave> /password= <contraseña>` en la línea de comandos.

Inicio y detención de la aplicación

Esta sección describe cómo configurar el inicio automático de la aplicación, cómo iniciar o detener la aplicación de forma manual y cómo suspender o reanudar los componentes de protección y control.

Habilitación y deshabilitación del inicio automático de la aplicación

El inicio automático permite que Kaspersky Endpoint Security se inicie inmediatamente después de que arranque el sistema operativo, sin necesidad de que el usuario intervenga. Esta opción de inicio de la aplicación está habilitada por defecto.

Después de la instalación, Kaspersky Endpoint Security se inicia automáticamente por primera vez. Luego, la aplicación se inicia automáticamente después de que arranca el sistema operativo.

Descargar las bases de datos antivirus de Kaspersky Endpoint Security después de que se inicia el sistema operativo puede demorar dos minutos según las capacidades del equipo. Durante este tiempo, el nivel de protección del equipo se reduce. Descargar bases de datos antivirus cuando se inicia Kaspersky Endpoint Security en un sistema operativo ya cargado no causa ninguna reducción en el nivel de protección del equipo.

Para habilitar o deshabilitar el inicio automático de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. Seleccione la sección **Protección antivirus** de la izquierda.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:

   - Si quiere activar la ejecución automática de la aplicación, seleccione la casilla **Iniciar Kaspersky Endpoint Security 10 para Windows al iniciar el equipo**.
   - Si quiere desactivar la ejecución automática de la aplicación, desmarque la casilla **Iniciar Kaspersky Endpoint Security 10 para Windows al iniciar el equipo**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Inicio y detención manuales de la aplicación

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.

Kaspersky Endpoint Security se tiene que iniciar manualmente si ha deshabilitado anteriormente el inicio automático de la aplicación.

Para iniciar la aplicación manualmente:

En el menú **Iniciar**, seleccione**Aplicaciones** → **Kaspersky Endpoint Security para Windows**.

Para detener la aplicación manualmente:

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 **Salir**.

Suspensión y reanudación de la protección y control del equipo

Suspender la protección y control del equipo significa desactivar 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 error occurred significa que la protección y control del equipo están suspendidos.
- El icono protection enabled significa que la protección y control del equipo están desactivados.

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 suspender la protección y control del equipo:

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

   Se abre la ventana **Suspender la protección**.
3. Seleccione una de las siguientes opciones:
   - **Suspender durante el tiempo especificado**: la protección y control del equipo se reanudan una vez transcurrido el tiempo que se especifica en la lista desplegable que se muestra a continuación.
   - **Suspender hasta reiniciar**: la protección y control del equipo se reanudan después de salir de la aplicación y de volver a abrirla, o de reiniciar el sistema operativo. Para utilizar esta opción, debe activarse el inicio automático de la aplicación.
   - **Suspender**: la protección y control del equipo se reanudan cuando usted decide volver a activarlos.
4. Si seleccionó la opción **Suspender durante el tiempo especificado** en el paso anterior, seleccione el intervalo necesario en la lista desplegable.

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 y control**.

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

Protección del sistema de archivos del equipo. Antivirus de archivos

Esta sección contiene información acerca del Antivirus de archivos e instrucciones para configurar los parámetros del componente.

Acerca del Antivirus de archivos

El Antivirus de archivos impide la infección del sistema de archivos del equipo. Por defecto, el Antivirus de archivos se inicia junto con Kaspersky Endpoint Security, permanece activo de manera continua en la memoria del equipo y analiza todos los archivos que se abren, se guardan o se inician en el equipo y en todas las unidades conectadas al equipo en busca de virus y otras amenazas.

Al detectar una amenaza en un archivo, Kaspersky Endpoint Security realiza lo siguiente:

1. Identifica el tipo de objeto que se detectó en el archivo (como *virus* o *troyano*).
2. Etiqueta el archivo como *probablemente infectado* cuando el análisis no puede identificar si el archivo está infectado. El archivo puede contener una secuencia de código característica de virus u otras clases de malware, o un código modificado de un virus conocido.
3. La aplicación muestra una notificación acerca del objeto malicioso detectado en el archivo (si las notificaciones están configuradas), y procesa el archivo; para ello, ejecuta la acción especificada en la configuración del Antivirus de archivos.

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. Si es necesario, puede deshabilitar la Protección contra amenazas de archivos.

Para habilitar o deshabilitar la Protección contra amenazas de archivos, realice lo siguiente:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas de archivos**.

   La configuración del componente Protección contra amenazas de archivos se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:
   - Si desea habilitar la Protección frente a amenazas en archivos, seleccione la casilla **Protección contra amenazas de archivos**.
   - Si desea deshabilitar la Protección frente a amenazas en archivos, desactive la casilla **Protección contra amenazas de archivos**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

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. En caso de que existan conflictos durante el funcionamiento de un componente, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky (https://companyaccount.kaspersky.com). 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 ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas de archivos**.

   La configuración del componente **Protección contra amenazas de archivos** se muestra en la parte derecha de la ventana.
3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Protección contra amenazas de archivos**.
4. En la ventana **Protección contra amenazas de archivos**, seleccione la ficha **Adicional**.
5. En la sección **Suspender tarea**:

   - Si desea configurar la suspensión automática de la Protección contra amenazas de archivos a una hora especificada, seleccione la casilla **Mediante programación** y haga clic en el botón **Programación**.

     Se abre la ventana **Suspender tarea**.
   - Si desea configurar la suspensión automática de la Protección contra amenazas de archivos al inicio de aplicaciones especificadas, seleccione la casilla **Al iniciarse ciertas aplicaciones** y haga clic en el botón **Seleccionar**.

     Se abre la ventana **Aplicaciones**.
6. Realice una de las siguientes acciones:

   - Si desea configurar la suspensión automática de la Protección contra amenazas de archivos a una hora especificada, en la ventana **Suspender tarea**, use los campos **Suspender tarea a las** y **Reanudar tarea a las** para especificar el período (en formato HH:MM) durante el cual se debe suspender el componente Protección contra amenazas de archivos. Haga clic en **Aceptar**.
   - Si está configurando la suspensión automática de la Protección contra amenazas de archivos cuando se inician determinadas aplicaciones, use los botones **Agregar**, **Modificar** y **Eliminar** de la ventana **Aplicaciones** para crear una lista de las aplicaciones que, cuando se ejecuten, suspendan la Protección contra amenazas de archivos. Haga clic en **Aceptar**.
7. En la ventana **Protección contra amenazas de archivos**, haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de la Protección contra amenazas de archivos

Puede realizar las siguientes acciones para configurar el componente Protección contra amenazas de archivos:

- Modificar el nivel de seguridad.

  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.

- Cambie la acción que realiza el componente Protección contra amenazas de archivos cuando detecta un archivo infectado.

- Forme el alcance de la protección del componente Protección contra amenazas de archivos.

  Puede ampliar o reducir el alcance de la protección agregando o eliminando objetos, o cambiando el tipo de archivos que se analizarán.

- Configurar el analizador heurístico.

  El componente Protección contra amenazas de archivos usa una técnica de análisis de firmas. Durante el análisis de la firma, el componente Protección contra amenazas de archivos compara el objeto detectado con los registros en las bases de datos antivirus de la aplicación. Según las recomendaciones de los expertos de Kaspersky, el análisis de firmas está siempre habilitado.

  Para aumentar la efectividad de la protección, puede utilizar el análisis heurístico. Durante el análisis heurístico, el componente Protección contra amenazas de archivos analiza la actividad de los objetos en el sistema operativo. El análisis heurístico permite detectar objetos maliciosos sobre los cuales no existen registros en las bases de datos antivirus de la aplicación.

- Optimizar el análisis.

  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.

- Configurar el análisis de archivos compuestos.

- Modificar el modo de análisis de archivos.

Modificación del nivel de seguridad

Para proteger el sistema de archivos del equipo, el componente Protección contra amenazas de archivos aplica diversos grupos de configuraciones. Estos grupos de configuraciones se denominan *niveles de seguridad*. Existen tres niveles de seguridad predeterminados: **Alto**, **Recomendado** y **Bajo**. Se considera que el nivel de seguridad **Recomendado** es la configuración óptima recomendada por los expertos de Kaspersky.

Para cambiar un nivel de seguridad:

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

2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas de archivos**.

   La configuración del componente Protección contra amenazas de archivos se muestra en la parte derecha de la ventana.

3. En la sección **Nivel de seguridad**, realice una de las siguientes acciones:

   - Si desea configurar uno de los niveles de seguridad predeterminados (**Alto**, **Recomendado** o **Bajo**), selecciónelo con el control deslizante.
   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** e introduzca sus preferencias de configuración en la ventana **Protección contra amenazas de archivos** que se abre.

     Después de configurar un nivel personalizado de seguridad, el nombre del nivel de seguridad que aparece en la sección **Nivel de seguridad** cambia a **Personalizado**.
   - Si desea cambiar el nivel de seguridad al nivel **Recomendado**, haga clic en el botón **Predeterminado**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de la acción que el Antivirus de archivos llevará a cabo en archivos infectados

Para modificar la acción que el Antivirus de archivos llevará a cabo en archivos infectados:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.

3. En la sección **Acción al detectar una amenaza**, seleccione la opción que desee:

   - **Seleccionar acción automáticamente**.
   - **Realizar acción: Desinfectar. Eliminar si falla la desinfección**.
   - **Realizar acción: Desinfectar**.

     Incluso si esta opción está seleccionada, Kaspersky Endpoint Security realiza la acción **Eliminar** en los archivos que son parte de la aplicación Tienda Windows.

   - **Realizar acción: Eliminar**.
   - **Realizar acción: Bloquear**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación del alcance de la protección del Antivirus 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 Antivirus de archivos. De manera predeterminada, el Antivirus de archivos analiza solamente archivos infectables almacenados e discos duros, unidades de red o medios extraíbles.

Para crear el alcance de la protección:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de archivos**.

4. En la ventana **Antivirus de archivos**, seleccione la ficha **General**.

5. En la sección **Tipos de archivos**, especifique el tipo de archivos que quiera que analice el Antivirus de archivos:

   - Si desea analizar todos los archivos, seleccione **Todos los archivos**.
   - Si desea analizar archivos con los formatos más vulnerables a infecciones, seleccione **Archivos analizados según su formato**.
   - Si desea analizar archivos con las extensiones más vulnerables a infecciones, seleccione **Archivos analizados según su extensión**.

   Cuando seleccione el tipo de archivos que se analizarán, recuerde la siguiente información:

   - Para algunos formatos de archivos (por ejemplo, .txt), la probabilidad de intrusión de código malicioso y su posterior activación es bastante reducida. Además, otros formatos contienen o pueden contener código ejecutable (por ejemplo, .exe, .dll y .doc). El riesgo de que el código malicioso ingrese en estos archivos y se active es relativamente alto.
   - Un intruso puede enviar un virus u otro programa malicioso al equipo en un archivo ejecutable al que se le ha cambiado el nombre con la extensión .txt. Si selecciona el análisis de archivos por extensión, en el análisis se ignorará este archivo. Si selecciona el análisis de archivos por formato, independientemente de la extensión, el Antivirus de archivos analiza el encabezado del archivo. Este análisis puede revelar que el archivo tiene un formato .exe. Este tipo de archivo se analiza en profundidad en busca de virus u otro tipo de malware.

6. En la lista **Alcance de la protección**, realice una de las siguientes acciones:

   - Si quiere agregar un nuevo objeto al alcance del análisis, haga clic en el botón **Agregar**.
   - Si quiere cambiar la ubicación de un objeto, selecciónelo en el área de alcance del análisis y haga clic en el botón **Modificar**.

   Se abre la ventana **Seleccionar alcance del análisis**.

   - Si desea eliminar un objeto de la lista de objetos que se analizarán, selecciónelo de la lista de objetos que se analizarán y haga clic en el botón **Eliminar**.

     Se abre una ventana para confirmar la eliminación.

7. Realice una de las siguientes acciones:

- Si quiere agregar un nuevo objeto o cambiar la ubicación de un objeto de la lista de objetos que se analizarán, selecciónelo en la ventana **Seleccionar alcance del análisis** y haga clic en el botón **Agregar**.

  Todos los objetos seleccionados en la ventana **Seleccionar alcance del análisis** se muestran en la ventana **Antivirus de archivos**, en la lista **Alcance de la protección**.

  Haga clic en **Aceptar**.

- Si desea eliminar un objeto, haga clic en el botón **Sí** en la ventana de confirmación de eliminación.

8. Si es necesario, repita los pasos 6 y 7 para agregar, mover o quitar objetos de la lista de objetos para analizar.

9. Para excluir un objeto de la lista de objetos a analizar, desactive la casilla junto al objeto en la lista **Alcance de la Protección**. Sin embargo, el objeto permanecerá en la lista de objetos que se analizarán aunque esté excluido del análisis del Antivirus de archivos.

10. En la ventana **Antivirus de archivos**, haga clic en **Aceptar**.

11. Para guardar los cambios, haga clic en el botón **Guardar**.

Uso del analizador heurístico con el Antivirus de archivos

Para configurar el uso del analizador heurístico en la operación del Antivirus de archivos:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de archivos**.

4. En la ventana **Antivirus de archivos**, seleccione la ficha **Rendimiento**.

5. En la sección **Métodos de análisis**:

   - Si quiere que el Antivirus de archivos use el análisis heurístico, seleccione la casilla **Análisis heurístico** y use el control deslizante para definir el nivel del análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.

   - Si no quiere que el Antivirus de archivos use el análisis heurístico, desmarque la casilla **Análisis heurístico**.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Uso de tecnologías de análisis en el funcionamiento del Antivirus de archivos

Para configurar el uso de tecnologías de análisis en el funcionamiento del Antivirus de archivos:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la ficha **Adicional**.
5. En la sección **Tecnologías de análisis**:
   - Seleccione las casillas adyacentes a los nombres de las tecnologías que quiera usar en el funcionamiento del Antivirus de archivos.
   - Desmarque las casillas adyacentes a los nombres de las tecnologías que no quiera usar en el funcionamiento del Antivirus de archivos.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Optimización del análisis de archivos

Para optimizar el análisis de archivos:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.
3. Haga clic en el botón **Configuración**.

   Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la ficha **Rendimiento**.
5. En la sección **Optimización del análisis**, seleccione la casilla **Analizar solo archivos nuevos y modificados**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Análisis de archivos compuestos

Una técnica común para ocultar virus u otro malware es incorporarlo en archivos compuestos, como archivos de almacenamiento o bases de datos de correo electrónico. 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 el conjunto 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 antivirus 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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la ficha **Rendimiento**.
5. 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.
6. Para analizar solo archivos compuestos nuevos y modificados, seleccione la casilla de verificación **Analizar solo archivos nuevos y modificados**.

   El Antivirus de archivos solo analizará archivos compuestos nuevos y modificados de todos los tipos.
7. Haga clic en el botón **Adicional**.

   Se abre la ventana **Archivos compuestos**.
8. En la sección **Análisis en segundo plano**, realice una de las siguientes acciones:

   - Para que el Antivirus de archivos no descomprima archivos compuestos en segundo plano, desmarque la casilla **Descomprimir archivos compuestos en segundo plano**.
   - Para permitir que el Antivirus de archivos descomprima archivos compuestos en segundo plano, marque la casilla **Descomprimir archivos compuestos en segundo plano** y especifique el valor que desee en el campo **Tamaño mínimo de archivo**.
9. En la sección **Límite de tamaño**, realice una de las siguientes acciones:

   - Para que el Antivirus de archivos no descomprima archivos compuestos de gran tamaño, marque la casilla **No desempaquetar archivos compuestos grandes** y especifique el valor deseado en el campo **Tamaño máximo de archivo**. El Antivirus de archivos no descomprimirá archivos compuestos que superen el tamaño especificado.
   - Para permitir que el Antivirus de archivos descomprima archivos compuestos de gran tamaño, desmarque la casilla de verificación **No desempaquetar archivos compuestos grandes**.

     Un archivo se considera de gran tamaño si su tamaño supera el valor especificado en el campo **Tamaño máximo de archivo**.

El Antivirus de archivos analiza los archivos de gran tamaño extraídos de archivos de almacenamiento, independientemente de que la casilla **No desempaquetar archivos compuestos grandes** esté activada o no.

10. Haga clic en **Aceptar**.
11. En la ventana **Antivirus de archivos**, haga clic en **Aceptar**.
12. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación del modo de análisis

Modo de análisis se refiere a la condición según la cual el Antivirus de archivos inicia el análisis de los archivos. Por defecto, Kaspersky Endpoint Security analiza los archivos en el modo inteligente. En este modo de análisis de archivos, el Antivirus 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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de archivos**.
   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.
   Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la ficha **Adicional**.
5. En la sección **Modo de análisis**, seleccione el modo que desee:
   - **Modo inteligente**.
   - **Ante operaciones de acceso y modificación**.
   - **Ante operaciones de acceso**.
   - **Ante operaciones de ejecución**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Protección del correo. Antivirus de correo electrónico

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca del Antivirus de correo electrónico e instrucciones para configurar los parámetros del componente.

Acerca del Antivirus de correo electrónico

El Antivirus de correo electrónico analiza mensajes de correo entrantes y salientes en busca de virus y otras amenazas. Se inicia junto con Kaspersky Endpoint Security, permanece continuamente en la memoria del equipo y analiza todos los mensajes que se envían o reciben a través de los protocolos POP3, SMTP, IMAP, MAPI y NNTP. Si no se detectan amenazas en el mensaje, el usuario podrá verlo y/o procesarlo.

Al detectar una amenaza en un mensaje de correo electrónico, el Antivirus de correo electrónico realiza lo siguiente:

1. Identifica el tipo de objeto que se detectó en el mensaje de correo electrónico (por ejemplo: un *troyano*).
2. Al mensaje de correo electrónico se le asigna uno de los siguientes estados:
    - *Probablemente infectado*. Este estado se asigna si el análisis no puede determinar si el mensaje de correo electrónico realmente está infectado. Es posible que el mensaje de correo electrónico contenga una sección de código característica de virus u otras clases de malware, o un código modificado de un virus conocido.
    - *Infectado*. Este estado se asigna a un objeto si el análisis de un mensaje de correo electrónico encuentra una sección de código de un virus conocido incluido en las bases de datos antivirus de Kaspersky Endpoint Security.
    - *No se encuentra*. Este estado se asigna a un objeto si el análisis de un mensaje de correo electrónico no detecta virus u otras amenazas.

Entonces, la aplicación bloquea el mensaje de correo electrónico, muestra una notificación acerca del objeto detectado (si se especifica en la configuración de las notificaciones), y realiza la acción que se especifica en la configuración del Antivirus de correo electrónico.

Este componente interactúa con clientes de correo instalados en el equipo. Se dispone de una extensión incrustable para el cliente de correo Microsoft Office Outlook® que le permite personalizar la configuración del análisis de mensajes. La extensión del Antivirus de correo electrónico se incorpora al cliente de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

La operación que realiza el Antivirus de correo electrónico se indica mediante el icono de la aplicación en el área de notificación de la barra de tareas. Cuando el Antivirus de correo electrónico analiza un mensaje de correo electrónico, el icono de la aplicación cambia a  .

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. Puede deshabilitar el componente Protección contra amenazas de correo si es necesario.

Para habilitar o deshabilitar el componente Protección contra amenazas de correo:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas de correo**.

   La configuración del componente Protección contra amenazas de correo se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:

   - Si desea habilitar el componente Protección contra amenazas de correo, seleccione la casilla **Protección contra amenazas de correo**.
   - Si desea deshabilitar el componente Protección contra amenazas de correo, desactive la casilla **Protección contra amenazas de correo**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del Antivirus de correo electrónico

Para configurar el Antivirus de correo electrónico, puede realizar lo siguiente:

- Cambiar el nivel de seguridad del correo.

  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.
- Cambiar la acción que realiza Kaspersky Endpoint Security en los mensajes infectados.
- Modificar el alcance de la protección del Antivirus de correo electrónico.
- Configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico.

  Puede activar o desactivar 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.
- Configurar el filtrado por el tipo de adjuntos del mensaje de correo electrónico.

  El filtrado de adjuntos a mensajes por tipo permite renombrar o eliminar automáticamente archivos de los tipos especificados.
- Configurar el analizador heurístico.

  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 en mensajes para las cuales no exista ningún registro en las bases de datos de Kaspersky Endpoint Security.

- Configurar el análisis de correo electrónico en Microsoft Office Outlook.

  Se dispone de una extensión que puede incorporarse al cliente de correo Microsoft Office Outlook y permite configurar fácilmente los parámetros del análisis del correo.

  Si se está trabajando con otros clientes de correo, como Microsoft Outlook Express®, Windows Mail y Mozilla™ Thunderbird™, el componente del Antivirus de correo electrónico analiza el tráfico de los protocolos de correo SMTP, POP3, IMAP y NNTP.

  Si se está trabajando con el cliente de correo Mozilla Thunderbird, el Antivirus de correo electrónico 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**.

Modificación del nivel de seguridad del correo

El componente Protección contra amenazas de correo implementa diversos grupos de configuraciones para proteger el correo. Los grupos de configuraciones se denominan *niveles de seguridad del correo*. Existen tres niveles de seguridad del correo: **Alto**, **Recomendado** y **Bajo**. El nivel de seguridad del correo **Recomendado** se considera la configuración óptima de configuraciones y es el nivel recomendado por Kaspersky.

Para modificar el nivel de seguridad del correo:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas de correo**.

   La configuración del componente Protección contra amenazas de correo se muestra en la parte derecha de la ventana.
3. En la sección **Nivel de seguridad**, realice una de las siguientes acciones:

   - Si desea instalar uno de los niveles preinstalados de seguridad del correo (**Alto**, **Recomendado** o **Bajo**), use el control deslizante para elegir uno.
   - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** e introduzca sus preferencias de configuración en la ventana **Protección contra amenazas de correo** que se abre.

     Después de configurar un nivel personalizado de seguridad del correo, el nombre del nivel de seguridad que aparece en la sección **Nivel de seguridad** cambia a **Personalizado**.
   - Si desea cambiar el nivel de seguridad del correo al nivel **Recomendado**, haga clic en el botón **Predeterminado**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de la acción que se llevará a cabo en mensajes de correo electrónico infectados

Para modificar la acción que se llevará a cabo en mensajes de correo infectados:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Antivirus de correo electrónico**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de correo electrónico.

3. En la sección **Acción al detectar una amenaza**, seleccione la acción que realizará Kaspersky Endpoint Security cuando se detecte un mensaje infectado:

   - **Seleccionar acción automáticamente**.
   - **Realizar acción: Desinfectar. Eliminar si falla la desinfección**.
   - **Realizar acción: Desinfectar**.
   - **Realizar acción: Eliminar**.
   - **Realizar acción: Bloquear**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación del alcance de la protección del Antivirus de correo electrónico

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 Antivirus de correo electrónico incluyen la configuración para integrar el Antivirus de correo electrónico en clientes de correo y el tipo de mensajes de correo electrónico y los protocolos de correo electrónico cuyo tráfico es analizado por el Antivirus de correo electrónico. 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 crear el alcance de la protección del Antivirus de correo electrónico.

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Antivirus de correo electrónico**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de correo electrónico.

3. Haga clic en el botón **Configuración**.

   Se abre la ventana **Antivirus de correo electrónico**.

4. Seleccione la ficha **General**.

5. En la sección **Alcance de la protección**, realice una de las siguientes acciones:

   - Si desea que el Antivirus de correo electrónico analice todos los mensajes de correo electrónico entrantes y salientes de su equipo, seleccione la opción **Mensajes entrantes y salientes**.
   - Si desea que el Antivirus de correo electrónico analice solamente los mensajes de correo entrantes de su equipo, seleccione la opción **Solo mensajes entrantes**.

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.

6. En la sección **Conectividad**, realice lo siguiente:

   - Si desea que el Antivirus de correo electrónico analice los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen a su equipo, seleccione la casilla **Tráfico POP3/SMTP/NNTP/IMAP**.

     Si no desea que el Antivirus de correo electrónico analice los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen a su equipo, desmarque la casilla **Tráfico POP3/SMTP/NNTP/IMAP**. En este caso, los mensajes son analizados por la extensión del Antivirus de correo electrónico incorporada al cliente de correo de Microsoft Office Outlook después de que lleguen al equipo del usuario si se selecciona la casilla **Adicional: extensión para Microsoft Office Outlook**.

     Si usa un cliente de correo que no sea Microsoft Office Outlook, el Antivirus de correo electrónico no analiza los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP e IMAP cuando se desmarca la casilla **Tráfico POP3/SMTP/NNTP/IMAP**.

   - Si desea abrir el acceso a la configuración del Antivirus de correo electrónico desde Microsoft Office Outlook y activar el análisis de los mensajes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que llegan al equipo utilizando la extensión incorporada a Microsoft Office Outlook, seleccione la casilla **Adicional: extensión para Microsoft Office Outlook**.

     Si desea bloquear el acceso a la configuración del Antivirus de correo electrónico desde Microsoft Office Outlook y desactivar 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 **Adicional: extensión para Microsoft Office Outlook**.

     La extensión del Antivirus de correo electrónico se incorpora al cliente de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Análisis de archivos compuestos adjuntos a mensajes de correo electrónico

Para configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Antivirus de correo electrónico**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de correo electrónico.

3. Haga clic en el botón **Configuración**.

   Se abre la ventana **Antivirus de correo electrónico**.

4. Seleccione la ficha **General**.

5. Haga lo siguiente en la sección **Análisis de archivos compuestos** :

   - Si quiere que el Antivirus de correo electrónico omita los archivos de almacenamiento adjuntos a mensajes, desmarque la casilla **Analizar archivos de almacenamiento adjuntos**.

   - Si quiere que el Antivirus de correo electrónico omita los adjuntos a mensajes que tengan más de N megabytes de tamaño, seleccione la casilla **No analizar archivos de almacenamiento mayores que N MB**. Si selecciona esta casilla, especifique el tamaño máximo del archivo en el campo junto al nombre de la casilla.

   - Si desea que el Antivirus de correo electrónico analice los adjuntos a mensajes cuyo análisis lleve más de N segundos, desmarque la casilla **No analizar archivos durante más de N segundos**.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Filtrado de archivos adjuntos a mensajes de correo electrónico

Los programas maliciosos pueden distribuirse como archivos adjuntos a mensajes de correo electrónico. 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 cambiar el nombre de un archivo adjunto de un determinado tipo, Kaspersky Endpoint Security puede proteger su equipo contra la ejecución automática de un programa malicioso.

Para configurar el filtrado de archivos adjuntos:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Antivirus de correo electrónico**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de correo electrónico.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de correo electrónico**.

4. En la ventana **Antivirus de correo electrónico**, seleccione la ficha **Filtrado de documentos adjuntos**.

5. Realice una de las siguientes acciones:

   - Si no desea que el Antivirus de correo electrónico filtre los archivos adjuntos de correo, seleccione la configuración **Deshabilitar el filtrado**.

   - Si desea que el Antivirus de correo electrónico cambie el nombre de los archivos adjuntos de los tipos especificados, seleccione la configuración **Cambiar el nombre de los tipos de adjuntos especificados**.

Tenga en cuenta que el formato real de un archivo puede no coincidir con la extensión de su nombre de archivo.

Si activa el filtrado de objetos que adjuntos a mensajes de correo electrónico, el Antivirus de correo electrónico 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 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: extensión para correos electrónicos de Microsoft Office Outlook guardados

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 compatibles con XML, 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. Es la próxima generación de metarchivos del SO de Microsoft Windows. Los archivos EMF no son compatibles con Microsoft Windows de 16 bits.

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

- Si desea que el Antivirus de correo electrónico elimine los adjuntos a mensajes de los tipos especificados, seleccione la opción **Eliminar los tipos de adjuntos especificados**.

6. Si seleccionó la opción **Cambiar el nombre de los tipos de adjuntos especificados** o la opción **Eliminar los tipos de adjuntos especificados** en el paso anterior, seleccione las casillas que se encuentran frente a los tipos de archivos relevantes.

   Puede modificar la lista de tipos de archivos con los botones **Agregar**, **Modificar** y **Eliminar**.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Análisis de correo electrónico en Microsoft Office Outlook

Durante la instalación de Kaspersky Endpoint Security, la extensión del Antivirus de correo electrónico se incorpora a Microsoft Office Outlook (en adelante, Outlook). Le permite abrir la configuración del Antivirus de correo electrónico desde Outlook y especificar en qué momento se deben analizar los mensajes de correo electrónico en busca de virus y otras amenazas. La extensión del Antivirus de correo electrónico para Outlook puede analizar mensajes entrantes y salientes transmitidos a través de los protocolos POP3, SMTP, NNTP, IMAP y MAPI.

La configuración del Antivirus de correo electrónico se puede definir directamente en Outlook si se selecciona la casilla **Adicional: extensión para Microsoft Office Outlook** en la interfaz de Kaspersky Endpoint Security.

En Outlook, los mensajes entrantes primero son analizados por el Antivirus de correo electrónico (si se selecciona la casilla **Tráfico POP3/SMTP/NNTP/IMAP** en la interfaz de Kaspersky Endpoint Security) y, luego, por la extensión del Antivirus de correo electrónico para Outlook. Si el Antivirus de correo electrónico detecta un objeto malicioso en un mensaje, le advierte sobre este evento.

La acción que usted elija en la ventana de notificación determinará qué componente eliminará la amenaza presente en el mensaje: el Antivirus de correo electrónico o la extensión del Antivirus de correo electrónico para Outlook.

- Si selecciona **Desinfectar** o **Eliminar** en la ventana de notificación, el Antivirus de correo electrónico eliminará la amenaza.
- Si selecciona **Omitir** en la ventana de notificación al usuario, la extensión del Antivirus de correo electrónico para Outlook eliminará la amenaza.

Los mensajes salientes primero son analizados por la extensión del Antivirus de correo electrónico para Outlook y, luego, por el Antivirus de correo electrónico.

Configuración del análisis del correo en Outlook

Para configurar el análisis del correo en Outlook 2007:

1. Abra la ventana principal de Outlook 2007.
2. Seleccione **Servicio** → **Configuración** en la barra de menús.

   Se abre la ventana **Opciones**.
3. En la ventana **Opciones**, seleccione la ficha **Protección del correo**.

Para configurar el análisis del correo en Outlook 2010/2013:

1. Abra la ventana principal de Outlook.

   Seleccione la ficha **Archivo** en la esquina superior izquierda.
2. Haga clic en el botón **Opciones**.

   Se abre la ventana **Opciones de Outlook**.
3. Seleccione la sección **Complementos**.

La configuración de los complementos incorporados en Outlook se muestra en la parte derecha de la ventana.

4. Haga clic en el botón **Opciones de complementos**.

Configuración del análisis del correo usando Kaspersky Security Center

Si el correo se analiza usando la extensión del Antivirus de correo electrónico para Outlook, se recomienda usar el Modo de intercambio en caché. Para información más detallada sobre el modo de almacenamiento en memoria caché de intercambio y recomendaciones sobre su uso, consulte la Base de conocimientos de Microsoft: https://technet.microsoft.com/es-mx/library/cc179175.aspx.

Para configurar el modo de funcionamiento de la extensión del Antivirus de correo electrónico 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 para el cual quiera configurar el análisis del correo.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Protección antivirus**, seleccione la subsección **Antivirus de correo electrónico**.
7. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de correo electrónico**.
8. En la sección **Conectividad**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección del correo electrónico**.
9. En la ventana **Protección del correo electrónico**:
   - Seleccione la casilla **Analizar al recibir** si quiere que la extensión del Antivirus de correo electrónico para Outlook analice mensajes entrantes cuando llegan al buzón de correo.
   - Seleccione la casilla **Analizar al leer** si quiere que la extensión del Antivirus de correo electrónico para Outlook analice mensajes entrantes cuando los abra el usuario.
   - Seleccione la casilla **Analizar al enviar** si quiere que la extensión del Antivirus de correo electrónico para Outlook analice mensajes salientes cuando son enviados.
10. En la ventana **Protección del correo electrónico**, haga clic en **Aceptar**.

11. En la ventana **Antivirus de correo electrónico**, haga clic en **Aceptar**.

12. Aplique la directiva.

    Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

Protección del equipo en Internet. Antivirus de Internet

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca del Antivirus de Internet e instrucciones para configurar los parámetros del componente.

Acerca del Antivirus de Internet

Cada vez que se conecta a Internet, expone información almacenada en su equipo a virus y otras clases de malware. Estos pueden infiltrarse en el equipo mientras el usuario descarga software gratuito o navega sitios web vulnerados por delincuentes. Los gusanos de red pueden encontrar un camino hacia el equipo apenas establece una conexión a Internet, incluso antes de que abra una página web o descargue un archivo.

El Antivirus de Internet protege los datos entrantes y salientes que se envían al equipo y desde el equipo mediante los protocolos HTTP y FTP y verifica las direcciones URL comparándolas con la lista de direcciones web maliciosas o de phishing.

El Antivirus de Internet intercepta y analiza todas las páginas web y todos los archivos a los que accedieron el usuario o una aplicación mediante los protocolos HTTP o FTP en busca de virus y otras amenazas. Después, sucede lo siguiente:

- Si se determina que la página o el archivo no contienen código malicioso, el usuario obtiene acceso inmediato a ellos.
- Si un usuario accede a una página web o a un archivo que contiene el código malicioso, la aplicación realiza la acción que se especifica en la configuración del Antivirus de Internet.

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. Puede deshabilitar el componente Protección contra amenazas web si es necesario.

Para habilitar o deshabilitar el componente Protección contra amenazas web:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas web**.

   La configuración del componente Protección contra amenazas web se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:

- Si desea habilitar el componente Protección frente amenazas web, seleccione la casilla **Protección contra amenazas web**.
- Si desea deshabilitar el componente Protección frente amenazas web, desactive la casilla **Protección contra amenazas web**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del Antivirus de Internet

Para configurar el Antivirus de Internet, puede realizar lo siguiente:

- Modifique el nivel de seguridad del tráfico de internet.

  Puede seleccionar uno de los niveles preinstalados de seguridad para el tráfico de internet que se recibe o se transmite mediante los protocolos HTTP y FTP, o configurar un nivel de seguridad personalizado del tráfico de internet.

  Si modifica la configuración del nivel de seguridad del tráfico de internet, siempre puede volver a la configuración recomendada del nivel de seguridad del tráfico de internet.

- Modifique la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos de tráfico de internet.

  Si el análisis de un objeto HTTP muestra que contiene código malicioso, la respuesta del Antivirus de Internet depende de la acción que se haya seleccionado.

- Configure el análisis que realiza el Antivirus de Internet de direcciones URL comparándolas con las bases de datos de direcciones web maliciosas y de phishing.

- Configure el uso del análisis heurístico cuando escanee si hay virus y otros programas maliciosos en el tráfico de Internet.

  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.

- Configure el uso del análisis heurístico cuando escanee páginas web para vínculos de phishing.

- Optimice el análisis que el Antivirus de Internet realiza del tráfico de internet que se envía y se recibe mediante los protocolos HTTP y FTP.

- Cree una lista de direcciones URL de confianza.

  Puede crear una lista de direcciones URL cuyo contenido considera confiable. El Antivirus de Internet no analiza información proveniente de direcciones URL de confianza en busca de virus u otras amenazas. Esta opción es útil, por ejemplo, cuando el Antivirus de Internet 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.

Modificación del nivel de seguridad del tráfico web

Para proteger los datos que se reciben y se transmiten mediante los protocolos HTTP y FTP, el componente Protección contra amenazas web aplica diversos grupos de configuraciones. Estos grupos de configuraciones se denominan *niveles de seguridad del tráfico web*. Existen tres niveles preinstalados de seguridad del tráfico web: **Alto**, **Recomendado** y **Bajo**. El nivel de seguridad del tráfico de internet **Recomendado** se considera la configuración óptima y es el nivel recomendado por Kaspersky.

Para modificar el nivel de seguridad del tráfico web:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección básica contra amenazas**, seleccione **Protección contra amenazas web**.

   La configuración del componente Protección contra amenazas web se muestra en la parte derecha de la ventana.
3. En la sección **Nivel de seguridad**, realice una de las siguientes acciones:

   - Si desea instalar uno de los niveles preinstalados de seguridad del tráfico web (**Alto**, **Recomendado** o **Bajo**), use el control deslizante para elegir uno.
   - Si desea configurar un nivel de seguridad personalizado para el tráfico web, haga clic en el botón **Configuración** y especifique la configuración en la ventana **Protección contra amenazas web** que se abre.

     Cuando se configura un nivel personalizado de seguridad del tráfico web, el nombre del nivel de seguridad en la sección **Nivel de seguridad** cambia a **Personalizado**.
   - Si desea cambiar el nivel de seguridad del tráfico web al nivel **Recomendado**, haga clic en el botón **Predeterminado**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de la acción que se llevará a cabo en objetos maliciosos del tráfico de Internet

Para modificar la acción que se llevará a cabo en objetos maliciosos del tráfico de internet:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de Internet**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de Internet.
3. En la sección **Acción al detectar una amenaza**, seleccione la acción que Kaspersky Endpoint Security realiza en los objetos maliciosos del tráfico de internet:

   - **Seleccionar acción automáticamente**.
   - **Bloquear descarga**.
   - **Permitir descarga**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Análisis de direcciones URL que realiza el Antivirus de Internet comparándolas con las bases de datos de direcciones web maliciosas 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 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 Antivirus de Internet supervisa los intentos de acceder a un sitio web de phishing en el nivel de tráfico de Internet 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 Antivirus de Internet para comprobar las direcciones URL comparándolas con las bases de datos de direcciones web maliciosas y de phishing:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de Internet**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de Internet.
3. Haga clic en el botón **Configuración**.

   Se abre la ventana **Antivirus de Internet**.
4. En la ventana **Antivirus de Internet**, seleccione la ficha **General**.
5. Haga lo siguiente:

   - Si desea que el Antivirus de Internet compruebe las direcciones URL comparándolas con las bases de datos de direcciones web maliciosas, en la sección **Métodos de análisis**, seleccione la casilla **Comprobar si los vínculos están incluidos en la base de datos de vínculos maliciosos**.
   - Si desea que el Antivirus de Internet compruebe las direcciones URL comparándolas con las bases de datos de direcciones web de phishing, en la sección **Configuración del componente Anti-Phishing**, seleccione la casilla **Comprobar si los vínculos están incluidos en la base de datos de vínculos fraudulentos**.

   También puede comprobar vínculos comparándolos con las bases de datos de reputación de Kaspersky Security Network.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Uso del Analizador heurístico con el Antivirus de Internet

Para configurar el uso del análisis heurístico:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de Internet**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de Internet.
3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abre la ventana **Antivirus de Internet**.
4. Seleccione la ficha **General**.
5. Si quiere que el Antivirus de Internet utilice el análisis heurístico para analizar el tráfico de Internet en busca de virus y otra clase de malware, en la sección **Métodos de análisis**, seleccione la casilla **Análisis heurístico para la detección de virus** y utilice el control deslizante para establecer el nivel del análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.
6. Si quiere que el Antivirus de Internet utilice el análisis heurístico para analizar páginas web en busca de vínculos de phishing, en la sección **Configuración del componente Anti-Phishing**, seleccione la casilla **Análisis heurístico para detectar vínculos fraudulentos**.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de la lista de direcciones URL de confianza

Para crear una lista de direcciones URL de confianza:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de Internet**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus de Internet.
3. Haga clic en el botón **Configuración**.

   Se abre la ventana **Antivirus de Internet**.
4. Seleccione la ficha **Direcciones URL de confianza**.
5. Seleccione la casilla **No analizar el tráfico web de las direcciones web de confianza**.
6. Cree una lista de direcciones URL o páginas web cuyo contenido considera confiable. Para crear una lista:

   a. Haga clic en el botón **Agregar**.

      Se abre la ventana **Dirección web/Máscara de dirección web**.

   b. Ingrese la dirección de un sitio web o de una página web, o la máscara de dicha dirección.

   c. Haga clic en **Aceptar**.

      Aparece un nuevo registro en la lista de direcciones URL de confianza.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Protección del tráfico de clientes de MI. Antivirus MI

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca del Antivirus MI e instrucciones para configurar los parámetros del componente.

Acerca del Antivirus MI

El Antivirus MI analiza el tráfico de clientes de mensajería instantánea (conocidos como *clientes de MI*).

El Antivirus MI no analiza mensajes transmitidos por canales cifrados.

Los mensajes que se envían mediante clientes de MI pueden contener los siguientes tipos de amenazas a la seguridad:

- Direcciones URL que intentan descargar un programa malicioso en el equipo
- Direcciones URL de programas y sitios web maliciosos usadas por intrusos para ataques de phishing

  Los ataques de phishing pretenden robar datos personales del usuario como números de tarjetas bancarias, detalles del pasaporte, contraseñas de sistemas de pagos bancarios y otros servicios en línea (como sitios de redes sociales o cuentas de correo electrónico).

Los archivos se pueden transmitir a través de los clientes de MI. Cuando se intentan guardar dichos archivos, se los analiza con el componente Antivirus de archivos.

El Antivirus MI intercepta cada uno de los mensajes que el usuario envía o recibe a través de un cliente de MI y lo analiza en busca de vínculos que puedan atentar contra la seguridad del equipo:

- Si no se detectan URL peligrosas en el mensaje, el usuario podrá tener acceso a él.
- Si se detectan vínculos peligrosas en un mensaje, el Antivirus MI reemplaza el mensaje con información sobre la amenaza en la ventana de mensajes del cliente de MI activo.

Activación y desactivación del Antivirus MI

De forma predeterminada, el Antivirus MI está activado, y se ejecuta en un modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar el Antivirus MI.

Existen dos formas de habilitar o deshabilitar el componente:

- Ficha **Protección y control** de la ventana principal de la aplicación.

- Desde la ventana de configuración de la aplicación.

Para Activar o desactivar el Antivirus MI en la ficha Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Protección**.

   Se abre la sección **Protección**.
4. Haga clic con el botón derecho del mouse en la línea del **Antivirus de MI** para visualizar el menú contextual de las acciones del componente.
5. Realice una de las siguientes acciones:

   - Para activar el Antivirus MI, seleccione **Iniciar** en el menú contextual.

     El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus de MI**, cambia al icono .
   - Para desactivar el Antivirus MI, seleccione **Detener** en el menú contextual.

     El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus de MI**, cambia al icono .

Para activar o desactivar el Antivirus MI en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de MI**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus MI.
3. Realice una de las siguientes acciones:

   - Si quiere activar el Antivirus MI, seleccione la casilla **Habilitar Antivirus de MI**.
   - Si quiere desactivar el Antivirus MI, desmarque la casilla **Habilitar Antivirus de MI**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del Antivirus MI

Puede realizar las siguientes acciones para configurar el Antivirus MI:

- Configure el alcance de la protección.

  Puede ampliar o reducir el alcance de la protección modificando el tipo de mensajes de clientes de MI que se deben analizar.
- Configure el Antivirus MI para analizar los vínculos presentes en mensajes de clientes de MI comparándolos con las bases de datos de direcciones web maliciosas y de phishing.

Creación del alcance de la protección del Antivirus MI

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. El tipo de mensajes de clientes de MI analizados, entrantes o salientes, es una propiedad del alcance de la protección del Antivirus MI. Por defecto, el Antivirus MI analiza mensajes tanto entrantes como salientes. Puede deshabilitar el análisis del tráfico saliente.

Para crear el alcance de la protección:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de MI**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus MI.
3. En la sección **Alcance de la protección**, realice una de las siguientes acciones:

   - Si desea que el Antivirus MI analice todos los mensajes de clientes de MI entrantes y salientes de su equipo, seleccione la opción **Mensajes entrantes y salientes**.
   - Si desea que el Antivirus MI analice solamente los mensajes de clientes de MI entrantes de su equipo, seleccione la opción **Solo mensajes entrantes**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Análisis de direcciones URL comparándolas con las bases de datos de direcciones web maliciosas y de phishing con el Antivirus MI

Para configurar el Antivirus MI para comprobar direcciones URL comparándolas con las bases de datos de direcciones web maliciosas y de phishing:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Antivirus de MI**.

   En la parte derecha de la ventana, se muestra la configuración del componente Antivirus MI.
3. En la sección **Métodos de análisis**, seleccione los métodos que desea que utilice el Antivirus MI:

   - Si quiere comprobar los vínculos presentes en mensajes de clientes de MI comparándolos con la base de datos de direcciones web maliciosas, seleccione la casilla **Comprobar si los vínculos están incluidos en la base de datos de vínculos maliciosos**.
   - Si quiere comprobar los vínculos presentes en mensajes de clientes de MI comparándolos con la base de datos de direcciones web de phishing, seleccione la casilla **Comprobar si los vínculos están incluidos en la base de datos de vínculos fraudulentos**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

System Watcher

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca del componente System Watcher y las instrucciones para configurarlo.

Acerca de System Watcher

System Watcher recopila datos sobre las acciones de las aplicaciones del equipo y transmite esta información a los demás componentes para lograr una protección más confiable.

Patrones de actividad peligrosa

La tecnología de Patrones de actividad peligrosa (BSS) (también denominadas "Patrones de actividad peligrosa") contiene las secuencias de las acciones de las aplicaciones que Kaspersky Endpoint Security clasifica como peligrosas. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Endpoint Security realiza la acción especificada. Las funcionalidades de Kaspersky Endpoint Security basadas en patrones de actividad peligrosa proporcionan una defensa proactiva para el equipo.

De forma predeterminada, si la actividad de la aplicación coincide con un patrón de actividad peligrosa, System Watcher mueve el archivo ejecutable de esa aplicación a la Cuarentena.

Reversión de las acciones realizadas por un malware

En función de la información que recopila System Watcher, Kaspersky Endpoint Security puede **revertir las acciones realizadas por malware en el sistema operativo** mientras lleva a cabo la desinfección.

Al revertir la actividad del malware en el sistema operativo, Kaspersky Endpoint Security toma medidas sobre los siguientes tipos de actividad de malware:

- Actividad de archivos.

  Kaspersky Endpoint Security elimina archivos ejecutables que han sido creados por un programa malicioso y que estén ubicados en cualquier medio, excepto los de la red.

  Kaspersky Endpoint Security elimina archivos ejecutables que han sido creados por un programa en el cual ha penetrado un programa malicioso.

  Kaspersky Endpoint Security no restaura archivos modificados o eliminados.

- Actividad del registro.

  Kaspersky Endpoint Security elimina particiones y claves del registro que han sido creadas por malware.

  Kaspersky Endpoint Security no restaura particiones ni claves del registro modificadas o eliminadas.

- Actividad del sistema.

  Kaspersky Endpoint Security cancela procesos que han sido iniciados por un programa malicioso.

  Kaspersky Endpoint Security cancela procesos en los cuales ha penetrado un programa malicioso.

  Kaspersky Endpoint Security no reanuda procesos que han sido interrumpidos por un programa malicioso.

- Actividad de red.

  Kaspersky Endpoint Security bloquea la actividad de red de programas maliciosos.

  Kaspersky Endpoint Security bloquea la actividad de red de procesos en los cuales ha penetrado un programa malicioso.

El Antivirus de archivos puede iniciar una reversión de acciones de malware; esto también puede realizarse durante un análisis antivirus.

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.

Activación y desactivación de System Watcher

Por defecto, el componente System Watcher está habilitado y se ejecuta en el modo recomendado por Kaspersky. Si es necesario, puede deshabilitar el componente System Watcher.

No se recomienda desactivar System Watcher a menos que sea absolutamente necesario, ya que afecta al desempeño de los componentes de protección. Los componentes de protección pueden solicitar datos recopilados por System Watcher para identificar en forma más exacta una amenaza detectada.

Existen dos formas de habilitar o deshabilitar System Watcher:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

*Para habilitar o deshabilitar el componente System Watcher en la ficha **Protección y control** de la ventana principal de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Protección**.

   Se abre la sección **Protección**.
4. Haga clic con el botón derecho del mouse para ver el menú contextual de la línea con información acerca del componente System Watcher.

   Se abre un menú para seleccionar acciones del componente.
5. Realice una de las siguientes acciones:

   - Para habilitar el componente System Watcher, seleccione **Iniciar**.

     El icono de estado del componente , que se muestra a la izquierda de la línea **System Watcher**, cambia al icono .
   - Para deshabilitar el componente System Watcher, seleccione **Detener**.

     El icono de estado del componente , que se muestra a la izquierda de la línea **System Watcher**, cambia al icono .

Para habilitar o deshabilitar el componente System Watcher desde la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **System Watcher**.

   En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. Realice una de las siguientes acciones:

   - Para habilitar el componente System Watcher, seleccione la casilla de verificación **Activar System Watcher**.
   - Para deshabilitar el componente System Watcher, desactive la casilla de verificación **Activar System Watcher**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de System Watcher

Puede realizar las siguientes acciones para configurar System Watcher:

- Habilitar o deshabilitar la protección contra puntos vulnerables.
- Elegir la acción si se detecta una actividad maliciosa en un programa.
- Activar o desactivar la reversión de acciones de malware durante la desinfección.

Habilitar o deshabilitar la protección contra puntos vulnerables

Para habilitar o deshabilitar la protección contra exploits:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **System Watcher**.

   En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. Realice una de las siguientes acciones:

   - Seleccione la casilla **Habilitar prevención de exploits** si desea que Kaspersky Endpoint Security supervise los archivos utilizados por los programas vulnerables cuando se inicien.

     Si Kaspersky Endpoint Security detecta que un archivo que está siendo usado por un programa vulnerable fue iniciado por algo que no sea el usuario, actuará en función de lo que se seleccione en la lista emergente **Acción al detectar una amenaza**.

   - Seleccione la casilla **Habilitar prevención de exploits** si desea que Kaspersky Endpoint Security supervise los archivos utilizados por los programas vulnerables cuando se inicien.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Elija la acción en caso de que se detecte actividad maliciosa en un programa.

A fin de elegir qué hacer si un programa comienza a realizar actividad maliciosa, realice los siguientes pasos:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **System Watcher**.

   En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. En la sección **Acción al detectar una amenaza** de la lista emergente **Al detectar actividad de malware**, elija la siguiente acción:

   - **Seleccionar acción automáticamente**.
   - **Mover archivo a Cuarentena**.
   - **Finalizar programa malicioso**.
   - **Omitir**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Activación o desactivación de la reversión de acciones de malware durante la desinfección

Para activar o desactivar la reversión de acciones de malware durante la desinfección:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **System Watcher**.

   En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. Realice una de las siguientes acciones:

   - Si desea que Kaspersky Endpoint Security revierta las acciones ocasionadas por un malware en el sistema operativo durante la desinfección, seleccione la casilla de verificación **Revertir acciones ocasionadas por malware durante la desinfección**.
   - Si desea que Kaspersky Endpoint Security ignore las acciones ocasionadas por un malware en el sistema operativo durante la desinfección, desactive la casilla de verificación **Revertir acciones ocasionadas por malware durante la desinfección**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Firewall

Esta sección contiene información acerca del Firewall e instrucciones para configurar los parámetros del componente.

Acerca del Firewall

Durante el uso de redes LAN e Internet, un equipo se expone a virus, otro malware y una variedad de ataques que aprovechan las vulnerabilidades del sistema operativo y del software.

El firewall protege los datos personales almacenados en el equipo del usuario, bloqueando la mayoría de las amenazas al sistema operativo mientras el equipo está conectado a Internet o a la red de área local. El Firewall detecta todas las conexiones de red en el equipo del usuario y provee una lista de direcciones IP, indicando el estado de la conexión de red por defecto.

El componente del Firewall filtra toda la actividad de red según reglas de red. La configuración de reglas de red le permite especificar el nivel deseado de protección del equipo, desde bloquear el acceso a Internet de todas las aplicaciones hasta permitir el acceso ilimitado.

Habilitación o deshabilitación del Firewall

Por defecto, el Firewall está habilitado y funciona en modo óptimo. Si es necesario, puede deshabilitar el Firewall.

Existen dos formas de habilitar o deshabilitar el componente:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

Para habilitar o deshabilitar el Firewall en la ficha Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Protección**.

   Se abre la sección **Protección**.
4. Haga clic con el botón derecho del mouse en la línea **Firewall** para abrir el menú contextual de las acciones del Firewall.
5. Realice una de las siguientes acciones:

   - Para habilitar el Firewall, seleccione **Iniciar** en el menú contextual.

     El ícono de estado del componente , que se muestra a la izquierda en la línea de **Firewall**, cambia al ícono .
   - Para desactivar el Firewall, seleccione **Detener** en el menú contextual.

     El ícono de estado del componente , que se muestra a la izquierda en la línea de **Firewall**, cambia al ícono .

Para habilitar o deshabilitar el Firewall en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Realice una de las siguientes acciones:
   - Para habilitar el Firewall, seleccione la casilla **Habilitar Firewall**.
   - Para deshabilitar el Firewall, seleccione la casilla **Desactivar Firewall**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Acerca de las reglas de red

Las *reglas de red* son acciones permitidas o bloqueadas que el Firewall realiza al detectar un intento de conexión de red.

El Firewall ofrece protección contra ataques de red de diferentes tipos en dos niveles: el nivel de red y el nivel de programa. La protección en el nivel de red se logra aplicando las reglas de paquetes de red. La protección en el nivel de programa se logra aplicando reglas por las cuales las aplicaciones instaladas pueden acceder a los recursos de red.

Según los dos niveles de protección del Firewall, puede crear:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones en los paquetes de red, sin tener en cuenta el programa. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. El Firewall especifica determinadas reglas de paquetes de red de forma predeterminada.
- *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. Dichas reglas hacen posible el ajuste del filtrado de la actividad de red, por ejemplo, cuando un determinado tipo de conexión de red se bloquea para algunas aplicaciones pero se permite para otras.

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.

Puede especificar una prioridad de ejecución para cada regla de paquetes de red y cada regla de red para aplicaciones.

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.

Acerca del estado de la conexión de red

El Firewall controla todas las conexiones de red en el equipo del usuario y automáticamente asigna un estado a cada conexión de red detectada.

La conexión de la red puede presentar uno de los siguientes tipos de estado:

- **Red pública**. Este estado se utiliza en las redes no protegidas por ninguna aplicación Anti-Virus, el Firewall o filtros (en redes de cibercafés, por ejemplo). 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.

  Firewall asigna el estado *Red pública* a Internet, por defecto. No puede cambiar el estado de Internet.

- **Red local**. Este estado se asigna a las redes cuyos usuarios son confiables para tener acceso a los archivos y las impresoras del equipo (LAN o red doméstica, por ejemplo).

- **Red confiable**. Este estado está diseñado para una red segura en la cual el equipo no está expuesto a ataques o intentos no autorizados de acceder a los datos. El Firewall permite cualquier actividad de red dentro de redes con este estado.

Cambio del estado de la conexión de red

Para cambiar el estado de la conexión de red:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Redes disponibles**.

   Se abre la ventana **Firewall**.
4. Seleccione la conexión de red cuyo estado quiera cambiar.
5. En el menú contextual, seleccione el estado de la conexión de red:
   - **Red pública**.
   - **Red local**.
   - **Red confiable**.
6. En la ventana **Firewall**, haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

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 y edición de una regla de paquetes de red

> Al crear reglas de paquetes de red, recuerde que estas tienen prioridad sobre las reglas de red para aplicaciones.

Para crear o editar una regla de paquetes de red:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Firewall**.

3. Haga clic en el botón **Reglas de paquetes de red**.

4. Se abre la ventana **Firewall** en la ficha **Reglas de paquetes de red**.

   Esta ficha muestra una lista de reglas de paquetes de red predeterminados que son establecidas por el Firewall.

5. Realice una de las siguientes acciones:

   - Para crear una nueva regla de paquetes de red, haga clic en el botón **Agregar**.
   - Para editar una regla de paquetes de red, selecciónela en la lista de reglas de paquetes de red y haga clic en el botón **Modificar**.

   Se abre la ventana **Regla de red**.

6. 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**.

7. En el campo **Nombre**, especifique el nombre del servicio de red de alguna de las siguientes maneras:

   - Haga clic en el icono a la derecha del campo **Nombre** y seleccione el nombre del servicio de red en la lista desplegable.

     La lista desplegable incluye servicios de red que definen las conexiones de red de uso más frecuente.

   - Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.

8. Especifique el protocolo de transferencia de datos:

   a. Seleccione la casilla **Protocolo**.

   b. En la lista desplegable, seleccione el tipo de protocolo para el cual se supervisará la actividad de red.

      El Firewall supervisa las conexiones de red que usan los protocolos TCP, UDP, ICMP, ICMPv6, IGMP y GRE.

      Si selecciona un servicio de red de la lista desplegable **Nombre**, la casilla **Protocolo** se selecciona automáticamente y la lista desplegable junto a la casilla se completa con el tipo de protocolo que corresponde al servicio de red seleccionado. De forma predeterminada, la casilla **Protocolo** está desactivada.

9. En la lista desplegable **Sentido**, seleccione la dirección de la actividad de red supervisada.

   El Firewall supervisa conexiones de red con las siguientes direcciones:

   - **Entrante (paquete)**.
   - **Entrante**.
   - **Entrante/Saliente**
   - **Saliente (paquete)**.
   - **Saliente**.

10. Si se selecciona ICMP o ICMPv6 como protocolo, puede especificar el tipo y el código del paquete ICMP:

    a. Seleccione la casilla **Tipo de ICMP** y seleccione el tipo de paquete ICMP en la lista desplegable.

    b. Seleccione la casilla **Código ICMP** y seleccione el código de paquete ICMP en la lista desplegable.

11. Si se selecciona TCP o UDP como el tipo de protocolo, puede especificar los números de puerto como valores separados por comas de los equipos locales y remotos entre los que se supervisará la conexión:

    a. Escriba los puertos del equipo remoto en el campo **Puertos remotos**.

    b. Escriba los puertos del equipo local en el campo **Puertos locales**.

12. En la tabla **Adaptadores de red**, especifique la configuración de los adaptadores de red desde los cuales se pueden enviar paquetes de red o que pueden recibir paquetes de red. Para hacerlo, utilice los botones **Agregar**, **Modificar** y **Eliminar**.

13. Si quiere restringir el control de paquetes de la red según su duración activa (TTL), seleccione la casilla **TTL** y, en el campo adyacente, especifique el rango de valores de la duración activa correspondiente a los paquetes de red entrantes y/o salientes.

    Una regla de red controlará la transmisión de los paquetes de red cuya duración activa no exceda el valor especificado.

    De lo contrario, desmarque la casilla **TTL**.

14. Especifique las direcciones de red de los equipos remotos que pueden enviar o recibir paquetes de red. Para hacerlo, seleccione los siguientes valores en la lista desplegable **Direcciones remotas**:

    - **Cualquier dirección**. La regla de red controla los paquetes de red enviados o recibidos por equipos remotos con cualquier dirección IP.
    - **Direcciones de subred**. La regla de red controla los paquetes de red enviados y/o recibidos por equipos remotos con direcciones IP asociadas al tipo de red seleccionado **Redes confiables**, **Redes locales** o **Redes públicas**.
    - **Direcciones de la lista**. La regla de red controla los paquetes de red enviados o recibidos por equipos remotos con direcciones IP que pueden especificarse en la lista a continuación usando los botones **Agregar**, **Modificar** y **Eliminar**.

15. Especifique las direcciones de red de los equipos con Kaspersky Endpoint Security instalado que pueden enviar y/o recibir paquetes de red. Para hacerlo, seleccione uno de los valores de la lista desplegable **Direcciones locales**:

    - **Cualquier dirección**. La regla de red controla los paquetes de red enviados o recibidos por equipos con Kaspersky Endpoint Security instalada y con cualquier dirección IP.
    - **Direcciones de la lista**. La regla de red controla paquetes de red enviados o recibidos por equipos con Kaspersky Endpoint Security instalada y con direcciones IP que pueden especificarse en la lista a continuación usando los botones **Agregar**, **Modificar** y **Eliminar**.

    En ocasiones, no se podrá obtener una dirección local en el caso de aplicaciones que trabajan con paquetes de red. Cuando sucede esto, se ignora el valor del parámetro **Direcciones locales**.

16. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

17. En la ventana **Regla de red**, haga clic en **Aceptar**.

Si crea una nueva regla de red, dicha regla se muestra en la ficha **Reglas de paquetes de red** de la ventana **Firewall**. Por defecto, la nueva regla de red se coloca al final de la lista de reglas de paquetes de red.

18. En la ventana **Firewall**, haga clic en **Aceptar**.
19. Para guardar los cambios, haga clic en el botón **Guardar**.

Habilitación o deshabilitación de una regla de paquetes de red

Para habilitar o deshabilitar una regla de paquetes de red:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.
   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de paquetes de red**.
   Se abre la ventana **Firewall** en la ficha **Reglas de paquetes de red**.
4. Seleccione la regla de paquetes de red necesaria en la lista.
5. Realice una de las siguientes acciones:
   - Para habilitar la regla, seleccione la casilla junto al nombre de la regla de paquetes de red.
   - Para deshabilitar la regla, desactive la casilla junto al nombre de la regla de paquetes de red.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.
   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de paquetes de red**.
   Se abre la ventana **Firewall** en la ficha **Reglas de paquetes de red**.
4. En la lista, seleccione la regla de paquetes de red cuya acción quiera cambiar.
5. En la columna **Permiso**, haga clic con el botón derecho para mostrar el menú contextual y seleccione la acción que desea asignar:
   - **Permitir**

- **Bloquear**
- **De acuerdo con la regla de la aplicación**
- **Registrar eventos**

6. En la ventana **Firewall**, haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de paquetes de red**.

   Se abre la ventana **Firewall** en la ficha **Reglas de paquetes de red**.
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. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

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 monitorea. 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.

De manera predeterminada, el componente Firewall aplica las reglas de red correspondientes a un grupo de aplicaciones al filtrar la actividad de red de todas las aplicaciones pertenecientes al grupo, de modo similar al componente Control de privilegios de aplicaciones. 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.

Puede realizar las siguientes acciones mientras administra reglas de red para aplicaciones:

- Crear una nueva regla de red para aplicaciones.

  Puede crear una regla de red nueva por la cual el Firewall deba regular la actividad de red de la aplicación o de las aplicaciones que pertenecen al grupo de aplicaciones seleccionado.

- Activar o desactivar una regla de red.

  Todas las reglas de red se agregan a la lista de reglas de red para las aplicaciones con estado *Activado*. Cuando se activa una regla de red, el Firewall la aplica.

  Puede desactivar una regla de red que se creó manualmente. Si se desactiva una regla de red, el Firewall no la aplica temporariamente.

- Cambiar la configuración de una regla de red.

  Luego de crear una nueva regla de red, siempre puede regresar para editar su configuración y modificarla según sea necesario.

- Cambiar la acción del Firewall para una regla de red.

  En la lista de reglas de red, puede editar la acción que realizará el Firewall para la regla de red al detectar actividad de red en esta aplicación o en este grupo de aplicaciones.

- Cambiar la prioridad de una regla de red.

  Puede elevar o disminuir la prioridad de una regla de red personalizada.

- Eliminar una regla de red.

  Puede eliminar una regla de red personalizada para hacer que el Firewall deje de aplicar esta regla de red a la aplicación o al grupo de aplicaciones seleccionado al detectar actividad de red, y para hacer que esta regla deje de aparecer en la lista de reglas de red para aplicaciones.

Creación y edición de una regla de red para aplicaciones

Para crear o editar una regla de red para un grupo de aplicaciones:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.

3. Haga clic en el botón **Reglas de red de aplicaciones**.

   Se abre la ventana **Firewall** en la ficha **Reglas de control de aplicaciones**.

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 **Reglas de aplicaciones** o **Reglas del grupo** según lo que tenga que hacer.

   Se abrirá una de las siguientes ventanas: **Reglas de control de aplicaciones** o **Reglas de control de grupo de aplicaciones**.

6. En la ventana que se abre, seleccione la ficha **Reglas de red**.

7. Realice una de las siguientes acciones:

   - Para crear una nueva regla de red, haga clic en el botón **Agregar**.
   - Para editar una regla de red, selecciónela en la lista de reglas de red y haga clic en el botón **Modificar**.

   Se abre la ventana **Regla de red**.

8. En la lista desplegable **Acción**, seleccione la acción que debe realizar el Firewall al detectar este tipo de actividad de red:

   - **Permitir**
   - **Bloquear**

9. En el campo **Nombre**, especifique el nombre del servicio de red de alguna de las siguientes maneras:

   - Haga clic en el icono a la derecha del campo **Nombre** y seleccione el nombre del servicio de red en la lista desplegable.

     La lista desplegable incluye servicios de red que definen las conexiones de red de uso más frecuente.

   - Ingrese manualmente el nombre del servicio de red en el campo **Nombre**.

10. Especifique el protocolo de transferencia de datos:

    a. Seleccione la casilla **Protocolo**.

    b. En la lista desplegable, seleccione el tipo de protocolo en el que se debe supervisar la actividad de la red.

       El Firewall supervisa las conexiones de red que usan los protocolos TCP, UDP, ICMP, ICMPv6, IGMP y GRE.

       Si selecciona un servicio de red de la lista desplegable **Nombre**, la casilla **Protocolo** se selecciona automáticamente y la lista desplegable junto a la casilla se completa con el tipo de protocolo que corresponde al servicio de red seleccionado. De forma predeterminada, la casilla **Protocolo** está desactivada.

11. En la lista desplegable **Sentido**, seleccione la dirección de la actividad de red supervisada.

    El Firewall supervisa conexiones de red con las siguientes direcciones:

    - **Entrante**.
    - **Entrante/saliente**.

- **Saliente**.

12. Si se selecciona ICMP o ICMPv6 como protocolo, puede especificar el tipo y el código del paquete ICMP:

    a. Seleccione la casilla **Tipo de ICMP** y seleccione el tipo de paquete ICMP en la lista desplegable.

    b. Seleccione la casilla **Código ICMP** y seleccione el código de paquete ICMP en la lista desplegable.

13. Si se selecciona TCP o UDP como el tipo de protocolo, puede especificar los números de puerto como valores separados por comas de los equipos locales y remotos entre los que se supervisará la conexión:

    a. Escriba los puertos del equipo remoto en el campo **Puertos remotos**.

    b. Escriba los puertos del equipo local en el campo **Puertos locales**.

14. Especifique las direcciones de red de los equipos remotos que pueden enviar o recibir paquetes de red. Para hacerlo, seleccione los siguientes valores en la lista desplegable **Direcciones remotas**:

    - **Cualquier dirección**. La regla de red controla los paquetes de red enviados o recibidos por equipos remotos con cualquier dirección IP.
    - **Direcciones de subred**. La regla de red controla los paquetes de red enviados y/o recibidos por equipos remotos con direcciones IP asociadas al tipo de red seleccionado **Redes confiables**, **Redes locales** o **Redes públicas**.
    - **Direcciones de la lista**. La regla de red controla los paquetes de red enviados o recibidos por equipos remotos con direcciones IP que pueden especificarse en la lista a continuación usando los botones **Agregar**, **Modificar** y **Eliminar**.

15. Especifique las direcciones de red de los equipos con Kaspersky Endpoint Security instalado que pueden enviar y/o recibir paquetes de red. Para hacerlo, seleccione uno de los valores de la lista desplegable **Direcciones locales**:

    - **Cualquier dirección**. La regla de red controla los paquetes de red enviados o recibidos por equipos con Kaspersky Endpoint Security instalada y con cualquier dirección IP.
    - **Direcciones de la lista**. La regla de red controla paquetes de red enviados o recibidos por equipos con Kaspersky Endpoint Security instalada y con direcciones IP que pueden especificarse en la lista a continuación usando los botones **Agregar**, **Modificar** y **Eliminar**.

    En ocasiones, no se podrá obtener una dirección local en el caso de aplicaciones que trabajan con paquetes de red. Cuando sucede esto, se ignora el valor del parámetro **Direcciones locales**.

16. Si quiere que las acciones de la regla de red se reflejen en el informe, marque la casilla **Registrar eventos**.

17. En la ventana **Regla de red**, haga clic en **Aceptar**.

    Si creó una nueva regla de red, la regla se muestra en la ficha **Reglas de red**.

18. Haga clic en **Aceptar** en la ventana **Reglas de control de grupo de aplicaciones** si la regla está destinada a un grupo de aplicaciones, o en la ventana **Reglas de control de aplicaciones** si la regla corresponde a una aplicación.

19. En la ventana **Firewall**, haga clic en **Aceptar**.

20. Para guardar los cambios, haga clic en el botón **Guardar**.

Activación y desactivación de una regla de red para aplicaciones

Para activar o desactivar una regla de red para aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de red de aplicaciones**.

   Se abre la ventana **Firewall** en la ficha **Reglas de control de aplicaciones**.
4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el cual quiera activar o desactivar una regla de red.
5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Reglas de aplicaciones** o **Reglas del grupo** según lo que tenga que hacer.

   Se abrirá una de las siguientes ventanas: **Reglas de control de aplicaciones** o **Reglas de control de grupo de aplicaciones**.
6. En la ventana que se abre, seleccione la ficha **Reglas de red**.
7. En la lista de reglas de red para un grupo de aplicaciones, seleccione la regla de red relevante.
8. Realice una de las siguientes acciones:

   - Para activar la regla, seleccione la casilla adyacente al nombre de la regla de red.
   - Para desactivar la regla, desmarque la casilla adyacente al nombre de la regla de red.

   No se puede desactivar una regla de red de un grupo de aplicaciones creada por el Firewall por defecto.
9. Haga clic en **Aceptar** en la ventana **Reglas de control de grupo de aplicaciones** si la regla está destinada a un grupo de aplicaciones, o en la ventana **Reglas de control de aplicaciones** si la regla corresponde a una aplicación.
10. En la ventana **Firewall**, haga clic en **Aceptar**.
11. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de red de aplicaciones**.

   Se abre la ventana **Firewall** en la ficha **Reglas de control de aplicaciones**.
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. En la columna **Red**, haga clic para mostrar el menú contextual y seleccionar la acción que desea asignar:
   - **Heredar**
   - **Permitir**
   - **Bloquear**
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Para cambiar la respuesta del Firewall para una regla de red correspondiente a una aplicación o a un grupo de aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de red de aplicaciones**.

   Se abre la ventana **Firewall** en la ficha **Reglas de control de aplicaciones**.
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 **Reglas de aplicaciones** o **Reglas del grupo** según lo que tenga que hacer.

   Se abrirá una de las siguientes ventanas: **Reglas de control de aplicaciones** o **Reglas de control de grupo de aplicaciones**.
6. En la ventana que se abre, seleccione la ficha **Reglas de red**.
7. Seleccione la regla de red para la cual quiera cambiar la acción del Firewall.
8. En la columna **Permiso**, haga clic con el botón derecho para mostrar el menú contextual y seleccione la acción que desea asignar:
   - **Permitir**
   - **Bloquear**
   - **Registrar eventos**

9. Haga clic en **Aceptar** en la ventana **Reglas de control de grupo de aplicaciones** si la regla está destinada a un grupo de aplicaciones, o en la ventana **Reglas de control de aplicaciones** si la regla corresponde a una aplicación.

10. En la ventana **Firewall**, haga clic en **Aceptar**.

11. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Firewall**.

   En la parte derecha de la ventana, se muestra la configuración del componente Firewall.

3. Haga clic en el botón **Reglas de red de aplicaciones**.

   Se abre la ventana **Firewall** en la ficha **Reglas de control de aplicaciones**.

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 **Reglas de aplicaciones** o **Reglas del grupo** según lo que tenga que hacer.

   Se abrirá una de las siguientes ventanas: **Reglas de control de aplicaciones** o **Reglas de control de grupo de aplicaciones**.

6. En la ventana que se abre, seleccione la ficha **Reglas de red**.

7. Seleccione la regla 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. Haga clic en **Aceptar** en la ventana **Reglas de control de grupo de aplicaciones** si la regla está destinada a un grupo de aplicaciones, o en la ventana **Reglas de control de aplicaciones** si la regla corresponde a una aplicación.

10. En la ventana **Firewall**, haga clic en **Aceptar**.

11. Para guardar los cambios, haga clic en el botón **Guardar**.

Monitor de red

Esta sección contiene información sobre el Monitor de red e instrucciones sobre cómo iniciar el Monitor de red.

Acerca del 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.

Inicio del Monitor de red

Para iniciar el Monitor de red:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Protección**.

   Se abre la sección **Protección**.
4. Haga clic con el botón derecho del mouse en la línea **Firewall** para abrir el menú contextual de las operaciones del Firewall.
5. En el menú contextual, seleccione **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.
   - La ficha **Puertos abiertos** enumera todos los puertos de red del equipo que se encuentran abiertos.
   - 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 Bloqueador de ataques de red después de detectar intentos de ataques de red desde estas direcciones IP.

Bloqueador de ataques de red

Esta sección contiene información acerca del Bloqueador de ataques de red e instrucciones para configurar los parámetros del componente.

Acerca del Bloqueador de ataques de red

El Bloqueador de ataques de red analiza el tráfico de red entrante en busca de actividad típica de 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. Luego, en su pantalla verá una advertencia en la que se le informa que se intentó un ataque de red y se muestra información sobre el equipo atacante.

El tráfico de red proveniente del equipo atacante se bloquea durante una hora. Puede modificar la configuración para bloquear un equipo atacante.

Las descripciones de los tipos de ataques de red actualmente conocidos y de las maneras de combatirlos están disponibles en las bases de datos de Kaspersky Endpoint Security. La lista de ataques de red que detecta el componente Bloqueador de ataques de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación.

Habilitación y deshabilitación del Bloqueador de ataques de red

De forma predeterminada, el Bloqueador de ataques de red está habilitado, funcionando en modo óptimo. Puede deshabilitar el Bloqueador de ataques de red si fuera necesario.

Existen dos formas de habilitar o deshabilitar el componente:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

Para habilitar o deshabilitar el componente Bloqueador de ataques de red, haga lo siguiente en la ficha Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Protección**.

   Se abre la sección **Protección**.
4. Haga clic con el botón derecho del mouse en la línea de **Bloqueador de ataques de red** para ver el menú contextual de las acciones de este componente.
5. Realice una de las siguientes acciones:

   - Para habilitar el componente Bloqueador de ataques de red, seleccione **Iniciar** en el menú contextual.

     El icono de estado del componente que se muestra a la izquierda de la línea **Bloqueador de ataques de red** cambia al icono .
   - Para deshabilitar el componente Bloqueador de ataques de red, seleccione **Detener** en el menú contextual.

El icono de estado del componente que se muestra a la izquierda de la línea **Bloqueador de ataques de red** cambia al icono .

Para habilitar o deshabilitar el componente Bloqueador de ataques de red en la ventana principal de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Bloqueador de ataques de red**.

   La configuración del Bloqueador de ataques de red se muestra en la parte derecha de la ventana.
3. Haga lo siguiente:
   - Para habilitar el Bloqueador de ataques de red, seleccione la casilla **Habilitar Bloqueador de ataques de red**.
   - Para deshabilitar el Bloqueador de ataques de red, desactive la casilla **Habilitar Bloqueador de ataques de red**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del Bloqueador de ataques de red

Puede realizar las siguientes acciones para configurar los parámetros del Bloqueador de ataques de red:

- Configurar los parámetros que se utilizan para bloquear un equipo desde el que se inicia un ataque.
- Generar una lista de direcciones para exclusiones del bloqueo.

Edición de la configuración usada en el bloqueo de un equipo desde el que se inicia un ataque

Para editar la configuración para bloquear un equipo desde el que se inicia un ataque:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Bloqueador de ataques de red**.

   La configuración del Bloqueador de ataques de red se muestra en la parte derecha de la ventana.
3. Seleccione la casilla **Agregar el equipo atacante a la lista de equipos bloqueados durante**.

   Si se selecciona esta casilla, al detectar un intento de ataque de red, el Bloqueador de ataques de red bloquea el tráfico de red desde el equipo atacante durante el tiempo especificado. Esto protege el equipo automáticamente contra posibles ataques de red futuros desde la misma dirección.

   Si se desactiva esta casilla, al detectar un intento de ataque de red, el Bloqueador de ataques de red no habilita una protección automática contra posibles ataques de red futuros desde la misma dirección.
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 el equipo atacante a la lista de equipos bloqueados durante**.

5. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de direcciones de exclusiones del bloqueo

Para configurar direcciones de exclusiones del bloqueo:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Bloqueador de ataques de red**.

   La configuración del Bloqueador de ataques de red se muestra en la parte derecha de la ventana.
3. Haga clic en el botón **Exclusiones**.

   Se abre la ventana **Exclusiones**.
4. Realice una de las siguientes acciones:

   - Si quiere agregar una dirección IP nueva, haga clic en el botón **Agregar**.
   - Si quiere editar una dirección IP ya agregada, selecciónela en la lista de direcciones y haga clic en el botón **Modificar**.

   Se abre la ventana **Dirección IP**.
5. Ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.
6. En la ventana **Dirección IP**, haga clic en **Aceptar**.
7. En la ventana **Exclusiones**, haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

Prevención de ataques BadUSB

Esta sección contiene información sobre el componente Prevención de ataques BadUSB.

Acerca de la Prevención de ataques BadUSB

Algunos virus modifican el firmware de los dispositivos USB para engañar el sistema operativo en lo que respecta a la detección del dispositivo USB como un teclado.

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 la aplicación 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 se encuentra disponible). Este procedimiento se conoce como autorización del teclado. La aplicación permite el uso de un teclado autorizado y bloquea un teclado que no haya sido autorizado.

La Prevención de ataques BadUSB se ejecuta en el modo de segundo plano no bien se instala este componente. Si la aplicación no está sujeta a ninguna directiva de Kaspersky Security Center, puede activar o desactivar la Prevención de ataques BadUSB si suspende temporariamente y reanuda la función de protección y control del equipo.

Instalación del componente de Prevención de ataques BadUSB

Si seleccionó instalación básica o estándar durante la instalación de Kaspersky Endpoint Security, el componente de Prevención de ataques BadUSB no estará disponible. Para instalarlo, debe cambiar el conjunto de componentes de la aplicación.

Para instalar el componente de Prevención de ataques BadUSB:

1. En el menú **Inicio**, seleccione **Aplicaciones → Kaspersky Endpoint Security 10 para Windows → Modificar, Reparar o Quitar.**

   Se inicia el Asistente de instalación.

2. En la ventana **Modificar, Reparar o Eliminar aplicación** del Asistente de instalación, haga clic en el botón **Modificar**.

   Se abre la ventana de **Instalación personalizada** del Asistente de instalación de la aplicación.

3. En el menú contextual del icono adyacente a nombre del componente **Prevención de ataques BadUSB**, seleccione el elemento **La función se instalará en el disco duro local**.

4. Haga clic en **Siguiente**.

5. Siga las instrucciones del Asistente de instalación.

Habilitación y deshabilitación de Prevención de ataques BadUSB

Para habilitar o deshabilitar la Protección de ataques BadUSB:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Prevención de ataques BadUSB**.

   La configuración de Prevención de ataques BadUSB se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:

   - Para habilitar la Prevención de ataques BadUSB, seleccione la casilla **Activar Prevención de ataques BadUSB**.
   - Para deshabilitar la Prevención de ataques BadUSB, anule la selección de la casilla **Activar Prevención de ataques BadUSB**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Permiso y prohibición del uso de teclado en pantalla para autorización

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la subsección **Prevención de ataques BadUSB**.

   Las configuraciones avanzadas del componente se muestran en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:

   - Seleccione la casilla **No permitir el uso del Teclado en pantalla para la autorización** para bloquear el uso del teclado en pantalla para autorización.
   - Desmarque la casilla **No permitir el uso del Teclado en pantalla para la autorización** para permitir el uso del teclado en pantalla para autorización.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Autorización del teclado

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.

La aplicación requiere la autorización del dispositivo USB conectado que ha sido identificado por el sistema operativo como teclado únicamente si la solicitud de autorización del teclado USB se encuentra activada. El usuario no puede usar un teclado no autorizado hasta que esté autorizado.

Si la solicitud de autorización del teclado USB está desactivada, el usuario puede usar todos los teclados conectados. Inmediatamente después de activada la solicitud de autorización del teclado USB, la aplicación presenta una solicitud de autorización para cada teclado no autorizado que se conecta.

Para autorizar un teclado:

1. Con la autorización del teclado USB activada, conecte el teclado a un puerto USB.

   Se abre la ventana **Autorización del teclado <Nombre del teclado>** con detalles del teclado conectado y un código numérico para su autorización.

2. Ingrese el código numérico generado aleatoriamente en la ventana de autorización desde el teclado conectado o desde el teclado en pantalla (si se encuentra disponible).

3. Haga clic en **Aceptar**.

   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.

   > Cuando el teclado autorizado se conecta a un puerto USB diferente del equipo, la aplicación muestra una solicitud de autorización de este teclado nuevamente.

   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.

Control de Inicio de las Aplicaciones

Esta sección contiene información acerca del Control de Inicio de las Aplicaciones e instrucciones para configurar los parámetros del componente.

Acerca del Control de Inicio de las Aplicaciones

El componente Control de Inicio de Aplicaciones supervisa los intentos de los usuarios por iniciar aplicaciones y regula el inicio de aplicaciones usando *reglas de Control de Inicio de las Aplicaciones*.

El inicio de aplicaciones cuyos parámetros no cumplen ninguna de las reglas de Control de Inicio de las Aplicaciones está regulado por el modo de operación seleccionado del componente. *El modo de Lista negra* se selecciona de forma predeterminada. Este modo autoriza a cualquier usuario a iniciar cualquier aplicación.

Todos los intentos de los usuario por iniciar aplicaciones se registran en informes.

Habilitación y deshabilitación del Control de aplicaciones

Aunque el componente Control de aplicaciones está deshabilitado por defecto, puede habilitarlo de ser necesario.

Para habilitar y deshabilitar el Control de aplicaciones, realice lo siguiente:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Controles de seguridad**, seleccione la subsección **Control de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de aplicaciones.
3. Realice una de las siguientes acciones:
   - Si desea habilitar el Control de aplicaciones, seleccione la casilla **Habilitar control de aplicaciones**.
   - Si desea deshabilitar el Control de aplicaciones, desactive la casilla **Habilitar control de aplicaciones**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Limitaciones de la funcionalidad del Control de Inicio de las Aplicaciones

El funcionamiento del componente Control de Inicio de las 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 Inicio de las Aplicaciones.

  Para restaurar la funcionalidad del Control de Inicio de las Aplicaciones, debe volver a configurar los parámetros del componente.

- 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. Si las bases de datos locales no contienen información sobre la aplicación, está no será categorizada en ningún grupo de confianza.

  La categorización de aplicaciones cuando hay una conexión con servidores de KSN puede diferir de su categorización cuando no hay ninguna conexión con 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 del Control de Inicio de las Aplicaciones permiten el inicio de un intérprete, el componente no bloqueará un script iniciado desde este 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:

  - { cCmdLineParser::itCmd, _T("%ComSpec%") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
  - { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };

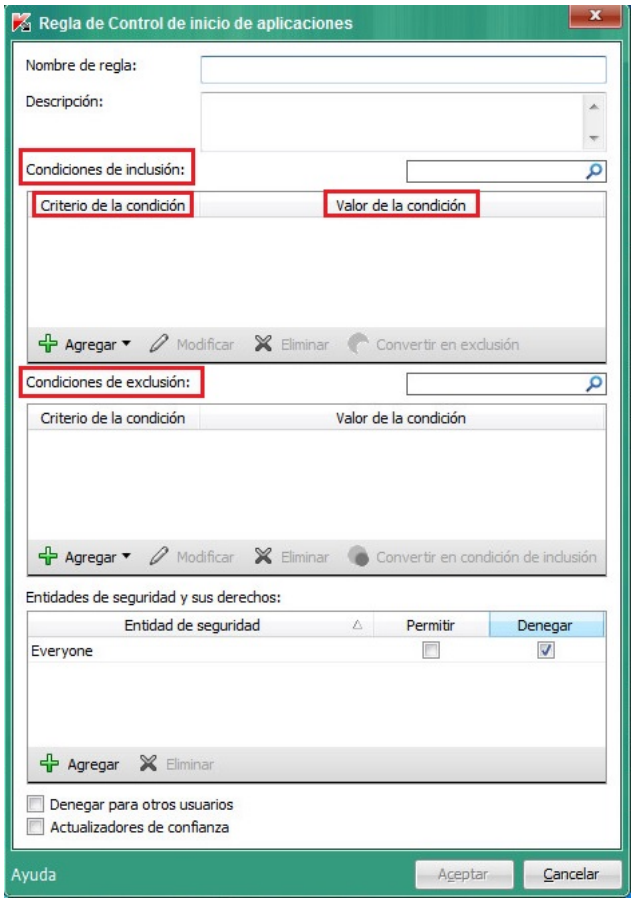
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Acerca de las Regla de control de aplicaciones

Kaspersky Endpoint Security controla el inicio de las aplicaciones por parte de los usuarios mediante reglas. Una regla de Control de aplicaciones especifica las condiciones de activación y la acción llevada a cabo por el componente Control de aplicaciones cuando la regla se activa (lo cual permite o bloquea el inicio de las aplicaciones por parte de los usuarios).

Condiciones de activación de regla

Una condición para activar la regla tiene la siguiente correspondencia: "tipo de condición - criterio de condición - valor de condición" (ver a la figura a continuación). Según las condiciones de activación de la regla, Kaspersky Endpoint Security aplica (o no) una regla a la aplicación.



Regla de control de aplicaciones. Parámetros de la condición de activación de regla

Las reglas utilizan condiciones de inclusión y exclusión:

- *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.

Administración de las reglas de Control de Inicio de las Aplicaciones

Puede realizar las siguientes acciones correspondientes a las reglas de Control de Inicio de las Aplicaciones:

- Agregar una nueva regla
- Crear o cambiar las condiciones para activar una regla
- Editar el estado de la regla

  Una regla de Control de Inicio de las Aplicaciones se puede activar (la casilla frente a la regla está seleccionada) o desactivar (la casilla frente a la regla no está seleccionada). Una regla de Control de Inicio de las Aplicaciones se activa de forma predeterminada después de su creación.
- Eliminar regla

Adición y edición de una regla de Control de Inicio de las Aplicaciones

Para agregar o editar una regla de Control de Inicio de las Aplicaciones:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.

3. Seleccione **Activar Control de Inicio de las Aplicaciones** para hacer que la configuración del componente esté disponible para edición.

4. 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 inicio de aplicaciones**.

5. Especifique o edite la configuración de la regla:

   a. En el campo **Nombre de regla**, escriba o edite el nombre de la regla.

   b. En la tabla **Condiciones de inclusión**, cree o edite la lista de condiciones de inclusión que activan una regla haciendo clic en los botones **Agregar**, **Modificar**, **Eliminar** y **Convertir en exclusión**.

   c. En la tabla **Condiciones de exclusión**, cree o edite la lista de condiciones de exclusión que activan una regla haciendo clic en los botones **Agregar**, **Modificar**, **Eliminar** y **Convertir en condición de inclusión**.

   d. Si es necesario, cambie el tipo de condición de activación de reglas:

      - Para cambiar el tipo de condición de una condición de inclusión a una condición de exclusión, seleccione una condición en la tabla **Condiciones de inclusión** y haga clic en el botón **Convertir en exclusión**.
      - Para cambiar el tipo de condición de una condición de exclusión a una condición de inclusión, seleccione una condición en la tabla **Condiciones de exclusión** y haga clic en el botón **Convertir en condición de inclusión**.

   e. 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 hacer esto, haga clic en el botón **Agregar** en la tabla **Entidades de seguridad y sus derechos**.

      Se abre la ventana **Seleccionar usuarios o grupos** de Microsoft Windows. En esta ventana, puede seleccionar usuarios o grupos de usuarios.

      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.

   f. En la tabla **Entidades de seguridad y sus derechos**, seleccione las casillas **Permitir** o **Bloquear** frente a los usuarios y/o los grupos de usuarios para determinar su derecho a iniciar aplicaciones.

      La casilla que se selecciona de forma predeterminada depende del modo de operación del Control de Inicio de las Aplicaciones.

   g. Seleccione la casilla **Denegar para otros usuarios** si quiere que todos los usuarios que no aparecen en la columna **Entidad de seguridad** y que no forman parte del grupo de usuarios especificados en la columna

Entidad de seguridad estén bloqueados para iniciar aplicaciones que coincidan con las condiciones de activación de las reglas.

> Si se desmarca la casilla **Denegar para otros usuarios**, el Kaspersky Endpoint Security no controlará el inicio de aplicaciones por parte de usuarios que no estén especificados en la tabla **Entidades de seguridad y sus derechos** y que no pertenezcan a los grupos o usuarios especificados en la tabla **Entidades de seguridad y sus derechos**.

h. 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 iniciar otras aplicaciones para las que no se han definido reglas del Control de Inicio de las Aplicaciones, seleccione la casilla **Actualizadores de confianza**.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

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 ventana principal de la aplicación, haga clic en el botón **Configuración**.

2. En la parte izquierda de la ventana, en la sección **Controles de seguridad**, seleccione la subsección **Control de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de aplicaciones.

3. Seleccione la casilla **Control de aplicaciones** para hacer que la configuración del componente esté disponible para edición.

4. Realice una de las siguientes acciones:

   - Si quiere crear una regla nueva y añadirle una condición de activación, haga clic en el botón **Agregar**.
   - Si quiere añadir una condición de activación a una regla existente, seleccione la regla de la lista de reglas y haga clic en el botón **Modificar**.

   Se abre la ventana **Regla de control de aplicaciones**.

5. En la tabla **Condiciones de inclusión** o en la tabla **Condiciones de exclusión**, haga clic en el botón **Agregar**.

Puede utilizar la lista desplegable debajo del botón **Agregar** para agregar diversas condiciones de activación a la regla (consulte las instrucciones que se indican a continuación).

Para añadir una condición de activación de una regla basada en las propiedades de los archivos de una carpeta especificada:

1. En la lista desplegable debajo del botón **Agregar**, seleccione **Condiciones de las propiedades de los archivos de la carpeta especificada**.

Se abre la ventana **Seleccionar carpeta** estándar de Microsoft Windows.

2. En la ventana **Seleccionar carpeta**, seleccione una carpeta que contenga los archivos ejecutables de las aplicaciones cuyas propiedades quiera usar como base para una o varias condiciones de activación de una regla.

3. Haga clic en **Aceptar**.

   Se abre la ventana **Agregar condición**.

4. En la lista desplegable **Mostrar criterio**, seleccione el criterio en función del cual quiera crear una o varias condiciones de activación de la regla: **Código hash de archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a carpeta**.

   Kaspersky Endpoint Security no admite un código 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.

5. Si seleccionó **Metadatos** en la lista desplegable **Mostrar criterio**, seleccione las casillas que se encuentran frente a las propiedades del archivo ejecutable que quiera utilizar en la condición de activación de la regla: **Nombre de archivo**, **Versión de archivo**, **Nombre de la aplicación**, **Versión de la aplicación** y **Proveedor**.

   Si no se selecciona ninguna de las propiedades especificadas, no se podrá guardar la regla.

6. Si seleccionó **Certificado** en la lista desplegable **Mostrar criterio**, seleccione las casillas que se encuentran frente a los ajustes que quiera utilizar en la condición de activación de la regla: **Emisor**, **Sujeto** y **Huella digital**.

   Si no se selecciona ninguno de las ajustes especificados, no se podrá guardar 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.

7. Seleccione las casillas que se encuentran frente a los nombres de los archivos ejecutables de la aplicación cuyas propiedades quiera incluir en las condiciones de activación de la regla.

8. Haga clic en **Siguiente**.

   Aparece una lista de condiciones de activación de reglas formuladas.

9. En la lista de condiciones de activación de reglas formuladas, seleccione las casillas que se encuentran frente a las condiciones de activación de reglas que quiera agregar a la regla de Control de aplicaciones.

10. Haga clic en el botón **Finalizar**.

Para agregar una condición de activación de una regla basada en las propiedades de las aplicaciones en ejecución en el equipo:

1. En la lista desplegable debajo del botón **Agregar**, seleccione **Condiciones de las propiedades de las aplicaciones iniciadas**.

2. En la ventana **Agregar condición** (en la lista desplegable **Mostrar criterio**), seleccione el criterio en función del cual quiera crear una o varias condiciones de activación de reglas: **Código hash de archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a carpeta**.

Kaspersky Endpoint Security no admite un código 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.

3. Si seleccionó **Metadatos** en la lista desplegable **Mostrar criterio**, seleccione las casillas que se encuentran frente a las propiedades del archivo ejecutable que quiera utilizar en la condición de activación de la regla: **Nombre de archivo**, **Versión de archivo**, **Nombre de la aplicación**, **Versión de la aplicación** y **Proveedor**.

   Si no se selecciona ninguna de las propiedades especificadas, no se podrá guardar la regla.

4. Si seleccionó **Certificado** en la lista desplegable **Mostrar criterio**, seleccione las casillas que se encuentran frente a los ajustes que quiera utilizar en la condición de activación de la regla: **Emisor**, **Sujeto** y **Huella digital**.

   Si no se selecciona ninguno de las ajustes especificados, no se podrá guardar 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.

5. Seleccione las casillas que se encuentran frente a los nombres de los archivos ejecutables de la aplicación cuyas propiedades quiera incluir en las condiciones de activación de la regla.

6. Haga clic en **Siguiente**.

   Aparece una lista de condiciones de activación de reglas formuladas.

7. En la lista de condiciones de activación de reglas formuladas, seleccione las casillas que se encuentran frente a las condiciones de activación de reglas que quiera agregar a la regla de Control de aplicaciones.

8. Haga clic en el botón **Finalizar**.

Para añadir una condición de activación de una regla basada en una categoría KL:

1. En la lista desplegable debajo del botón **Agregar**, seleccione **Condición "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.

2. En la ventana **Condiciones "Categoría KL"**, seleccione las casillas que se encuentran al lado de los nombre de las categorías KL en función de las cuales quiera crear condiciones de activación de reglas.

   Puede hacer clic en el botón unfold_key a la izquierda del nombre de la categoría KL para marcar selectivamente las categorías KL anidadas.

3. Haga clic en **Aceptar**.

Para añadir una condición de activación de una regla personalizada:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición personalizada**.

2. En la ventana **Condición personalizada**, haga clic en el botón **Seleccionar** y especifique la ruta al archivo ejecutable de la aplicación.

3. Seleccione el criterio en función del cual quiera crear una condición de activación de la regla: **Código hash de archivo**, **Certificado**, **Metadatos** o **Ruta de acceso a archivo o carpeta**.

Kaspersky Endpoint Security no admite un código 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.

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**.

4. Configure los parámetros del criterio seleccionado.
5. Haga clic en **Aceptar**.

Para añadir una condición de activación de una regla basada en la información sobre la unidad que almacena el archivo ejecutable de una aplicación:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición por unidad de archivo**.
2. En la ventana **Condición por unidad de archivo**, en la lista desplegable **Unidad**, seleccione el tipo de dispositivo de almacenamiento desde el cual el inicio de aplicaciones servirá como una condición de activación de reglas.
3. Haga clic en **Aceptar**.

Edición del estado de una regla de Control de Inicio de las Aplicaciones

Para cambiar el estado de una regla de Control de Inicio de las Aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.
3. Seleccione **Activar Control de Inicio de las Aplicaciones** para hacer que la configuración del componente esté disponible para edición.
4. Seleccione la regla cuyo estado desea editar.
5. En la columna **Estado**, haga lo siguiente:
   - Si desea activar el uso de una regla, marque la casilla que se encuentra frente a la regla.
   - Si desea desactivar el uso de una regla, desmarque la casilla que se encuentra frente a la regla.
6. Para guardar los cambios, haga clic en el botón **Guardar**.

Prueba de las reglas de Control de Inicio de las Aplicaciones

Para asegurarse de que las reglas de Control de Inicio de las Aplicaciones no bloqueen aplicaciones necesarias para el trabajo, se recomienda poner las reglas recién creadas en el modo de prueba y analizar su funcionamiento.

El análisis del funcionamiento de las reglas del Control de Inicio de las Aplicaciones en el modo de prueba incluye revisar los eventos de Control de Inicio de las Aplicaciones informados a Kaspersky Security Center. Si se permite el inicio de todas las aplicaciones necesarias para el trabajo del usuario del equipo, las reglas se han creado correctamente. De lo contrario, le recomendamos que modifique la configuración de las reglas que creó.

El modo de prueba para las reglas del Control de Inicio de las Aplicaciones está desactivado de forma predeterminada.

Para probar reglas de Control de Inicio de las Aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.
3. Seleccione **Activar Control de Inicio de las Aplicaciones** para hacer que la configuración del componente esté disponible para edición.
4. En la lista desplegable **Modo de Control de inicio de aplicaciones**, seleccione uno de los siguientes elementos:

   - **Lista negra**, si quiere permitir el inicio de todas las aplicaciones, salvo por las especificadas en reglas de bloqueo.
   - **Lista blanca**, si quiere bloquear el inicio de todas las aplicaciones, salvo por las especificadas en reglas de autorización.
5. En la lista desplegable **Acción**, seleccione **Notificar**.
6. Para guardar los cambios, haga clic en el botón **Guardar**.

Kaspersky Endpoint Security no bloqueará aplicaciones cuyo inicio no esté permitido por las reglas del Control de Inicio de las Aplicaciones, pero enviará notificaciones sobre su inicio al Servidor de administración.

Edición de las plantillas de mensajes de Control de Inicio de las Aplicaciones

Cuando un usuario intenta iniciar una aplicación bloqueada por una regla de Control de Inicio de las 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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.

3. Seleccione **Activar Control de Inicio de las Aplicaciones** para hacer que la configuración del componente esté disponible para edición.

4. Haga clic en el botón **Plantillas**.

   Se abre la ventana **Plantillas de mensajes**.

5. Realice una de las siguientes acciones:

   - Si quiere modificar la plantilla del mensaje que se muestra cuando el inicio de la aplicación está bloqueado, seleccione la ficha **Bloqueo**.

   - Si quiere modificar la plantilla del mensaje que se envía al administrador de la red LAN, seleccione la ficha **Mensaje para el administrador**.

6. Modifique la plantilla del mensaje que se muestra cuando el inicio de la aplicación está bloqueado o el mensaje que se envía al administrador. Para hacerlo, utilice los botones **Predeterminado** y **Variable**.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Acerca de los modos de operación del Control de Inicio de las Aplicaciones

El componente Control de Inicio de las Aplicaciones funciona en dos modos:

- **Lista negra**. En este modo, el Control de Inicio de las Aplicaciones permite que todos los usuarios inicien todas las aplicaciones, excepto las que se especifican en las reglas de bloqueo del Control de Inicio de las Aplicaciones.

  Este modo de Control de Inicio de las Aplicaciones se habilita por defecto.

- **Lista blanca**. En este modo, el componente Control de Inicio de las Aplicaciones bloquea para todos los usuarios el inicio de todas las aplicaciones, excepto para las aplicaciones que se especifican en las reglas de bloqueo de Control de Inicio de las Aplicaciones.

  Si se configuran completamente las reglas de autorización del Control de Inicio de las 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.

Cada modo tiene dos acciones que se pueden tomar en aplicaciones en ejecución: Kaspersky Endpoint Security puede bloquear el inicio de las aplicaciones o notificar al usuario sobre el inicio de una aplicación que coincide con las condiciones de las reglas del Control de Inicio de las Aplicaciones.

El Control de Inicio de las 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 del Control de Inicio de las Aplicaciones creadas en la Consola de administración de Kaspersky Security Center se basan en categorías de aplicaciones personalizadas, y no en condiciones de inclusión y exclusión como es el caso de la interfaz local de Kaspersky Endpoint Security.

- Recopilación 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 Inicio de las Aplicaciones.

Selección del modo de Control de Inicio de las Aplicaciones

Para seleccionar el modo de Control de Inicio de las Aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.
3. Seleccione **Activar Control de Inicio de las Aplicaciones** para hacer que la configuración del componente esté disponible para edición.
4. En la lista desplegable **Modo de Control de inicio de aplicaciones**, seleccione una de las siguientes opciones:

   - **Lista negra**, si quiere permitir el inicio de todas las aplicaciones, salvo por las especificadas en reglas de bloqueo.
   - **Lista blanca**, si quiere bloquear el inicio de todas las aplicaciones, salvo por las especificadas en reglas de autorización.

     Cuando se selecciona este modo, se crean dos reglas de Control de Inicio de las Aplicaciones de forma predeterminada: **Imagen de oro** y **Actualizadores de confianza**. No puede eliminar estas reglas. No se puede modificar la configuración de estas reglas. Puede activar o desactivar estas reglas si selecciona o desmarca la casilla que se encuentra frente a la regla relevante. De forma predeterminada, la regla **Imagen de oro** está activada, y la regla **Actualizadores de confianza** está desactivada. 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 revertir al uso de estas reglas, lo único que tiene que hacer es seleccionar el modo necesario en la lista desplegable **Modo de Control de Inicio de las Aplicaciones**.
5. En la lista desplegable **Acción**, seleccione la acción que deberá realizar el componente cuando un usuario intente iniciar una aplicación que esté bloqueada por reglas de Control de Inicio de las Aplicaciones.
6. Seleccione la casilla **Supervisar módulos DLL y controladores** 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.

Si la casilla está seleccionada, los módulos DLL y los controladores se supervisan antes de que se inicie Kaspersky Endpoint Security. Para configurar la supervisión posterior de todos los módulos DLL y controladores antes del inicio de la aplicación, reinicie el equipo después de seleccionar la casilla **Supervisar módulos DLL y controladores**. Si no puede reiniciar el equipo, después de seleccionar la casilla **Supervisar módulos DLL y controladores**, puede cargar los módulos DLL y controladores mientras se ejecuta Kaspersky Endpoint Security. En este caso, la supervisión solo entra en vigor para módulos DLL y controladores que se cargan mientras Kaspersky Endpoint Security está en ejecución.

Cuando se supervisan módulos DLL y controladores, no se recomienda usar las reglas de Control de inicio de aplicaciones que se crearon según las categorías KL. La determinación de categorías KL (incluidas en la regla "Sistema operativo y sus componentes") para módulos DLL y controladores puede no funcionar correctamente. En particular, la regla "Sistema operativo y sus componentes" se creó de forma predeterminada y no se distribuye en la ejecución de módulos DLL y controladores. Al activar esta función, es necesario crear reglas de autorización por separado para módulos DLL y controladores. El uso de la función **Controlar DLL y controladores** si no existen las reglas de autorización podría causar inestabilidad en el sistema.

Recomendamos que se active la protección con contraseña para configurar el programa de modo que sea posible desactivar las reglas de autorización que bloquean el inicio de módulos DLL y controladores de importancia crítica sin cambiar la configuración de la directiva de Kaspersky Security Center en el proceso.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Administración de las reglas del Control de Inicio de las Aplicaciones utilizando Kaspersky Security Center

Esta sección contiene información sobre el uso de Kaspersky Security Center para configurar reglas del Control de Inicio de las Aplicaciones y proporciona recomendaciones para utilizar el Control de Inicio de las Aplicaciones de la mejor manera posible.

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 las aplicaciones en la carpeta **Registro de aplicaciones**:*

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Administración de aplicaciones** → **Registro de aplicaciones**.
3. Seleccione una aplicación.
4. En el menú contextual de la aplicación, seleccione **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre de la aplicación>**.

*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**.

   Se abre la ventana **Propiedades: <Nombre de archivo ejecutable>**.

Creación de categorías de aplicaciones

Para mayor comodidad al crear reglas, puede crear categorías de aplicaciones y usarlas cuando cree reglas de Control de Inicio de las Aplicaciones.

Se recomienda crear la categoría "Aplicaciones de trabajo" que cubra el conjunto de aplicaciones estándar que se utilizan en la compañía. Si diferentes grupos de usuarios usan conjuntos de aplicaciones diferentes en su trabajo, se puede crear una categoría de aplicaciones separada para cada grupo de usuario.

Para crear una categoría de aplicación:

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 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.

Creación de reglas del Control de Inicio de las Aplicaciones utilizando Kaspersky Security Center

Para crear una regla de Control de Inicio de las 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.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.

   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.

7. Haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de Control de inicio de aplicaciones**.

8. En la lista desplegable **Categoría**, seleccione la categoría de aplicaciones creada en función de la cual quiera crear una regla.

9. 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. Para hacerlo, haga clic en el botón **Agregar** de la tabla **Entidades de seguridad y sus derechos**.

   Se abre la ventana **Seleccionar usuarios o grupos** estándar de Microsoft Windows. En esta ventana, puede seleccionar usuarios o grupos de usuarios.

10. En la tabla **Entidades de seguridad y sus derechos**:

    - Si quiere permitir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione las casillas **Permitir** que se encuentran frente a esos usuarios.

    - Si no quiere permitir que los usuarios y/o los grupos de usuarios inicien aplicaciones que pertenezcan a la categoría seleccionada, seleccione las casillas **Bloquear** que se encuentran frente a esos usuarios.

11. Seleccione la casilla **Denegar para otros usuarios** si quiere que todos los usuarios que no aparecen en la columna **Entidad de seguridad** y que no forman parte del grupo de usuarios especificados en la columna **Entidad de seguridad** estén bloqueados para iniciar aplicaciones que pertenezcan a la categoría seleccionada.

12. Si quiere que Kaspersky Endpoint Security considere las aplicaciones de la categoría especificada en la regla como actualizadores de confianza con derecho a iniciar otras aplicaciones para las que no se hayan definido reglas del Control de Inicio de las Aplicaciones, seleccione la casilla **Actualizadores de confianza**.

13. Haga clic en **Aceptar**.

14. En la sección **Control de inicio de aplicaciones** de la ventana de propiedades de la directiva, haga clic en el botón **Aplicar**.

Cambio del estado de una regla de Control de Inicio de las Aplicaciones utilizando Kaspersky Security Center

Para cambiar el estado de una regla de Control de Inicio de las 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.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.

   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Control del endpoint**, seleccione la subsección **Control de inicio de aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Inicio de las Aplicaciones.

7. Seleccione la Regla de Control de Inicio de las Aplicaciones cuyo estado quiera cambiar.

8. En la columna **Estado**, realice una de las siguientes acciones:

   - Si desea activar el uso de una regla, marque la casilla que se encuentra frente a la regla.

   - Si desea desactivar el uso de una regla, desmarque la casilla que se encuentra frente a la regla.

9. Haga clic en el botón **Aplicar**.

Control de Privilegios de Aplicaciones

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca de Control de Privilegios de Aplicaciones e instrucciones para configurar los parámetros del componente.

Acerca del Control de Privilegios de Aplicaciones

El Control de Privilegios de Aplicaciones impide que las aplicaciones realicen acciones que pudieran ser peligrosas para el sistema operativo, garantiza el control del acceso a los recursos del sistema operativo y a los datos de identidad.

Este componente controla la actividad de las aplicaciones, incluido el acceso por parte de estas a recursos protegidos (tales como archivos y carpetas, claves del registro) mediante el uso de *Reglas de control de aplicaciones*. Las reglas de control de aplicaciones son un conjunto de restricciones que se aplican a diversas acciones de las aplicaciones en el sistema operativo y a los permisos de acceso a los recursos del equipo.

La actividad de red de las aplicaciones se controla mediante el componente Firewall.

Cuando se inician las aplicaciones por primera vez, el componente Control de Privilegios de Aplicaciones analiza la aplicación y la coloca en un grupo de confianza. Los grupos de confianza definen las reglas de control de aplicaciones que Kaspersky Endpoint Security aplica al controlar la actividad de las aplicaciones.

Recomendamos que participe en Kaspersky Security Network para que el Control de Privilegios de Aplicaciones funcione con mayor efectividad. Los datos obtenidos mediante Kaspersky Security Network le permiten ordenar las aplicaciones en grupos con mayor precisión y aplicar reglas de control de aplicaciones óptimas.

La próxima vez que inicie la aplicación, Control de Privilegios de Aplicaciones verifica la integridad de la aplicación. Si la aplicación no presenta modificaciones, el componente le aplica las reglas de control de aplicaciones vigentes. Si la aplicación presenta modificaciones, Control de Privilegios de Aplicaciones la analiza nuevamente como si se estuviera iniciando por primera vez.

Limitaciones del control de dispositivos de audio y video

Acerca de protección de transmisiones de audio

La protección de transmisiones de audio tiene las siguientes consideraciones especiales:

- Se debe habilitar el componente Prevención contra intrusos para habilitar esta funcionalidad.

- 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 movió la aplicación al grupo **No confiables** o al grupo **Restricción máxima** luego de que la aplicación comenzara a recibir la transmisión de audio, Kaspersky Endpoint Security permitirá que la aplicación reciba la transmisión de audio y no mostrará ninguna notificación.

- Una vez modificados los parámetros de acceso de la aplicación a dispositivos para grabar sonidos (por ejemplo, si se bloqueó el acceso de la aplicación para la recepción de la transmisión de audio en la ventana de configuración de Prevención contra intrusos), se deberá reiniciar esta aplicación para que deje de recibir la transmisión 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.

Consideraciones especiales para el funcionamiento de dispositivos de audio y video durante instalación y actualización de Kaspersky Endpoint Security

Cuando ejecute aplicaciones para grabar o reproducir audio y video por primera vez desde la instalación de Kaspersky Endpoint Security, la reproducción o grabación de audio y video puede interrumpirse. Esto es necesario a fin de activar 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.

Acerca del acceso de las aplicaciones a cámaras 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.

Cámaras web admitidas

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.

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. Puede deshabilitar el componente Prevención contra intrusos si es necesario.

Para habilitar o deshabilitar el componente Prevención contra intrusos:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección avanzada contra amenazas**, seleccione **Prevención contra intrusos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Prevención contra intrusos.
3. En la parte derecha de la ventana, realice una de las siguientes acciones:
   - Seleccione la casilla **Prevención contra intrusos** si desea habilitar el componente Prevención de intrusiones en el host.
   - Desactive la casilla **Prevención contra intrusos** si desea deshabilitar el componente Prevención de intrusiones en el host.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Administración de grupos de confianza de aplicaciones

Cuando se inicia cada aplicación por primera vez, el componente Control de Privilegios de Aplicaciones comprueba la seguridad de la aplicación y la ubica en un grupo 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 un grupo de confianza al que Kaspersky Endpoint Security asigna automáticamente todas las aplicaciones desconocidas. Las aplicaciones que se iniciaron antes que Kaspersky Endpoint Security se mueven automáticamente al grupo de confianza especificado en la ventana **Seleccionar grupo de confianza**.

El componente solo controla la actividad de red de aplicaciones iniciadas antes que Kaspersky Endpoint Security en función de las reglas de red definidas en la configuración del Firewall.

Configuración de los parámetros para asignar aplicaciones a grupos de confianza

Si la participación en Kaspersky Security Network está activada, Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que se inicia la aplicación. En función de la respuesta de KSN, la aplicación se puede mover a un grupo de confianza que difiera del especificado en la configuración de Control de Privilegios de Aplicaciones.

Para configurar los parámetros para la ubicación de aplicaciones en grupos de confianza:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.
3. Si desea colocar de manera automática las aplicaciones que tienen una firma digital de proveedores confiables en el grupo de confianza, seleccione la casilla **Confiar en aplicaciones que tienen firma digital**.

   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.
4. Elija la forma en que desea asignar las aplicaciones desconocidas a grupos de confianza:

   - Para usar el análisis heurístico para asignar aplicaciones desconocidas a grupos de confianza, seleccione la opción **Utilizar análisis heurístico para definir el grupo** y especifique la cantidad de tiempo asignado para analizar la aplicación iniciada en el campo **Tiempo máximo para definir el grupo**.
   - Si desea asignar todas las aplicaciones desconocidas a un determinado grupo de confianza, seleccione la opción **Automáticamente mover al grupo** y seleccione el grupo de confianza correspondiente en la lista desplegable.

     Por razones de seguridad, el grupo **De confianza** no se incluye en los valores del grupo **Automáticamente mover al grupo**.
5. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de un grupo de confianza

Cuando se inicia la aplicación por primera vez, Kaspersky Endpoint Security coloca automáticamente la aplicación en un grupo de confianza. Si es necesario, puede mover la aplicación a otro grupo de confianza manualmente.

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.

Para cambiar el grupo de confianza al que Kaspersky Endpoint Security asignó automáticamente una aplicación cuando se inició por primera vez:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Protección avanzada contra amenazas**, seleccione **Prevención contra intrusos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Prevención contra intrusos.
3. Haga clic en el botón **Aplicaciones**.

   Se abre la ficha **Derechos de aplicaciones** en la ventana **Prevención contra intrusos**.
4. Seleccione la aplicación requerida en la ficha **Derechos de la aplicación**.
5. Realice una de las siguientes acciones:

   - Haga clic con el botón derecho del mouse para abrir el menú contextual de la aplicación. En el menú contextual de la aplicación, seleccione **Mover al grupo → <nombre del grupo>**.
   - Para abrir el menú contextual, haga clic en el vínculo **De confianza/Restricción mínima/Restricción máxima/No confiables**. En el menú contextual, seleccione el grupo de confianza requerido.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Selección de un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security

El componente solo controla la actividad de red de aplicaciones que se iniciaron antes que Kaspersky Endpoint Security. El control se realiza según las reglas de red especificadas en la configuración del Firewall. Para especificar qué reglas de red se deben aplicar a la supervisión de la actividad de red para dichas aplicaciones, debe seleccionar un grupo de confianza.

Para seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Haga clic en el botón **Modificar**.

   Se abre la ventana **Seleccionar grupo de confianza**.

4. Seleccione el grupo de confianza necesario.

5. Haga clic en **Aceptar**.

6. Para guardar los cambios, haga clic en el botón **Guardar**.

Administración de las reglas del Control de Aplicaciones

Por defecto, la actividad de las aplicaciones es controlada por las reglas de control de aplicaciones definidas para el grupo de confianza al que Kaspersky Endpoint Security asignó la aplicación en el primer inicio. Si es necesario, puede modificar las reglas de control de aplicaciones para un grupo de confianza completo, para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza.

Las reglas de control de la aplicación definidas para aplicaciones individuales o grupos de aplicaciones dentro de un grupo de confianza tienen una prioridad mayor que las reglas de control de aplicaciones definidas para un grupo de confianza. En otras palabras, si la configuración de las reglas de control de aplicaciones para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza difiere de la configuración de las del grupo de confianza, el componente Control de Privilegios de Aplicaciones controla la actividad de la aplicación o del grupo de aplicaciones dentro del grupo de confianza según las reglas de control de aplicaciones que son para la aplicación o el grupo de aplicaciones.

Cambio de las reglas de control de aplicaciones para grupos de confianza y grupos de aplicaciones

Las reglas de control de aplicaciones para diferentes grupos de confianza se crean por defecto. La configuración de las reglas de control de grupos de aplicaciones heredan valores de la configuración de las reglas de control de grupos de confianza. Puede modificar las reglas de control de grupos de confianza predeterminadas y las reglas de control de grupos de aplicaciones.

Para modificar las reglas de control de grupos de confianza o las reglas de control de grupos de aplicaciones:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Haga clic en el botón **Aplicaciones**.

   Se abre la ficha **Reglas de control de aplicaciones** en la ventana **Control de privilegios de aplicaciones**.

4. Seleccione el grupo de confianza o el grupo de aplicaciones necesarios.

5. Desde el menú contextual de un grupo de confianza o un grupo de aplicaciones, seleccione **Reglas del grupo**.

   Se abre la ventana **Reglas de control de grupos de aplicaciones**.

6. En la ventana **Reglas de control de grupos de aplicaciones**, realice una de las siguientes acciones:

- Para modificar las reglas de control de grupos de confianza o de grupos de aplicaciones que rigen los derechos del grupo de confianza o del grupo de aplicaciones para obtener acceso al registro del sistema operativo, los archivos de usuario y la configuración de aplicaciones, seleccione la ficha **Archivos y registro del sistema**.

- Para modificar las reglas de control de grupos de confianza o de grupos de aplicaciones que rigen los derechos del grupo de confianza o del grupo de aplicaciones para obtener acceso a los procesos y objetos del sistema operativo, seleccione la ficha **Derechos**.

7. Para el recurso requerido en la columna de la acción correspondiente, haga clic con el botón derecho del mouse para abrir el menú contextual.

8. Desde el menú contextual, seleccione el elemento requerido.

   - **Heredar**
   - **Permitir**
   - **Bloquear**
   - **Registrar eventos**

   Cuando modifica las reglas de control de grupos de confianza, el elemento **Heredar** no está disponible.

9. Haga clic en **Aceptar**.

10. En la ventana **Aplicaciones**, haga clic en **Aceptar**.

11. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de una regla de control de aplicaciones

Por defecto, la configuración de las reglas de control de aplicaciones de las aplicaciones que pertenecen a un grupo de aplicaciones o a un grupo de confianza heredan los valores de configuración de las reglas de control de grupos de confianza. Puede modificar la configuración de las reglas de control de aplicaciones.

Para cambiar una regla de Control de aplicaciones:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Haga clic en el botón **Aplicaciones**.

   Se abre la ficha **Reglas de control de aplicaciones** en la ventana **Control de privilegios de aplicaciones**.

4. Seleccione la aplicación necesaria.

5. Realice una de las siguientes acciones:

- Desde el menú contextual de la aplicación, seleccione **Reglas de aplicaciones**.
- Haga clic en el botón **Adicional** en la esquina inferior derecha de la ficha **Reglas de control de aplicaciones**.

Se abre la ventana **Reglas de control de aplicaciones**.

6. En la ventana **Reglas de control de aplicaciones**, realice una de las siguientes acciones:
   - Para modificar las reglas de control de aplicaciones que rigen los permisos de la aplicación para obtener acceso al registro del sistema operativo, los archivos de usuario y la configuración de la aplicación, seleccione la ficha **Archivos y registro del sistema**.
   - Para modificar las reglas de control de aplicaciones que rigen los permisos de la aplicación para obtener acceso a los objetos y procesos del sistema operativo, seleccione la ficha **Derechos**.
7. Para el recurso requerido en la columna de la acción correspondiente, haga clic con el botón derecho del mouse para abrir el menú contextual.
8. Desde el menú contextual, seleccione el elemento requerido.
   - **Heredar**
   - **Permitir**
   - **Bloquear**
   - **Registrar eventos**
9. Haga clic en **Aceptar**.
10. En la ventana **Aplicaciones**, haga clic en **Aceptar**.
11. Para guardar los cambios, haga clic en el botón **Guardar**.

Desactivación de las descargas y las actualizaciones de las reglas del control de aplicaciones desde la base de datos de Kaspersky Security Network

De forma predeterminada, cuando se detecta información nueva sobre una aplicación en la base de datos de Kaspersky Security Network, Kaspersky Endpoint Security aplica las reglas de control descargadas desde la base de datos de KSN para esta aplicación. Entonces, usted puede modificar manualmente las reglas de control para la aplicación.

Si una aplicación no se encuentra en la base de datos de Kaspersky Security Network cuando se inicia por primera vez, pero la información acerca de esta se agrega más tarde a la base de datos, por defecto Kaspersky Endpoint Security actualiza automáticamente las reglas de control para esta aplicación.

Puede desactivar las descargas de las reglas de control de aplicaciones de la base de datos de Kaspersky Security Network y actualizaciones automáticas de las reglas de control para aplicaciones anteriormente desconocidas.

Para desactivar las descargas y las actualizaciones de las reglas de control de aplicaciones de la base de datos de Kaspersky Security Network:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Anule la selección de la casilla **Actualizar reglas de control para aplicaciones anteriormente desconocidas usando las bases de datos de KSN**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Desactivación de la herencia de las restricciones del proceso principal

La aplicación puede ser iniciada por el usuario o por otra aplicación en ejecución. Cuando la aplicación se inicia por otra aplicación, se crea una secuencia de inicio que consta de procesos principales y secundarios.

Cuando una aplicación intenta obtener acceso a un recurso protegido, el componente Control de Privilegios de Aplicaciones analiza todos los procesos principales de esta aplicación para determinar si estos procesos tienen derecho a acceder al recurso protegido. Se observa la regla de la mínima prioridad: cuando se comparan los permisos de acceso de la aplicación y de los procesos principales, se aplican los permisos con la mínima prioridad a la actividad de la aplicación.

La prioridad de los permisos de acceso es la siguiente:

1. **Permitir** Este permiso de acceso tiene la prioridad mayor.

2. **Bloquear** Este permiso de acceso tiene la prioridad menor.

Este mecanismo impide que una aplicación no confiable o con derechos restringidos utilice una aplicación de confianza para realizar acciones que requieran ciertos privilegios.

Si la actividad de una aplicación se bloquea debido a la ausencia de derechos que se otorgan a un proceso principal, puede modificar estos derechos o desactivar la herencia de las restricciones del proceso principal.

Para desactivar la herencia de las restricciones del proceso principal:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Haga clic en el botón **Aplicaciones**.

   Se abre la ficha **Reglas de control de aplicaciones** en la ventana **Control de privilegios de aplicaciones**.

4. Seleccione la aplicación necesaria.

5. Desde el menú contextual de la aplicación, seleccione **Reglas de aplicaciones**.

   Se abre la ventana **Reglas de control de aplicaciones**.

6. En la ventana **Reglas de control de aplicaciones**, seleccione la ficha **Exclusiones**.

7. Seleccione la casilla **No heredar restricciones del proceso principal (aplicación)**.

8. Haga clic en **Aceptar**.
9. En la ventana **Aplicaciones**, haga clic en **Aceptar**.
10. Para guardar los cambios, haga clic en el botón **Guardar**.

Exclusión de acciones de aplicaciones específicas de las reglas de control de aplicaciones

Para excluir acciones de aplicaciones específicas de las reglas de control de aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.
3. Haga clic en el botón **Aplicaciones**.

   Se abre la ficha **Reglas de control de aplicaciones** en la ventana **Control de privilegios de aplicaciones**.
4. Seleccione la aplicación necesaria.
5. Desde el menú contextual de la aplicación, seleccione **Reglas de aplicaciones**.

   Se abre la ventana **Reglas de control de aplicaciones**.
6. Seleccione la ficha **Exclusiones**.
7. Seleccione las casillas adyacentes a las acciones de aplicaciones que no es necesario supervisar.
8. Haga clic en **Aceptar**.
9. En la ventana **Aplicaciones**, haga clic en **Aceptar**.
10. Para guardar los cambios, haga clic en el botón **Guardar**.

Eliminar reglas de control de aplicaciones desactualizadas

Por defecto, las reglas de control para aplicaciones que no se han iniciado durante 60 días, se eliminan de forma automática. Puede cambiar la duración de almacenamiento de las reglas de control para las aplicaciones no utilizadas o desactivar la eliminación automática de las reglas.

Para eliminar reglas de control de aplicaciones desactualizadas:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Realice una de las siguientes acciones:

   - Si desea que Kaspersky Endpoint Security elimine las reglas de control de aplicaciones no utilizadas, seleccione la casilla **Eliminar reglas de aplicaciones que no se inician por más de** y especifique la cantidad relevante de días.

   - Para desactivar la eliminación automática de las reglas de control de aplicaciones no utilizadas, anule la selección de la casilla **Eliminar reglas de aplicaciones que no se inician por más de**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Protección de los recursos del sistema operativo y los datos de identidad

El Control de Privilegios de Aplicaciones administra los derechos de las aplicaciones para realizar acciones sobre diversas categorías de recursos del sistema operativo y datos de identidad.

Los especialistas de Kaspersky han establecido categorías predefinidas de recursos protegidos. No puede modificar ni eliminar las categorías predefinidas de recursos protegidos o los recursos protegidos que están dentro de estas categorías.

Puede realizar las siguientes acciones:

- Agregar una nueva categoría de recursos protegidos.
- Agregar un nuevo recurso protegido.
- Desactivar la protección de un recurso.

Adición de una categoría de recursos protegidos

Para agregar una nueva categoría de recursos protegidos:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Haga clic en el botón **Recursos**.

   Se abre la ficha **Recursos protegidos** en la ventana **Control de privilegios de aplicaciones**.

4. En la parte izquierda de la ficha **Recursos protegidos**, seleccione la sección o la categoría de recursos protegidos a la que desea agregar una nueva categoría de recursos protegidos.

5. Haga clic en el botón **Agregar** y, en la lista desplegable, seleccione **Categoría**.

Se abre la ventana **Categoría de recursos protegidos**.

6. En la ventana **Categoría de recursos protegidos** que se abre, introduzca el nombre de la nueva categoría de recursos protegidos.

7. Haga clic en **Aceptar**.

   Aparece un nuevo elemento en la lista de categorías de recursos protegidos.

8. En la ventana **Control de privilegios de aplicaciones**, haga clic en **Aceptar**.

9. Para guardar los cambios, haga clic en el botón **Guardar**.

Puede editar o eliminar una categoría de recursos protegidos después de agregarla. Para ello, haga clic en el botón **Modificar** o **Eliminar** en la parte superior izquierda de la ficha **Recursos protegidos**.

Adición de un recurso protegido

Para agregar un recurso protegido:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. Haga clic en el botón **Recursos**.

   Se abre la ficha **Recursos protegidos** en la ventana **Control de privilegios de aplicaciones**.

4. En la parte izquierda de la ficha **Recursos protegidos**, seleccione la categoría de recursos protegidos a la que desea agregar un nuevo recurso protegido.

5. Haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el tipo de recurso que quiera agregar:

   - **Archivo o carpeta**.
   - **Clave del Registro**.

   Se abre la ventana **Recurso protegido**.

6. En la ventana **Recurso protegido**, introduzca el nombre del recurso protegido en el campo **Nombre**.

7. Haga clic en el botón **Examinar**.

8. En la ventana que se abre, especifique la configuración necesaria según el tipo de recurso protegido que desee agregar. Haga clic en **Aceptar**.

9. En la ventana **Recurso protegido**, haga clic en **Aceptar**.

   En la lista de recursos protegidos de la categoría seleccionada en la ficha **Recursos protegidos**, aparece un nuevo elemento.

10. En la ventana **Control de privilegios de aplicaciones**, haga clic en **Aceptar**.

11. Para guardar los cambios, haga clic en el botón **Guardar**.

Puede editar o eliminar recursos protegidos después de agregarlos. Para ello, haga clic en el botón **Modificar** o **Eliminar** en la parte superior izquierda de la ficha **Recursos protegidos**.

Desactivación de la protección de recursos

Para desactivar la protección de recursos:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Privilegios de Aplicaciones**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de Privilegios de Aplicaciones.

3. En la parte derecha de la ventana, haga clic en el botón **Recursos**.

   Se abre la ficha **Recursos protegidos** en la ventana **Control de privilegios de aplicaciones**.

4. Realice una de las siguientes acciones:

   - En la parte izquierda de la ventana, en la lista de recursos protegidos, seleccione el recurso para el que desea desactivar la protección y desmarque la casilla ubicada junto a su nombre.

   - Haga clic en **Exclusiones** y realice los pasos siguientes:

     a. En la ventana **Exclusiones**, haga clic en el botón **Agregar**. En la lista desplegable, seleccione el tipo de recurso que quiera agregar a la lista de exclusiones de la protección del componente Control de Privilegios de Aplicaciones: **Archivo o carpeta** o **Clave del Registro**.

        Se abre la ventana **Recurso protegido**.

     b. En la ventana **Recurso protegido**, introduzca el nombre del recurso protegido en el campo **Nombre**.

     c. Haga clic en el botón **Examinar**.

     d. En la ventana que se abre, especifique la configuración necesaria según el tipo de recurso protegido que desea agregar a la lista de exclusiones de protección del componente Control de Privilegios de Aplicaciones.

     e. Haga clic en **Aceptar**.

     f. En la ventana **Recurso protegido**, haga clic en **Aceptar**.

        Aparecerá un nuevo elemento en la lista de recursos excluidos de la protección del componente Control de Privilegios de Aplicaciones.

        Una vez agregado un recurso a la lista de exclusiones de protección del componente Control de Privilegios de Aplicaciones, se lo puede editar o eliminar. Para ello, haga clic en el botón **Modificar** o **Eliminar** en la parte superior de la ventana **Exclusiones**.

g. En la ventana **Exclusiones**, haga clic en **Aceptar**.

5. En la ventana **Control de privilegios de aplicaciones**, haga clic en **Aceptar**.

6. Para guardar los cambios, haga clic en el botón **Guardar**.

Monitor de vulnerabilidades

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información sobre el Monitor de vulnerabilidades e instrucciones sobre cómo para activar o desactivar el componente.

Acerca del Monitor de vulnerabilidades

El componente Monitor de vulnerabilidades ejecuta un análisis de vulnerabilidades en tiempo real de las aplicaciones que se ejecutan en el equipo del usuario y que inicia el usuario. Cuando el componente Monitor de vulnerabilidades está habilitado, no es necesario iniciar la tarea Análisis de vulnerabilidades. Este análisis es relevante si nunca se ha ejecutado una tarea de Análisis de vulnerabilidades para las aplicaciones instaladas en el equipo del usuario o si se ejecutó hace mucho tiempo.

Activación y desactivación del Monitor de vulnerabilidades

El componente Monitor de vulnerabilidades está deshabilitado de manera predeterminada. Si es necesario, puede habilitar el Monitor de vulnerabilidades.

Existen dos formas de habilitar o deshabilitar el componente:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

Para habilitar o deshabilitar el Monitor de vulnerabilidades en la ficha Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Control del endpoint**.

   Se abre la sección **Control del endpoint**.
4. Haga clic con el botón derecho del mouse para mostrar el menú contextual de la línea con información acerca del componente Monitor de vulnerabilidades.

   Se abre un menú para seleccionar acciones del componente.
5. Realice una de las siguientes acciones:

   - Para habilitar el Monitor de vulnerabilidades, seleccione **Iniciar**.

     El icono de estado del componente , que se muestra a la izquierda de la línea **Monitor de vulnerabilidades**, cambia al icono.

- Para deshabilitar el Monitor de vulnerabilidades, seleccione **Detener**.

  El icono de estado del componente , que se muestra a la izquierda de la línea **Monitor de vulnerabilidades**, cambia al icono.

Para habilitar o deshabilitar el Monitor de vulnerabilidades en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione **Monitor de vulnerabilidades**.

   En la parte derecha de la ventana, se muestra la configuración del componente Monitor de vulnerabilidades.
3. En la parte derecha de la ventana, realice una de las siguientes acciones:

   - Si desea que Kaspersky Endpoint Security inicie un análisis de vulnerabilidades en las aplicaciones que se ejecutan en el equipo del usuario o que inicia el usuario, seleccione la casilla **Habilitar el Monitor de vulnerabilidades**.

   - Si no desea que Kaspersky Endpoint Security inicie un análisis de vulnerabilidades en las aplicaciones que se ejecutan en el equipo del usuario o que inicia el usuario, desactive la casilla **Habilitar el Monitor de vulnerabilidades**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Control de dispositivos

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca del Control de dispositivos e instrucciones para configurar los parámetros del componente.

Acerca del Control de dispositivos

El Control de dispositivos garantiza la seguridad de los datos confidenciales porque restringe el acceso a los dispositivos instalados en el equipo o conectados al equipo, a saber:

- Dispositivos de almacenamiento de datos (discos duros, discos extraíbles, unidades de cinta, unidades de CD/DVD)
- Herramientas de transferencia de datos (módems, tarjetas de red externas)
- Dispositivos diseñados para convertir datos en copias impresas (impresoras)
- Buses de conexión (también llamados simplemente "buses"), es decir, interfaces para conectar dispositivos a equipos (tales como USB, FireWire y tecnologías infrarrojas)

El Control de dispositivos administra el acceso de los usuarios a los dispositivos mediante la aplicación de reglas de acceso a dispositivos (también llamadas "reglas de acceso") y *reglas de acceso a buses de conexión* (también llamadas "reglas de acceso a buses").

Habilitación y deshabilitación del Control de dispositivos

Por defecto, el Control de dispositivos está habilitado. Si es necesario, puede deshabilitar el Control de dispositivos.

Existen dos formas de habilitar o deshabilitar el componente:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

*Para activar o desactivar el complemento Control de dispositivos en la ficha **Protección y control** de la ventana principal de la aplicación, realice lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Control del endpoint**.

   Se abre la sección **Control del endpoint**.

4. Haga clic con el botón derecho para mostrar el menú contextual de la línea con información acerca del componente Control de dispositivos.

   Se abre un menú para seleccionar acciones del componente.

5. Realice una de las siguientes acciones:

   - Para habilitar el Control de dispositivos, seleccione **Iniciar** en el menú.
   - Para deshabilitar el Control de dispositivos, seleccione **Detener** en el menú.

Para habilitar o deshabilitar el Control de dispositivos en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. Realice una de las siguientes acciones:

   - Si desea habilitar el Control de dispositivos, active la casilla **Habilitar Control de dispositivos**.
   - Si desea deshabilitar el Control de dispositivos, desactive la casilla **Habilitar Control de dispositivos**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Acerca de las reglas de acceso a los dispositivos y a los buses de conexión

Una regla de acceso a dispositivos es una combinación de parámetros que define las siguientes funciones del componente Control de dispositivos:

- Permitir a usuarios o grupos de usuarios seleccionados acceder a tipos de dispositivos específicos durante períodos de tiempo específicos.

  Puede seleccionar un usuario o grupos de usuarios y crear una programación de acceso a dispositivos para ellos.

- Configurar el permiso para leer el contenido de dispositivos de memoria.
- Configurar el permiso para editar el contenido de dispositivos de memoria.

Por defecto, las reglas de acceso se crean para todos los tipos de dispositivos en la clasificación del componente Control de dispositivos. Estas reglas les otorgan acceso completo a todos los usuarios a los dispositivos en todo momento si está habilitado el acceso a los buses de conexión de los tipos respectivos de dispositivos.

La regla de acceso a buses de conexión permite o bloquea el acceso al bus de conexión.

Por defecto, se crean reglas que permiten el acceso a los buses para todos los buses de conexión incluidos en la clasificación del componente Control de dispositivos.

No puede crear ni eliminar reglas de acceso a dispositivos o buses de conexión; solo puede editarlas.

Acerca de los dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

Las siguientes acciones están disponibles para trabajar con los dispositivos de confianza:

- Agregar un dispositivo a la lista de dispositivos de confianza.
- Cambiar el usuario o grupo de usuarios que tienen permiso para acceder al dispositivo de confianza.
- Eliminar un dispositivo a la lista de dispositivos de confianza.

Si agregó un dispositivo a la lista de dispositivos de confianza y creó una regla de acceso para este tipo de dispositivo que bloquea o restringe el acceso, Kaspersky Endpoint Security decide si otorga o no acceso al dispositivo según su inclusión en la lista de dispositivos de confianza. La inclusión en la lista de dispositivos de confianza tiene prioridad sobre una regla de acceso.

Decisiones estándares sobre el acceso a dispositivos

Kaspersky Endpoint Security decide si permitirá el acceso a un dispositivo después de que el usuario conecta el dispositivo al equipo.

Decisiones estándares sobre el acceso a dispositivos

Número	Condiciones iniciales	Pasos provisionales hasta que se tome una decisión sobre el acceso al dispositivo			Decisión sobre el acceso al dispositivo
		Comprobación de si el dispositivo se incluye en la lista de dispositivos de confianza	Prueba de acceso al dispositivo según la regla de acceso	Prueba de acceso al bus según la regla de acceso al bus	
1	El dispositivo no se encuentra en la clasificación del dispositivo del componente Control de dispositivos.	No incluido en la lista de dispositivos de confianza.	Sin regla de acceso.	No sujeto a análisis.	Acceso permitido.
2	El dispositivo es de confianza.	Incluido en la lista de dispositivos de confianza.	No sujeto a análisis.	No sujeto a análisis.	Acceso permitido.
3	El acceso al dispositivo está permitido.	No incluido en la lista de dispositivos de confianza.	Acceso permitido.	No sujeto a análisis.	Acceso permitido.

4	El acceso al dispositivo depende del bus.	No incluido en la lista de dispositivos de confianza.	El acceso depende del bus.	Acceso permitido.	Acceso permitido.
5	El acceso al dispositivo depende del bus.	No incluido en la lista de dispositivos de confianza.	El acceso depende del bus.	Acceso bloqueado.	Acceso bloqueado.
6	El acceso al dispositivo está permitido. No se encuentra una regla de acceso al bus.	No incluido en la lista de dispositivos de confianza.	Acceso permitido.	Sin regla de acceso al bus.	Acceso permitido.
7	El acceso al dispositivo está bloqueado.	No incluido en la lista de dispositivos de confianza.	Acceso bloqueado.	No sujeto a análisis.	Acceso bloqueado.
8	No se encuentra una regla de acceso al dispositivo ni regla de acceso al bus.	No incluido en la lista de dispositivos de confianza.	Sin regla de acceso.	Sin regla de acceso al bus.	Acceso permitido.
9	No hay regla de acceso al dispositivo.	No incluido en la lista de dispositivos de confianza.	Sin regla de acceso.	Acceso permitido.	Acceso permitido.
10	No hay regla de acceso al dispositivo.	No incluido en la lista de dispositivos de confianza.	Sin regla de acceso.	Acceso bloqueado.	Acceso bloqueado.

Puede editar la regla de acceso a dispositivos después de que conecte el dispositivo. Si el dispositivo está conectado y la regla de acceso permite acceder, pero más tarde se edita la regla y se bloquea el acceso, Kaspersky Endpoint Security bloqueará el acceso la próxima vez que se solicite cualquier operación de archivo desde el dispositivo (visualización del árbol de carpetas, lectura, escritura). 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.

Edición de una regla de acceso a dispositivos

Según el tipo de dispositivo, puede modificar diversos parámetros de acceso, como la lista de usuarios que reciben el acceso al dispositivo, la programación del acceso y el acceso permitido/bloqueado.

Para editar una regla de acceso a dispositivos:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. En la parte derecha de la ventana, seleccione la ficha **Tipos de dispositivos**.

   La ficha **Tipos de dispositivos** contiene reglas de acceso para todos los dispositivos incluidos en la clasificación del componente Control de dispositivos.
4. Seleccione la regla de acceso que desea editar.

5. Haga clic en el botón **Modificar**. Este botón está disponible solamente para los tipos de dispositivos que tienen un sistema de archivos.

   Se abre la ventana **Configuración de regla de acceso a dispositivos**.

   Por defecto, una regla de acceso a dispositivos otorga a todos los usuarios acceso completo al tipo de dispositivos especificado en cualquier momento. En la lista de **Usuarios o grupos de usuarios**, esta regla de acceso contiene el grupo **Todo**. En la tabla **Derechos del grupo de usuarios seleccionado según programaciones de acceso**, esta regla de acceso contiene la **Programación predeterminada** para acceder a los dispositivos, con los derechos para realizar todo tipo de operaciones con los dispositivos.

6. Edite la configuración de la regla de acceso a dispositivos:

   a. Seleccione un usuario o grupo de usuarios desde la lista **Usuarios o grupos de usuarios**.

      Para editar la lista **Usuarios o grupos de usuarios**, use los botones **Agregar**, **Modificar** y **Eliminar**.

   b. En la tabla **Derechos del grupo de usuarios seleccionado según programaciones de acceso**, configure la programación para el acceso a dispositivos para el usuario o grupo de usuarios seleccionados. Para hacer esto, seleccione las casillas junto a los nombres de las programaciones de acceso para los dispositivos que desea usar en la regla de acceso a dispositivos que se va a editar.

      Para editar la lista de programaciones de acceso a dispositivos, use los botones **Crear**, **Modificar**, **Copiar** y **Eliminar** en la tabla **Derechos del grupo de usuarios seleccionado según programaciones de acceso**.

   c. Para cada programación para el acceso a dispositivos que se utilice en la regla que se esté editando, especifique las operaciones que se permiten al trabajar con los dispositivos. Para hacer esto, en la tabla **Derechos del grupo de usuarios seleccionado según programaciones de acceso**, seleccione las casillas en las columnas con los nombres de las operaciones relevantes.

   d. Haga clic en **Aceptar**.

   Después de editar los parámetros predeterminados de una regla de acceso a los dispositivos, el parámetro para acceder al tipo de dispositivo que aparezca en la columna **Acceso** de la tabla de la ficha **Tipos de dispositivos** se convierte en el valor *Restringir por reglas*.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Adición o exclusión de registros en el registro de eventos

El registro de eventos solo está disponible para operaciones con archivos en discos extraíbles.

Para activar o desactivar el registro de eventos:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, seleccione la ficha **Tipos de dispositivos**.

   La ficha **Tipos de dispositivos** contiene reglas de acceso para todos los dispositivos incluidos en la clasificación del componente Control de dispositivos.

4. Seleccione **Unidades extraíbles** en la tabla de dispositivos.

El botón **Seguimiento** se vuelve disponible en la parte superior de la tabla.

5. Haga clic en el botón **Seguimiento**.

   Esto abre la ventana **Configuración de seguimiento**.

6. Realice una de las siguientes acciones:

   - Si desea activar el registro de la eliminación de archivos y operaciones de escritura en discos extraíbles, seleccione la casilla **Habilitar seguimiento**.

     Kaspersky Endpoint Security guardará un evento en el archivo de registro y enviará un mensaje al Servidor de administración de Kaspersky Security Center cada vez que el usuario ejecute operaciones de escritura o eliminación con archivos en discos extraíbles.

   - De lo contrario, desmarque la casilla **Habilitar seguimiento**.

7. Especifique qué operaciones se deben registrar. Para ello, realice una de las siguientes acciones:

   - Si quiere que Kaspersky Endpoint Security registre todos los eventos, seleccione la casilla **Guardar la información sobre todos los archivos**.

   - Si quiere que Kaspersky Endpoint Security solo registre información sobre archivos de un formato específico, en la sección **Filtro en los formatos de archivo**, seleccione las casillas que se encuentran frente a los formatos de archivo relevantes.

8. Especifique qué acciones de los usuarios de Kaspersky Endpoint Security se deben registrar como eventos. Para hacerlo:

   a. En la sección **Usuarios**, haga clic en el botón **Seleccionar**.

      Se abre la ventana **Seleccionar usuarios o grupos** estándar de Microsoft Windows.

   b. Especifique o modifique la lista de usuarios y/o grupos de usuarios.

   Cuando los usuarios especificados en la sección **Usuarios** escriban en archivos ubicados en discos extraíbles o eliminen archivos de discos 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.

9. En la ventana **Configuración de seguimiento**, haga clic en **Aceptar**.

10. Para guardar los cambios, haga clic en el botón **Guardar**.

Puede ver eventos asociados con archivos en discos 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.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. En la parte derecha de la ventana, seleccione la ficha **Tipos de dispositivos**.

   La ficha **Tipos de dispositivos** contiene reglas de acceso para todos los dispositivos incluidos en la clasificación del componente Control de dispositivos.
4. En la columna **Acceso** que se encuentra frente al dispositivo **Wi-Fi**, haga clic con el botón derecho del mouse para abrir el menú contextual.
5. Seleccione la opción **Bloquear con excepciones**.
6. En la lista de dispositivos, seleccione **Wi-Fi** y haga clic en el botón **Modificar**.

   Se abre la ventana **Redes Wi-Fi confiables**.
7. Haga clic en el botón **Agregar**.

   Se abre la ventana **Red Wi-Fi confiable**.
8. En la ventana **Red Wi-Fi confiable**:
   - En el campo **Nombre de red**, especifique el nombre de la red Wi-Fi que quiera agregar a la lista de confianza.
   - En la lista desplegable **Tipo autenticación**, seleccione el tipo de autenticación que se utiliza al conectarse a la red Wi-Fi de confianza.
   - 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.
   - 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.
9. En la ventana **Red Wi-Fi confiable**, haga clic en **Aceptar**.
10. En la ventana **Redes Wi-Fi confiables**, haga clic en **Aceptar**.

Edición de una regla de acceso a buses de conexión

Para editar una regla de acceso a buses de conexión:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. Seleccione la ficha **Buses de conexión**.

La ficha **Buses de conexión** muestra las reglas de todos los buses de conexión que están clasificados en el componente Control de dispositivos.

4. Seleccione el bus de conexión que desea editar.
5. Cambie el valor del parámetro de acceso:
   - Para permitir el acceso a un bus de conexión, haga clic en la columna **Acceso** para abrir el menú contextual y seleccione **Permitir**.
   - Para bloquear el acceso a un bus de conexión, haga clic en la columna **Acceso** para abrir el menú contextual y seleccione **Bloquear**.
6. Para guardar los cambios, haga clic en el botón **Guardar**.

Acciones con dispositivos de confianza

Esta sección contiene información sobre las acciones con dispositivos de confianza.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. En la parte derecha de la ventana, seleccione la ficha **Dispositivos de confianza**.
4. Haga clic en el botón **Seleccionar**.

   Se abre la ventana **Seleccionar dispositivos de confianza**.
5. Seleccione la casilla junto al nombre de un dispositivo que desea agregar a la lista de dispositivos de confianza.

   La lista en la columna **Dispositivos** depende del valor que se selecciona en la lista desplegable **Mostrar dispositivos conectados**.
6. Haga clic en el botón **Seleccionar**.

   Se abre la ventana **Seleccionar usuarios o grupos** de Microsoft Windows.
7. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o grupos de usuarios para los cuales Kaspersky Endpoint Security reconoce los dispositivos seleccionados como de confianza.

   Los nombres de los usuarios o los grupos de usuarios especificados en la ventana **Seleccione usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Autorizar a usuarios o grupos de usuarios**.

8. En la ventana **Seleccionar dispositivos de confianza**, haga clic en **Aceptar**.

   En la tabla, en la ficha **Dispositivos de confianza** de la ventana de configuración del componente **Control de dispositivos**, aparece una línea y muestra los parámetros del dispositivo de confianza que se ha agregado.

9. Repita los pasos 4 a 7 para cada dispositivo que desee agregar a la lista de dispositivos de confianza para los usuarios o los grupos de usuarios especificados.

10. Para guardar los cambios, haga clic en el botón **Guardar**.

Añadir dispositivos a la lista De confianza basados en modelos de dispositivos o identificadores

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 dispositivos a la lista De confianza basados en modelos de dispositivos o identificadores:

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 para el cual desea crear una lista de dispositivos de confianza.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.

   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Control del endpoint**, seleccione la subsección **Control de dispositivos**.

7. En la parte derecha de la ventana, seleccione la ficha **Dispositivos de confianza**.

8. Haga clic en el botón **Agregar**.

   Se abre el menú contextual del botón.

9. En el menú contextual del botón **Agregar**, realice una de las siguientes acciones:

   - Seleccione el botón **Dispositivos por id** si desea seleccionar dispositivos con identificadores únicos conocidos a agregar a la lista de dispositivos de confianza.

   - Seleccione el elemento de **Dispositivos por modelo** que desea añadir a la lista de aquellos dispositivos de confianza de los cuales se conoce VID (identificador del proveedor) y PID (identificador del producto).

10. En la ventana que se abre, en la lista desplegable **Tipo de dispositivo** seleccione el tipo de dispositivos a mostrar en la tabla a continuación.

11. Haga clic en el botón **Actualizar**.

La tabla muestra una lista de dispositivos para los que se conocen los identificadores y/o modelos de dispositivos y que pertenecen al tipo seleccionado en la lista desplegable **Tipo de dispositivo**.

12. Seleccione las casillas junto a los nombres de los dispositivos que desea añadir a la lista de dispositivos de confianza.

13. Haga clic en el botón **Seleccionar**.

    Se abre la ventana **Seleccionar usuarios o grupos** de Microsoft Windows.

14. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o grupos de usuarios para los cuales Kaspersky Endpoint Security reconoce los dispositivos seleccionados como de confianza.

    Los nombres de los usuarios o los grupos de usuarios especificados en la ventana **Seleccione usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Autorizar a usuarios o grupos de usuarios**.

15. Haga clic en **Aceptar**.

    Aparecen líneas con los parámetros de los dispositivos de confianza que se han añadido a fin de que aparezcan en la tabla de la ficha **Dispositivos de confianza**.

16. Haga clic en **Aceptar** o **Aplicar** para guardar los cambios.

Añadir dispositivos a la lista De confianza basados en la máscara del identificador del dispositivo

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).

Solo se pueden agregar dispositivos a la lista De confianza basados en la máscara de su identificador en la Consola de administración de Kaspersky Security Center.

Para añadir dispositivos a la lista De confianza basados en la máscara del identificador del dispositivo:

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 para el cual desea crear una lista de dispositivos de confianza.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.

   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Control del endpoint**, seleccione la subsección **Control de dispositivos**.

7. En la parte derecha de la ventana, seleccione la ficha **Dispositivos de confianza**.

8. Haga clic en el botón **Agregar**.

   Se abre el menú contextual del botón.

9. En el menú contextual del botón **Agregar**, seleccione el objeto **Dispositivos por máscara de id**.

   Se abre la ventana **Añadir dispositivos de confianza por máscara de id.**

10. En la ventana **Añadir dispositivos de confianza por máscara de id.**, ingrese la máscara para el identificador del dispositivo en el campo **Máscara**.

11. Haga clic en el botón **Seleccionar**.

    Se abre la ventana **Seleccionar usuarios o grupos** de Microsoft Windows.

12. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o grupos de usuarios para los cuales Kaspersky Endpoint Security reconoce como de confianza a los dispositivos cuyo modelo o identificador coincide con la máscara especificada.

    Los nombres de los usuarios o los grupos de usuarios especificados en la ventana **Seleccione usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Autorizar a usuarios o grupos de usuarios**.

13. Haga clic en **Aceptar**.

    En la tabla en la ficha **Dispositivos de confianza** de la ventana de configuración del componente **Control de Dispositivos**, aparece una línea con las características de la regla para agregar dispositivos a la lista de dispositivos de confianza por la máscara de sus identificadores.

14. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del acceso del usuario a un dispositivo de confianza

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). Puede configurar el acceso de usuarios (o grupos de usuarios) a un dispositivo de confianza.

Para configurar el acceso del usuario a un dispositivo de confianza:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, seleccione la ficha **Dispositivos de confianza**.

4. En la lista de dispositivos de confianza, seleccione un dispositivo para el cual desea editar las reglas de acceso.

5. Haga clic en el botón **Modificar**.

   Se abre la ventana **Configuración de regla de acceso al dispositivo de confianza**.

6. Haga clic en el botón **Seleccionar**.

   Se abre la ventana **Seleccionar usuarios o grupos** de Microsoft Windows.

7. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o grupos de usuarios para los cuales Kaspersky Endpoint Security reconoce los dispositivos seleccionados como de confianza.

8. Haga clic en **Aceptar**.

   Los nombres de los usuarios o los grupos de usuarios especificados en la ventana **Seleccionar usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Autorizar a usuarios o grupos de usuarios** de la ventana **Configuración de regla de acceso al dispositivo de confianza**.

9. Haga clic en **Aceptar**.

10. Para guardar los cambios, haga clic en el botón **Guardar**.

Eliminación de un dispositivo de la lista de dispositivos de confianza

Para eliminar un dispositivo de la lista de dispositivos de confianza:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, seleccione la ficha **Dispositivos de confianza**.

4. Seleccione el dispositivo que desea eliminar de la lista de dispositivos de confianza.

5. Haga clic en el botón **Eliminar**.

6. Para guardar los cambios, haga clic en el botón **Guardar**.

Kaspersky Endpoint Security toma una decisión sobre el acceso al dispositivo eliminado de la lista de dispositivos de confianza según las reglas de acceso a dispositivos y de acceso a buses de conexión.

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. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control de Dispositivos**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, haga clic en el botón **Plantillas**.

   Se abre la ventana **Plantillas de mensajes**.

4. Realice una de las siguientes acciones:

   - Para modificar la plantilla del mensaje sobre acceso bloqueado a un dispositivo o una operación prohibida con contenido del dispositivo, seleccione la ficha **Bloqueo**.
   - Para modificar la plantilla del mensaje que se envía al administrador de la red LAN, seleccione la ficha **Mensaje para el administrador**.

5. Modifique la plantilla del mensaje. También puede usar los siguientes botones: **Variable**, **Predeterminado** y **Vínculo** (este botón solo está disponible en la ficha **Bloqueo**).

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Obtención de acceso a un dispositivo bloqueado

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

> La funcionalidad de Kaspersky Endpoint Security que otorga acceso temporario a un dispositivo está disponible solamente cuando Kaspersky Endpoint Security funciona bajo la directiva de Kaspersky Security Center y esta funcionalidad está habilitada en la configuración de directivas (consulte la *Guía del administrador de Kaspersky Security Center*).

Para solicitar acceso a un dispositivo bloqueado desde la ventana de configuración del componente Control de dispositivos:

1. En la ventana principal de la aplicación, seleccione la ficha **Protección y control**.

2. Haga clic en la sección **Control del endpoint**.

   Se abre la sección **Control del endpoint**.

3. Haga clic con el botón derecho para mostrar el menú contextual de la línea con información acerca del componente Control de dispositivos.

   Se abre un menú para seleccionar acciones del componente.

4. Haga clic en el botón **Acceso a dispositivo**.

   Se abre la ventana **Solicitar acceso al dispositivo**.

5. En la lista de dispositivos conectados, seleccione el dispositivo al que desea obtener acceso.

6. Haga clic en el botón **Generar archivo de solicitud de acceso**.

   Se abre la venta **Creando archivo de solicitud de acceso**.

7. En el campo **Duración del acceso**, especifique el período durante el cual quiera tener acceso al dispositivo.

8. Haga clic en el botón **Guardar**.

   Se abre la ventana **Guardar archivo de solicitud de acceso** estándar de Microsoft Windows.

9. En la ventana **Guardar archivo de solicitud de acceso** de Microsoft Windows, seleccione la carpeta donde quiera guardar el archivo de solicitud de acceso correspondiente al dispositivo, y haga clic en el botón **Guardar**.

10. Envíe el archivo de solicitud de acceso correspondiente al dispositivo al administrador de la red LAN.

11. Reciba el archivo de clave de acceso al dispositivo del administrador de la red LAN.

12. En la ventana **Solicitar acceso al dispositivo**, haga clic en el botón **Activar clave de acceso**.

    Se abre la ventana **Abrir clave de acceso** estándar de Microsoft Windows.

13. En la ventana **Abrir clave de acceso** de Microsoft Windows, seleccione el archivo de clave de acceso al dispositivo que recibió del administrador de la red LAN y haga clic en el botón **Abrir**.

    Se abre la ventana **Activación de la clave de acceso para el dispositivo** con información acerca del acceso otorgado.

14. En la ventana **Activación de la clave de acceso para el dispositivo**, haga clic en **Aceptar**.

Para solicitar acceso a un dispositivo bloqueado haciendo clic en el vínculo del mensaje en el que se informa que el dispositivo está bloqueado:

1. En la ventana con el mensaje que indica que un dispositivo o bus de conexión está bloqueado, haga clic en el vínculo **Solicitar acceso**.

   Se abre la venta **Creando archivo de solicitud de acceso**.

2. En el campo **Duración del acceso**, especifique el período durante el cual quiera tener acceso al dispositivo.

3. Haga clic en el botón **Guardar**.

   Se abre la ventana **Guardar archivo de solicitud de acceso** estándar de Microsoft Windows.

4. En la ventana **Guardar archivo de solicitud de acceso** de Microsoft Windows, seleccione la carpeta donde quiera guardar el archivo de solicitud de acceso correspondiente al dispositivo, y haga clic en el botón **Guardar**.

5. Envíe el archivo de solicitud de acceso correspondiente al dispositivo al administrador de la red LAN.

6. Reciba el archivo de clave de acceso al dispositivo del administrador de la red LAN.

7. En la ventana **Solicitar acceso al dispositivo**, haga clic en el botón **Activar clave de acceso**.

   Se abre la ventana **Abrir clave de acceso** estándar de Microsoft Windows.

8. En la ventana **Abrir clave de acceso** de Microsoft Windows, seleccione el archivo de clave de acceso al dispositivo que recibió del administrador de la red LAN y haga clic en el botón **Abrir**.

   Se abre la ventana **Activación de la clave de acceso para el dispositivo** con información acerca del acceso otorgado.

9. En la ventana **Activación de la clave de acceso para el dispositivo**, haga clic en **Aceptar**.

El periodo de tiempo para el cual se otorga acceso al dispositivo puede diferir del tiempo que ha solicitado. Se otorga acceso al dispositivo durante el período que especifica el administrador de la red de área local cuando se genera la clave de acceso al dispositivo.

Creación de una clave para acceder a un dispositivo bloqueado usando Kaspersky Security Center

Para otorgar acceso temporario al usuario a un dispositivo bloqueado, se requiere una clave de acceso al dispositivo. Puede crear una clave de acceso usando Kaspersky Security Center.

Para crear una clave de acceso para un dispositivo bloqueado:

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 a dispositivos y datos en el modo offline**.

   Se abre la ventana **Otorgar acceso a dispositivos y datos en el modo offline**.
6. Seleccione la ficha **Control de Dispositivos**.
7. En la ficha **Control de dispositivos**, haga clic en el botón **Examinar**.

   Se abre la ventana **Seleccionar archivo de solicitud de acceso** estándar de Microsoft Windows.
8. En la ventana **Seleccionar archivo de solicitud de acceso**, seleccione el archivo de solicitud de acceso que ha recibido del usuario y haga clic en el botón **Abrir**.

   El componente **Control de dispositivos** muestra los detalles del dispositivo bloqueado para el cual el usuario solicitó acceso.
9. Especifique el valor de la configuración **Duración del acceso**.

   Esta configuración define el lapso durante el cual le otorga al usuario acceso al dispositivo bloqueado. El valor predeterminado es el valor que especificó el usuario cuando creo el archivo de solicitud de acceso.
10. Especifique el valor de la configuración **Periodo de activación**.

    Esta configuración define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado con la clave de acceso provista.
11. Haga clic en el botón **Guardar**.

    Se abre la ventana **Guardar clave de acceso** estándar de Microsoft Windows.
12. Seleccione la carpeta de destino en la que quiera guardar el archivo que contiene la clave de acceso correspondiente al dispositivo bloqueado.

13. Haga clic en el botón **Guardar**.

Control Web

Este componente está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información acerca del Control Web e instrucciones para configurar los parámetros del componente.

Acerca del Control Web

El Control Web permite controlar acciones realizadas por usuarios de LAN a través de la restricción o el bloqueo del acceso a los recursos web.

Un recurso web es una página o un sitio web individual, o varias páginas o sitios web, que tienen una característica en común.

El Control Web proporciona las siguientes opciones:

- Disminución del tráfico.

  El tráfico se controla mediante la restricción o el bloqueo de las descargas de archivos multimedia, o mediante la restricción o el bloqueo del acceso a recursos web que no están relacionados con las responsabilidades del puesto del usuario.

- Delimitación del acceso por categorías de contenido de los recursos web.

  Para disminuir el tráfico y reducir pérdidas potenciales debidas al mal uso del tiempo de los empleados, puede restringirse o bloquearse el acceso a categorías de recursos web específicas (por ejemplo: bloquear el acceso a todos los recursos web que pertenecen a la categoría "Medios de comunicación a través de Internet").

- Control centralizado del acceso a los recursos web.

  Al utilizar Kaspersky Security Center, se dispone de configuraciones de acceso a recursos web personales y grupales.

Todas las restricciones y los bloqueos que se aplican para acceder a recursos web se implementan como reglas de acceso a recursos web.

Habilitación y deshabilitación del Control Web

Por defecto, el Control Web está habilitado. Si es necesario, puede deshabilitar el Control Web.

Existen dos formas de habilitar o deshabilitar el componente:

- Ficha **Protección y control** de la ventana principal de la aplicación.

- Desde la ventana de configuración de la aplicación.

*Para activar o desactivar el complemento Control Web en la ficha **Protección y control** de la ventana principal de la aplicación, realice lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Control del endpoint**.

   Se abre la sección **Control del endpoint**.
4. Haga clic con el botón derecho para mostrar el menú contextual de la línea con información acerca del componente Control Web.

   Se abre un menú para seleccionar acciones del componente.
5. Realice una de las siguientes acciones:

   - Para habilitar Control Web, seleccione **Iniciar** en el menú.
   - Para deshabilitar el Control Web, seleccione **Detener** en el menú.

Para habilitar o deshabilitar el Control Web en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control Web**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Realice una de las siguientes acciones:

   - Si desea habilitar el Control Web, active la casilla **Habilitar Control Web**.
   - Si desea deshabilitar el Control Web, desactive la casilla **Habilitar Control Web**.

   Si el Control Web está deshabilitado, Kaspersky Endpoint Security no controla el acceso a recursos web.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Categorías de contenido de recursos web

Las categorías de contenido de recursos web (en adelante también denominadas "categorías") que se enumeran a continuación se han seleccionado para describir en la mayor medida posible los bloques de datos alojados por los recursos web, y se tomaron en cuenta sus características funcionales y temáticas. El orden en el que aparecen las categorías en esta lista no refleja la importancia relativa o el predominio de dichas categorías en Internet. Los nombres de categorías web son provisorios y se utilizan solamente para los propósitos de los productos y sitios web de Kaspersky. Los nombres no reflejan necesariamente el significado implícito por ley. Un recurso web puede pertenecer a múltiples categorías web a la vez.

Contenido para adultos

Esta categoría incluye los siguientes tipos de recursos web:

- Recursos web que contengan cualquier material de fotografía o video de genitales de humanos o criaturas humanoides, actos de relaciones sexuales o auto estimulación realizados por seres humanos o criaturas humanoides.
- Recursos web que contengan cualquier material de texto, incluyendo materiales literarios o artísticos, que describan genitales de humanos o criaturas humanoides, actos de relaciones sexuales o auto estimulación realizados por seres humanos o criaturas humanoides.
- Recursos web dedicados a la discusión del aspecto sexual de las relaciones humanas.

  Coincide con la categoría "Medios de comunicación a través de Internet".

- Recursos web que contengan material erótico, trabajos que ofrezcan un retrato realista del comportamiento sexual de los humanos, o trabajos de arte diseñados a estimular la excitación sexual.
- Recursos web de Web canales de medios oficiales y comunidades en línea con una audiencia objetivo establecida, que contengan una sección especial y/o artículos individuales dedicados al aspecto sexual de las relaciones humanas.
- Recursos web dedicados a perversiones sexuales.
- Recursos web que publiciten y vendan objetos para su uso sexual y en la estimulación de la excitación sexual, servicios sexuales y citas íntimas, incluyendo los servicios ofrecidos en línea a través de chats de video eróticos, "sexo telefónico", "sexting" ("sexo virtual").
- Recursos web con los siguientes contenidos:
  - Artículos y blogs que tratan sobre educación sexual tanto con enfoque científico como generalizado.
  - Enciclopedias médicas, en especial sus secciones sobre reproducción sexual.
  - Recursos de instituciones médicas, en concreto sus secciones relacionadas con el tratamiento de órganos sexuales.

Software, audio, video

Esta categoría incluye las siguientes subcategorías que puede seleccionar individualmente:

- **Audio y video**.

  Esta subcategoría incluye recursos web que distribuyen materiales de audio y video: películas, grabaciones de transmisiones deportivas, grabaciones de conciertos, canciones, videos musicales, videos, grabaciones de instructivos de audio y video, etc.

- **Torrents**.

  Esta subcategoría incluye sitios web de rastreadores torrent diseñados con el fin de compartir archivos de tamaño ilimitado.

- **Uso compartido de archivos**.

  Esta subcategoría incluye sitios web para uso compartido de archivos, independientemente de la ubicación física de los archivos que se estén distribuyendo.

Alcohol, tabaco, narcóticos

Esta categoría incluye los recursos web cuyo contenido está directa o indirectamente relacionado con productos alcohólicos o que contengan alcohol, productos de tabaco, y sustancias narcóticas, psicotrópicas y/o estupefacientes.

- Recursos web que publicitan y venden dichas sustancias y parafernalia para el consumo.

  Coincide con la categoría "Comercio electrónico".

- Recursos web con instrucciones sobre cómo consumir o producir sustancias narcóticas, psicotrópicas y/o estupefacientes.

Esta categoría incluye recursos web que se dirigen a asuntos científicos y medicinales.

Violencia

Esta categoría incluye los recursos web que contengan cualquier foto, video o texto que describa actos de violencia física o psicológica dirigida a seres humanos, o tratamiento cruel de animales.

- Recursos web que describen escenas de ejecuciones, tortura o abuso, como así también herramientas destinadas a dichas prácticas.

  Coincide con la categoría "Armas, explosivos, pirotecnia".

- Recursos web que describen escenas de asesinato, pelea, lesiones o violaciones, escenas en las que humanos, animales o criaturas imaginarias son abusadas o humilladas.
- Recursos web con información que incita a los actos que ponen en riesgo la vida y/o la salud, incluyendo daños a uno mismo o el suicidio.
- Recursos web con información que sustenta o justifica la admisibilidad de la violencia y/o crueldad, o que incita a actos violentos contra humanos o animales.
- Retratos web con retratos o descripciones particularmente realistas de víctimas y atrocidades de guerra, conflictos armados y conflictos militares, accidentes, catástrofes, desastres naturales, cataclismos industriales o sociales, o sufrimiento humano.
- Videojuegos de navegador con escenas de violencia y crueldad, incluyendo los llamados "shooters" (juegos de disparos), "fightings" (juegos de pelea), "slashers" (juegos de supervivencia), etc.

  Coincide con la categoría "Videojuegos".

Armas, explosivos, pirotecnia

Esta categoría incluye los recursos web con información sobre armas, explosivos y productos de pirotecnia:

- Sitios web de fabricantes y tiendas de armas, explosivos y productos de pirotecnia.

Coincide con la categoría "Comercio electrónico".

- Sitios web dedicados a la fabricación o utilización de armas, explosivos y productos pirotécnicos.
- Recursos web que contienen material analítico, histórico, de fabricación y enciclopédico dedicado a armas, explosivos y productos pirotécnicos.

El término "armas" significa a aparatos, objetos, y significa diseñado a dañar la vida o salud de humanos y animales y/o dañar equipamiento y estructuras.

Malas palabras

Esta categoría incluye los recursos web donde se ha detectado lenguaje profano.

Coincide con la categoría "Contenido para adultos".

Esta categoría también incluye los recursos web con material lingüístico y filológico que contienen profanidad como objeto de estudio.

Juegos de azar, loterías, sorteos

Esta categoría incluye los recursos web que ofrecen a los usuarios a participar en forma financiera en juegos en línea, incluso si dicha participación financiera no es condición obligatoria para el acceso al sitio web. Esta categoría incluye los recursos web que ofrecen:

- Juegos en línea en los que se requiere que los participantes realicen contribuciones monetarias.

  Coincide con la categoría "Videojuegos".

- Loterías que involucran la apuesta con dinero.
- Loterías que involucran la adquisición de billetes o números de lotería.
- Información que puede disparar el deseo de participar en juegos en línea, sorteos y loterías.

Coincide con la categoría "Comercio electrónico".

Esta categoría incluye los juegos que ofrecen la participación sin costo como modo separado, como así también los recursos web que publicitan en forma activa los recursos web que recaen en esta categoría.

Comunicaciones de red

Esta categoría incluye los recursos web que le permiten a los usuarios (ya sea que estén registrados o no) enviar mensajes personales a otros usuarios de los recursos web relevantes u otros servicios en línea y/o agregar contenido (ya sea abierto al público o restringido) a los recursos web relevantes en ciertos términos. Puede seleccionar individualmente las siguientes subcategorías:

- **Chats y foros**.

  Esta subcategoría incluye recursos web diseñados para el debate público de diversos temas usando aplicaciones web especiales, así como recursos web diseñados para distribuir o admitir aplicaciones de mensajería instantánea que hacen posible la comunicación en tiempo real.

- **Blogs**.

  Esta subcategoría incluye plataformas de blog, que son sitios web que proporcionan servicios pagos o gratuitos para crear y mantener blogs.

- **Redes sociales**.

  Esta subcategoría incluye sitios web diseñados para la creación, la visualización y la administración de contactos entre personas, organizaciones y gobiernos, y que requieren el registro de una cuenta de usuario como condición de participación.

- **Portales de citas**.

  Esta subcategoría incluye recursos web que funcionan como una variedad de redes sociales y ofrecen servicios pagos o gratuitos.

  > Coincide con las categorías "Contenido para adultos" y "Comercio Electrónico".

- **Correo electrónico basado en la web**.

  Esta subcategoría incluye páginas de inicio de sesión exclusivas de un servicio de correo electrónico y páginas de buzón de correo que contienen correos electrónicos y datos asociados (como contactos personales). Esta categoría no incluye otros sitios web de un proveedor de servicios que también ofrezca el servicio de correo electrónico.

E-tailers, bancos y sistemas de pago

Esta categoría incluye los recursos web diseñados para cualquier transacción en línea de fondos monetarios que no sean efectivo utilizando aplicaciones web con ese propósito especial. Puede seleccionar individualmente las siguientes subcategorías:

- **Tiendas y subastas**.

  Esta categoría incluye tiendas y remates en línea en los que se vende cualquier producto, trabajo o servicio a individuos y/o entidades legales, incluyendo sitios web de tiendas que realizan ventas solamente en línea y perfiles en línea de tiendas físicas que aceptan pagos en línea.

- **Bancos**.

  Esta subcategoría incluye páginas web especializadas de bancos con funcionalidad de banca en línea, incluyendo transferencias electrónicas entre cuentas bancarias, realizar depósitos bancarios, realizar conversiones de monedas, pagar por servicios de terceros, etc.

- **Sistemas de pago**.

  Esta subcategoría incluye páginas web de diversos sistemas de dinero electrónico que ofrecen acceso a la cuenta personal del usuario.

En términos técnicos, el pago se realizará utilizando tarjetas bancarias de cualquier tipo (plástico o virtual, débito o crédito, locales o internacionales) y dinero electrónico. Los recursos web que pueden entrar en esa categoría sin importar si no tiene tantos aspectos técnicos como la transmisión de datos mediante el protocolo SSL, la utilización de la autenticación segura 3D, etc.

Búsqueda de trabajo

Esta categoría incluye los recursos web diseñados a reunir a los empleadores y a los buscadores de trabajos:

- Sitios web de agencias consultoras (agencias de empleo y/o agencias en busca de directivos).
- Sitios web de empleadores con descripciones de las búsquedas laborales en curso y sus ventajas.
- Portales independientes con ofertas de empleo de empleadores y agencias de contratación.
- Redes sociales profesionales que, entre todas, hacen posible publicar o encontrar información sobre especialistas que no están buscando un empleo en forma activa.

  Coincide con la categoría "Medios de comunicación a través de Internet".

Sistemas del acceso anónimo

Esta categoría incluye los recursos web que funcionan como intermediarios en la descarga de contenidos de otros recursos web mediante aplicaciones web especiales con el fin de:

- Saltearse las restricciones impuestas por el Administrador de la Red de Área Local (LAN) para acceder a direcciones web o IP;
- Acceder en forma anónima a los recursos web, incluidos los recursos web que rechazan en forma específica las solicitudes HTTP desde ciertas direcciones IP o sus grupos (por ejemplo, las direcciones IP agrupadas por país de origen).

Esta categoría incluye tanto los recursos web con el fin específico de los propósitos arriba mencionados ("anonimizadores") y de los recursos me tienen una funcionalidad técnicamente similar.

Videojuegos

Esta categoría incluye los recursos web dedicados a los videojuegos de varios géneros:

- Sitios web de desarrolladores de videojuegos.
- Sitios web dedicados a la discusión de videojuegos.

  Coincide con la categoría "Medios de comunicación a través de Internet".

- Recursos web que proveen la capacidad técnica para la participación en línea para videojuegos, junto con otros participantes o en forma individual, con instalación local de aplicaciones o sin dicha instalación ("juegos de

navegador").

- Recursos web diseñados a publicitar, distribuir y soportar programas de juego.

> Coincide con la categoría "Comercio electrónico".

Religiones, asociaciones religiosas

Esta categoría incluye los recursos web con material sobre movimientos públicos, asociaciones y organizaciones con una ideología religiosa y/o culto en cualquier manifestación.

- Sitios web de organizaciones religiosas oficiales en diferentes niveles, de religiones internacionales a comunidades religiosas locales.
- Sitios web de asociaciones religiosas sin registrar y sociedades que emergieron históricamente al separarse de una asociación o comunidad religiosa dominante.
- Sitios web de asociaciones y comunidades religiosas que emergieron en forma independiente de los movimientos religiosos tradicionales, incluyendo por la iniciativa de un fundador específico.
- Sitios web de organizaciones interconfesionales que buscan la cooperación entre representantes de diferentes religiones tradicionales.
- Recursos web con material educativo, histórico y enciclopédico referido a las religiones.
- Recursos web con retratos detallados o descripciones de la adoración como parte de los cultos religiosos, incluyendo ritos y rituales que involucran la adoración a Dios, seres y/u objetos que se creen tienen poderes sobrenaturales.

Medios de comunicación

Esta categoría incluye los recursos web con contenido de noticias públicas creado por los medios masivos o publicaciones en línea que permiten a los usuarios agregar sus propios informes de noticias:

- Sitos web de canales de medios oficiales.
- Sitios web que ofrecen servicios de información con la atribución de fuentes oficiales de información.
- Sitios web que ofrecen servicios de compilación, de colecciones de noticias de varias fuentes oficiales y no oficiales.
- Sitios web donde el contenido de noticias es creado por los usuarios ("sitios de noticias sociales").

> Coincide con la categoría "Medios de comunicación a través de Internet".

Anuncios

Esta categoría incluye los recursos web con anuncios. La información publicitaria de los banners pueden distraer a los usuarios de sus actividades, y la descarga de los banners aumenta el tráfico de la red.

Acerca de las reglas de acceso a recursos web

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 de determinadas 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 tres reglas configuradas previamente:

- La regla Tabla de escenarios y estilos, que otorga acceso a todos los usuarios en todo momento a los recursos web cuyas direcciones contienen nombres de archivos con las extensiones css, js o vbs. Por ejemplo: http://www.ejemplo.com/style.css, http://www.ejemplo.com/style.css?mode=normal.

- La "Regla por defecto", que otorga acceso a todos los usuarios a todos los recursos web en todo momento.

Acciones con las reglas de acceso a recursos web

Puede realizar las siguientes acciones en las reglas de acceso a recursos web:

- Agregar una nueva regla

- Editar una regla

- Asignar prioridad a una regla

  La prioridad de una regla es definida por la posición de la línea que contiene una breve descripción de esta regla en la tabla de reglas de acceso de la ventana de configuración del componente Control Web. Esto significa que una regla que se encuentra más arriba en la tabla de reglas de acceso tiene prioridad sobre una regla ubicada más abajo.

Si el recurso web al que el usuario intenta acceder coincide con los parámetros de varias reglas, Kaspersky Endpoint Security realiza una acción de acuerdo con la regla que tiene la mayor prioridad.

- Probar una regla.

  Puede comprobar la coherencia de las reglas mediante la función de diagnóstico de las reglas.

- Habilitar y deshabilitar una regla.

  Una regla de acceso a recursos web se puede habilitar (estado operativo: *Activo*) o deshabilitar (estado operativo: *Inactivo*). Por defecto, una vez que se creó una regla, queda habilitada (estado operativo: *Activo)*. Puede deshabilitar la regla.

- Eliminar regla

Adición y edición de una regla de acceso a recursos web

Para agregar o editar una regla de acceso a recursos web:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control Web**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Realice una de las siguientes acciones:

   - Para agregar una regla, haga clic en el botón **Agregar**.
   - Si desea editar una regla, seleccionar la regla en la tabla y haga clic en el botón **Modificar**.

   Se abre la ventana **Regla de acceso a recursos web**.
4. Especifique o edite la configuración de la regla. Para hacerlo:

   a. En el campo **Nombre**, escriba o edite el nombre de la regla.

   b. En la lista desplegable **Filtrar contenido**, seleccione la opción requerida:

      - **Cualquier contenido**.
      - **Por categorías de contenido**.
      - **Por tipos de datos**.
      - **Por categorías de contenido y tipos de datos**.

   c. Si se selecciona cualquier opción que no sea **Cualquier contenido**, se abren secciones para seleccionar categorías de contenido y/o tipos de datos. 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.

   d. En la lista desplegable **Aplicar a las direcciones**, seleccione la opción requerida:

- **A todas las direcciones**.
- **A direcciones individuales**.

e. Si se selecciona la opción **A direcciones individuales**, se abre una sección donde usted crea una lista de recursos web. Puede agregar o editar las direcciones de los recursos web mediante los botones **Agregar**, **Modificar** y **Eliminar**.

f. Seleccione la casilla **Especificar usuarios o grupos**.

g. Haga clic en el botón **Seleccionar**.

Se abre la ventana **Seleccionar usuarios o grupos** de Microsoft Windows.

h. Especifique o edite la lista de usuarios o grupos de usuarios para los cuales se debe permitir o bloquear el acceso a recursos web que describe la regla.

i. En la lista desplegable **Acción**, seleccione la opción requerida:

- **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.

j. 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:

1. Haga clic en el botón **Configuración** que se encuentra junto a la lista desplegable **Programación de la regla**.

   Se abre la ventana **Programación de la regla**.

2. Para agregar la programación de la regla con un intervalo de tiempo durante el cual la regla no debe aplicarse, en la tabla que muestra la programación de la regla, haga clic en las celdas de la tabla que corresponden a la hora y al día de la semana que quiera seleccionar.

   El color de las celdas se pone gris.

3. Para sustituir un intervalo de tiempo durante el cual se aplica la regla por un intervalo de tiempo durante el cual no se aplica la regla, haga clic en las celdas grises de la tabla que corresponden a la hora y al día de la semana que quiera seleccionar.

   El color de las celdas se pone verde.

4. Haga clic en el botón **Guardar como**.

   Se abre la ventana **Nombre de la programación de la regla**.

5. Escriba un nombre para la programación de reglas o deje el nombre predeterminado sugerido.

6. Haga clic en **Aceptar**.

5. En la ventana **Regla de acceso a recursos web**, haga clic en **Aceptar**.

6. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control Web**.
   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, seleccione la regla para la cual desea cambiar la prioridad.
4. Use los botones **Subir** y **Bajar** para mover la regla al lugar que desee en la lista de reglas.
5. Repita los pasos 3 y 4 para las reglas cuya prioridad desee cambiar.
6. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control Web**.
   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, haga clic en el botón **Diagnóstico**.
   Se abre la ventana **Diagnóstico de las reglas**.
4. Complete los campos de la sección **Condiciones**:
   a. 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.
   b. 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.
   c. 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, en la lista desplegable **Filtrar contenido**, seleccione la opción que desee (**Por categorías de contenido**, **Por tipos de datos** o **Por categorías de contenido y tipos de datos**).

d. 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.

5. 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.

Habilitación y deshabilitación de una regla de acceso a recursos web

Para habilitar o deshabilitar una regla de acceso a recursos web:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control Web**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, seleccione la regla que desea habilitar o deshabilitar.
4. En la columna **Estado**, haga lo siguiente:
   - Si desea habilitar el uso de la regla, seleccione el valor *Activado*.
   - Si desea deshabilitar el uso de la regla, seleccione el valor *Desactivado*.
5. Para guardar los cambios, haga clic en el botón **Guardar**.

Migración de reglas de acceso a recursos web a partir de versiones anteriores de la aplicación

Cuando se actualiza la versión Service Pack 1 Maintenance Release 1 o una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, las reglas de acceso a recursos web basadas en categorías de contenido de los recursos web se migran de la siguiente manera:

- Las reglas de acceso a recursos web basadas en una o más de las categorías de contenido de recursos web de las listas "Foros y chat", "Correo electrónico web" y "Redes sociales" migran a la categoría de contenido de recursos web "Medios de comunicación a través de 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 "Comercio Electrónico".
- Las reglas de acceso a recursos web basadas en la categoría de contenido "Juegos de azar" migran a la categoría de contenido de recursos web "Juegos de azar, loterías, sorteos".

- Las reglas de acceso a recursos web basadas en la categoría de contenido "Juegos de Navegador" migran a la categoría de contenido de recursos web "videojuegos".
- 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.

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 exportar una lista de direcciones de recursos web a un archivo:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Controles de seguridad**, seleccione **Control web**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Seleccione la regla cuyas direcciones de recursos web desea exportar a un archivo.
4. Haga clic en el botón **Modificar**.

   Se abre la ventana **Regla de acceso a recursos web**.
5. Si en lugar de exportar la lista completa de direcciones de recursos web desea exportar una parte de ella, seleccione las direcciones de recursos web requeridos.
6. A la derecha del campo con la lista de direcciones de recursos web, haga clic en el botón .

   Se abre la ventana de confirmación de acción.
7. Realice una de las siguientes acciones:
   - Si desea exportar solamente los elementos seleccionados de la lista de direcciones de recursos web, en la ventana de confirmación, haga clic en el botón **Sí**.
   - Si desea exportar todos los elementos de la lista de direcciones de recursos web, en la ventana de confirmación, haga clic en el botón **No**.

     Se abre la ventana **Guardar como** estándar de Microsoft Office.
8. En la ventana **Guardar como** de Microsoft Windows, seleccione el archivo al cual desea exportar la lista de direcciones de recursos web. Haga clic en el botón **Guardar**.

Para importar la lista de direcciones de recursos web de un archivo a una regla:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Controles de seguridad**, seleccione **Control web**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Realice una de las siguientes acciones:

- Si desea crear una nueva regla de acceso a recursos web, haga clic en el botón **Agregar**.
- Seleccione la regla de acceso a recursos web que desea editar. A continuación, haga clic en el botón **Modificar**.

Se abre la ventana **Regla de acceso a recursos web**.

4. Realice una de las siguientes acciones:
   - Si está creando una nueva regla de acceso a recursos web, seleccione **A direcciones individuales** de la lista desplegable **Aplicar a las direcciones**.
   - Si está editando una regla de acceso a recursos web, vaya al paso 5 de estas instrucciones.
5. A la derecha del campo con la lista de direcciones de recursos web, haga clic en el botón .

   Si está creando una regla nueva, se abre la ventana **Abrir archivo** estándar de Microsoft Windows.

   Si está editando una regla, se abre una ventana en la que se solicita confirmación.
6. Realice una de las siguientes acciones:
   - Si está editando una nueva regla de acceso a recursos web, vaya al paso 7 de estas instrucciones.
   - Si está editando una regla de acceso a recursos web, realice una de las siguientes acciones en la ventana de confirmación:
     - Si desea agregar elementos importados de la lista de direcciones de recursos web a los elementos existentes, haga clic en el botón **Sí**.
     - Si desea eliminar elementos existentes de la lista de direcciones de recursos web y agregar los importados, haga clic en el botón **No**.

   Se abre la ventana **Abrir archivo** de Microsoft Windows.
7. En la ventana **Abrir archivo** de Microsoft Windows, seleccione el archivo con la lista de direcciones de recursos web que desea importar.
8. Haga clic en el botón **Abrir**.
9. En la ventana **Regla de acceso a recursos web**, haga clic en **Aceptar**.

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 escribe la máscara de dirección *abc*, la regla de acceso se aplica a todos los recursos web que contengan la secuencia abc. Ejemplo: http://www.ejemplo.com/pagina_0-9abcdef.html.

Para incluir el carácter * en la máscara de dirección, ingrese el carácter * dos veces.

2. La secuencia de caracteres `www.` al comienzo de la máscara de dirección se interpreta como una secuencia `*.`

   Ejemplo: la máscara de dirección www.ejemplo.com se trata como *.ejemplo.com.

3. 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 `*.`.

4. Una secuencia de caracteres `*.` al principio de una máscara de dirección se interpreta como `*.` o como una cadena vacía.

   Ejemplo: la máscara de dirección http://www.*.ejemplo.com abarca la dirección http://www2.ejemplo.com.

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 de dirección http://www.ejemplo.com abarca direcciones como http://www.ejemplo.com/abc, donde a, b y c son 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 ejemplo.com abarca las direcciones http://ejemplo.com y https://ejemplo.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 de dirección http://*.ejemplo.com abarca la dirección http://www.ejemplo.com pero no abarca la dirección https://www.ejemplo.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.ejemplo.com	Sí	Consulte la regla 1.

3	*ejemplo.com	http://www.123ejemplo.com	Sí	Consulte la regla 1.
4	*ejemplo.com	http://www.123.ejemplo.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.ejemplo.com	Sí	Consulte las reglas 2, 1.
7	www.ejemplo.com	https://www.ejemplo.com	Sí	Consulte las reglas 2, 1.
8	http://www.*.ejemplo.com	http://123.ejemplo.com	Sí	Consulte las reglas 2, 4, 1.
9	www.ejemplo.com	http://www.ejemplo.com/abc	Sí	Consulte las reglas 2, 5, 1.
10	ejemplo.com	http://www.ejemplo.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://ejemplo.com	Sí	Consulte la regla 7.
13	http://ejemplo.com	https://ejemplo.com	No	Consulte la regla 8.
14	"ejemplo.com"	http://www.ejemplo.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.ejemplo.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.ejemplo.com; https://www.ejemplo.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.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Control del endpoint**, seleccione la subsección **Control Web**.

   En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, haga clic en el botón **Plantillas**.

   Se abre la ventana **Plantillas de mensajes**.
4. Realice una de las siguientes acciones:

   - Si desea modificar la plantilla del mensaje que advierte al usuario que no visite un recurso web, seleccione la ficha **Advertencia**.
   - Si desea editar la plantilla del mensaje que indica al usuario que se bloqueó el acceso a un recurso web, seleccione la ficha **Bloqueo**.
   - Para modificar la plantilla del mensaje que se envía al administrador, seleccione la ficha **Mensaje para el administrador**.
5. Modifique la plantilla del mensaje. También puede usar la lista desplegable **Variable**, así como los botones **Predeterminado** y **Vínculo** (este botón no está disponible en la ficha **Mensaje para el administrador**).
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

KATA Sensor de punto final

La configuración del componente KATA Sensor de punto final solo está disponible en la Consola de administración de Kaspersky Security Center. Para usar este componente, debe instalar el complemento de administración.

Esta sección contiene información sobre KATA Sensor de punto final e instrucciones sobre cómo activar o desactivar este componente.

Acerca de KATA Sensor de punto final

KATA Sensor de punto final es un componente de la Plataforma antiataques dirigidos de Kaspersky. Esta solución está diseñada para detectar rápidamente amenazas como los ataques dirigidos.

Este componente se instala en equipos cliente. En estos equipos, el componente supervisa continuamente procesos, conexiones de red activas y archivos que se modifican, y transmite esta información a la plataforma antiataques dirigidos de Kaspersky.

El componente está diseñado para funcionar en los siguientes sistemas operativos:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Para obtener información sobre Kaspersky Anti Targeted Attack Platform que no se trate en este documento, consulte la ayuda de Kaspersky Anti Targeted Attack Platform.

Las conexiones entrantes a equipos con el componente KATA Sensor de punto final se deberían permitir desde el servidor de la Plataforma antiataques dirigidos de Kaspersky directamente, sin ningún servidor proxy.

Activación y desactivación del componente KATA Sensor de punto final

Para activar y desactivar el componente KATA Sensor de punto final:

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 relevante para el cual quiera modificar la configuración de directivas.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Configuración avanzada**, seleccione la subsección **KATA Sensor de punto final**.

7. Realice una de las siguientes acciones:

   - Si quiere activar KATA Sensor de punto final, seleccione la casilla **KATA Sensor de punto final**.
   - Si quiere desactivar KATA Sensor de punto final, desmarque la casilla **KATA Sensor de punto final**.

8. Si seleccionó la casilla **KATA Sensor de punto final** en el paso anterior, en el campo **Dirección del servidor**, especifique la dirección del servidor de la Plataforma antiataques dirigidos de Kaspersky, que está compuesta por las siguientes partes:

   a. Nombre del protocolo

   b. Dirección IP o nombre de dominio totalmente calificado (FQDN) del servidor

   c. Ruta al Recopilador de eventos de Windows en el servidor

9. Haga clic en **Aceptar**.

10. Aplique la directiva.

    Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

Cifrado de datos

Si Kaspersky Endpoint Security se instala en un equipo que ejecuta Microsoft Windows para estaciones de trabajo, la funcionalidad de cifrado está completamente disponible. Si Kaspersky Endpoint Security se instala en un equipo que ejecuta Microsoft Windows para servidores de archivos, solo estará disponible el cifrado de discos duros con la tecnología de Cifrado de disco de BitLocker.

Esta sección contiene información sobre el cifrado y descifrado de discos duros, discos extraíbles y archivos y carpetas en discos locales del equipo, y se proporcionan instrucciones sobre cómo configurar y realizar el cifrado y descifrado de datos con Kaspersky Endpoint Security y con el complemento de administración de Kaspersky Endpoint Security.

Si no hay acceso a los datos cifrados, consulte las instrucciones especiales para trabajar con datos cifrados (Trabajar con archivos cifrados en caso de funcionalidad de cifrado de archivos limitada, Trabajar con dispositivos cifrados en caso de que no exista acceso a ellos).

Habilitación de la visualización de la configuración de cifrado en la directiva de Kaspersky Security Center

Para habilitar la visualización de la configuración de cifrado en la directiva de Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el menú contextual del nodo **Servidor de administración – <Nombre del equipo>** del árbol de la Consola de administración, seleccione **Ver → Configuración de la interfaz**.

   Se abre la ventana **Configuración de la interfaz**.
3. En la ventana **Configuración de la interfaz**, seleccione la casilla **Mostrar cifrado y protección de datos**.
4. Haga clic en **Aceptar**.

Acerca del 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.

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 el programa se active con una licencia nueva que permita el uso de cifrado.

Si caducó la licencia o se violó el Contrato de licencia de usuario final, o si la clave, Kaspersky Endpoint Security o los componentes de cifrado se han eliminado, el estado de cifrado de los archivos previamente cifrados no está garantizado. 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 locales del equipo**. 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. Después de aplicar una directiva de Kaspersky Security Center, Kaspersky Endpoint Security cifra y descifra 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 obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

- **Cifrado de discos 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.

  La aplicación realiza la acción especificada en la regla de cifrado cuando se implementa la directiva de Kaspersky Security Center.

- **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 archivos de almacenamiento 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 discos extraíbles.

- **Cifrado de discos duros**. 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 discos duros y crear una lista de los discos duros que se excluirán del cifrado. Kaspersky Endpoint Security cifra los discos duros sector por sector una vez aplicada la directiva de Kaspersky Security Center. La aplicación cifra simultáneamente todas las particiones lógicas de los discos duros. Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

  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 esto es necesario ingresar la contraseña del token o la tarjeta inteligente conectada al equipo, o el nombre de usuario y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local que utiliza las tareas de administración de 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. Puede administrar cuentas del Agente de autenticación y utilizar la tecnología de inicio de sesión único (SSO), que le permite iniciar sesión automáticamente en el sistema operativo por medio del 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 *Guía del administrador de Kaspersky Security Center*.

  > Cuando se actualiza la versión de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, no se guarda la lista de cuentas del Agente de autenticación.

  Solo es posible acceder a los discos duros cifrados desde equipos en los que esté instalado Kaspersky Endpoint Security con la funcionalidad de cifrado de discos duros. 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 todos los datos estén protegidos, incluso los datos eliminados que todavía podrían contener información recuperable.

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. En consecuencia, ya que los archivos nuevos se escriben en un dispositivo nuevo durante el inicio del cifrado normal con la función **Solo cifrar el espacio de disco usado** activada en el equipo, después de algún tiempo todos los sectores se cifrarán.

El Servidor de administración de Kaspersky Security Center que controló el equipo cuando se realzó el cifrado brinda los datos necesarios para descifrar los archivos. Si el equipo con archivos cifrados estuvo controlado por otro Servidor de administración por algún motivo y no se accedió ni una vez a los archivos cifrados, se puede obtener acceso de las siguientes maneras:

- Solicitar acceso a objetos cifrados al administrador de la red LAN.
- restauración los datos en 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.

La aplicación crea archivos de servicio durante el cifrado. Para almacenarlos, se requiere aproximadamente 2% a 3% 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.

No está soportada la compatibilidad entre la funcionalidad de cifrado de Kaspersky Endpoint Security y Kaspersky Anti-Virus para UEFI. El cifrado de discos duros del equipo en el que está instalado Kaspersky Anti-Virus para UEFI deja inoperativo a Kaspersky Anti-Virus para UEFI.

Limitaciones de la función de cifrado

Si crea una partición nueva en un disco duro cifrado o formatea una de las existentes, puede perderse la información de la unidad.

El cifrado de discos duros 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.

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.
- Tecnología Intel® Rapid Start y unidades que tienen una partición de hibernación, incluso con la tecnología Intel® Rapid Start activada.
- Unidades en formato MBR con más de cuatro particiones extendidas.

- Archivo de intercambio ubicado en una unidad que no es de sistema.
- Sistema multi-inicio con varios sistemas operativos instalados a la vez.
- Particiones dinámicas (solo se admiten particiones primarias).
- Unidades con menos del 2% 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.

Cambio del algoritmo de cifrado

El algoritmo del cifrado que utiliza Kaspersky Endpoint Security para el cifrado de datos depende de las bibliotecas de cifrado que se incluyen en el kit de distribución.

Para cambiar el algoritmo de cifrado:

1. Descifre los objetos que Kaspersky Endpoint Security cifró antes de comenzar a cambiar el algoritmo de cifrado.

   Una vez modificado el algoritmo de cifrado, los objetos que se cifraron anteriormente se vuelven no disponibles.

2. Eliminar Kaspersky Endpoint Security.
3. Instalar Kaspersky Endpoint Security desde el kit de distribución que contiene bibliotecas de cifrado para diferentes cantidades de bits.

Habilitación de la tecnología de inicio de sesión único (SSO)

La tecnología de inicio de sesión único (SSO) es incompatible con proveedores externos de credenciales de cuentas.

Para habilitar la tecnología de inicio de sesión único (SSO):

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 para el cual quiera habilitar la tecnología de inicio de sesión único (SSO).
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Cifrado de datos**, seleccione la subsección **Configuración común de cifrado**.
7. En la subsección **Configuración común de cifrado**, haga clic en el botón **Configurar** de la sección **Configuración de contraseñas**.

   Se abre la ficha **Agente de autenticación** de la ventana **Configuración de contraseña de cifrado**.
8. Seleccione la casilla **Usar tecnología de inicio de sesión único (SSO)**.
9. Haga clic en **Aceptar**.
10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.
11. Aplique la directiva.

    Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center.*

Consideraciones especiales para el cifrado de archivos

Cuando utilice la funcionalidad de cifrado de archivos, tenga en cuenta lo siguiente:

- La directiva de Kaspersky Security Center con configuración preestablecida para el cifrado de discos extraíbles se realiza 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 cifrará ni descifrará archivos con estado de solo lectura almacenados en unidades extraíbles.
- 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 archivos en carpetas predefinidas de perfiles de usuario móvil, perfiles de usuario obligatorio, perfiles de usuario temporal ni carpetas redirigidas. La lista de las carpetas estándar que Kaspersky recomienda cifrar incluye las siguientes carpetas:
  - Mis documentos.
  - Favoritos.
  - Cookies
  - Escritorio.
  - Archivos temporales de Internet Explorer
  - Archivos temporales.
  - Archivos de Outlook.

- 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%, %PROGRAMFILES(X86)%.
  - Archivos de registro de Windows.

  No es posible ver ni modificar la lista de exclusiones de cifrado. Si bien los archivos y las carpetas de la lista de exclusiones de cifrado se pueden agregar a la lista de cifrado, no serán cifrados durante una tarea de cifrado de archivos.

- 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

Cifrado de archivos en discos locales del equipo.

El cifrado de archivos en discos locales del equipo está disponible si Kaspersky Endpoint Security está instalado en un equipo que se ejecuta en Microsoft Windows para estaciones de trabajo. El cifrado de archivos en discos locales del equipo no está disponible si Kaspersky Endpoint Security está instalado en un equipo que se ejecuta en Microsoft Windows para servidores de archivos.

En esta sección se describe el cifrado de archivos en discos locales del equipo y se proporcionan instrucciones sobre cómo configurar y realizar el cifrado de archivos en discos locales del equipo con Kaspersky Endpoint Security y con el complemento de la consola de Kaspersky Endpoint Security.

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.

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 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.
5. Haga doble clic en él para abrir la ventana de propiedades de la política.
6. En la sección **Cifrado de datos**, seleccione **Cifrado de archivos**.
7. En la parte derecha de la ventana, seleccione la ficha **Cifrado**.
8. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas por defecto**.
9. 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.
      Se abre la ventana **Seleccionar carpetas predefinidas**.
   b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de carpeta introducida manualmente a una regla de cifrado.
      Se abre la ventana **Agregar carpeta personalizada**.
   c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo a una regla de cifrado. Kaspersky Endpoint Security cifrará los archivos con las extensiones especificadas en todos los discos locales del equipo.
      Se abre la ventana **Agregar o modificar lista de extensiones de archivos**.
   d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones de archivo 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.
      Se abre la ventana **Seleccionar grupos de extensiones de archivos**.
10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.
11. Aplique la directiva.
    Para obtener más información sobre la aplicación de una directiva de Kaspersky Security Center, consulte la ayuda de Kaspersky Security Center.

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.

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.

Kaspersky Endpoint Security cifrará archivos no cifrados si sus propiedades (ruta de archivo/nombre de archivo/extensión de archivo) todavía cumplen los criterios de la regla de cifrado después de la modificación.

Kaspersky Endpoint Security pospone el cifrado de los archivos abiertos hasta que se los cierre.

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.

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.

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 relevante para el que quiera configurar reglas de acceso a archivos cifrados para aplicaciones.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de archivos y carpetas**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas por defecto**.

   Las reglas de acceso solo se aplican en el modo **Reglas por defecto**. Después de aplicar reglas de acceso en el modo **Reglas por defecto**, si pasa al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de acceso. Todas las aplicaciones tendrán acceso a todos los archivos cifrados.

8. En la parte derecha de la ventana, seleccione la ficha **Reglas para aplicaciones**.
9. 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**, seleccione las casillas junto a las aplicaciones para las que desea formar las reglas de acceso a archivos cifrados.

d. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a archivos cifrados.

e. 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.

f. 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. 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 su extensión.

       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**.

11. Haga clic en **Aceptar** para guardar 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 relevante para el cual quiera configurar el cifrado de archivos que son creados por aplicaciones específicas.

3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de archivos y carpetas**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas por defecto**.

   Las reglas de cifrado solo se aplican en el modo **Reglas por defecto**. Después de aplicar reglas de cifrado en el modo **Reglas por defecto**, si pasa al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de cifrado. Los archivos que se cifraron anteriormente permanecerán cifrados.

8. En la parte derecha de la ventana, seleccione la ficha **Reglas para aplicaciones**.
9. 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 **Aplicación**, seleccione las casillas que se encuentran frente a las aplicaciones cuyos archivos creados se tienen que cifrar.

   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**.

10. 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 su extensión.

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**.

11. Haga clic en **Aceptar** para guardar 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.
5. Haga doble clic en él para abrir la ventana de propiedades de la política.
6. En la sección **Cifrado de datos**, seleccione **Cifrado de archivos**.
7. En la parte derecha de la ventana, seleccione la ficha **Descifrado**.
8. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas por defecto**.
9. 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.

Se abre la ventana **Seleccionar carpetas predefinidas**.

b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de carpeta introducida manualmente a una regla de descifrado.

Se abre la ventana **Agregar carpeta personalizada**.

c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo a una regla de descifrado. Kaspersky Endpoint Security no cifrará los archivos con las extensiones especificadas en todos los discos locales del equipo.

Se abre la ventana **Agregar o modificar lista de extensiones de archivos**.

d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones de archivo a una regla de descifrado. Kaspersky Endpoint Security no cifrará archivos que tengan las extensiones indicadas en los grupos de extensiones en todos los discos locales de los equipos.

Se abre la ventana **Seleccionar grupos de extensiones de archivos**.

10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.

11. Aplique la directiva.

Para obtener más información sobre la aplicación de una directiva de Kaspersky Security Center, consulte la ayuda de Kaspersky Security Center.

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 discos 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 para el cual quiera configurar el descifrado de archivos en discos locales.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.

- Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de archivos y carpetas**.

7. En la parte derecha de la ventana, seleccione la ficha **Cifrado**.

8. 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.

9. Formar una lista de descifrado de archivos.

10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.

11. Aplique la directiva.

Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center.*

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

Kaspersky Endpoint Security no realiza la compresión de archivos cuando crea un paquete cifrado.

Para crear un paquete cifrado:

1. En un equipo con Kaspersky Endpoint Security instalado y la funcionalidad de cifrado habilitada, utilice cualquier administrador de archivos para seleccionar los archivos o las carpetas que desea agregar al paquete cifrado. Haga clic con el botón derecho del mouse para abrir su menú contextual.

2. En el menú contextual, seleccione **Añadir a paquete cifrado**.

   Se abre el cuadro de diálogo estándar de Microsoft Windows **Elegir ruta para guardar el paquete cifrado**.

3. En el cuadro de diálogo estándar de Microsoft Windows **Elegir ruta para guardar el paquete cifrado**, seleccione el destino donde se guardará el paquete cifrado en el disco extraíble. Haga clic en el botón **Guardar**.

   Se abre la ventana **Añadir a paquete cifrado**.

4. En la ventana **Añadir a paquete cifrado**, escriba y confirme una contraseña.

5. Haga clic en el botón **Crear**.

   Se inicia el proceso de creación del paquete cifrado. Cuando finaliza el proceso, se crea un paquete cifrado protegido con contraseña y autoextraíble en la carpeta de destino seleccionada en el disco extraíble.

Si se cancela la creación de un paquete cifrado, Kaspersky Endpoint Security realiza las siguientes operaciones:

1. Cancela los procesos de copiado de archivos al paquete de almacenamiento y finaliza todas las operaciones de cifrado de paquetes, si hubiera alguna.

2. Elimina todos los archivos temporales creados durante el proceso de creación y cifrado del paquete y el archivo del paquete cifrado en sí.

3. Notifica al usuario sobre la cancelación forzada del proceso de creación del paquete cifrado.

Extracción de paquetes cifrados

Para extraer un paquete cifrado:

1. En cualquier administrador de archivos, seleccione un paquete cifrado. Haga clic para iniciar el asistente de descompresión.

   Se abre la ventana **Escribir contraseña**.

2. Escriba la contraseña que protege el paquete cifrado.

3. En la ventana **Escribir contraseña**, haga clic en **Aceptar**.

   Si la contraseña se escribe correctamente, se abre el cuadro de diálogo **Examinar** estándar de Microsoft Windows.

4. En el cuadro de diálogo **Examinar** estándar de Microsoft Windows, seleccione la carpeta de destino para extraer el paquete cifrado y haga clic en **Aceptar**.

   Comienza el proceso de extracción del paquete cifrado en la carpeta de destino.

Si el paquete cifrado ya se había extraído en la carpeta de destino especificado, los archivos del paquete cifrado sobrescribirán los archivos existentes en la carpeta.

Si se cancela la extracción de un paquete cifrado, Kaspersky Endpoint Security realiza las siguientes operaciones:

1. Detiene el proceso de descifrado del paquete y finaliza todas las operaciones de copiado de archivos desde el paquete cifrado, si tales operaciones están en curso.

2. Elimina todos los archivos temporales creados en el transcurso del descifrado y extracción del paquete cifrado, y elimina además todos los archivos que ya se habían copiado del paquete cifrado en la carpeta de destino.

3. Notifica al usuario sobre la cancelación forzada del proceso de extracción del paquete cifrado.

Cifrado de discos extraíbles

El cifrado de discos extraíbles está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. El cifrado de discos extraíbles no está disponible si Kaspersky Endpoint Security está instalado en un equipo que ejecuta Microsoft Windows para servidores de archivos.

Esta sección contiene información sobre el cifrado de discos extraíbles e instrucciones sobre la configuración y la realización del cifrado de discos extraíbles con Kaspersky Endpoint Security y con el complemento de administración de Kaspersky Endpoint Security.

Inicio del cifrado de discos extraíbles

Para cifrar discos 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 para el cual quiera configurar el cifrado de discos extraíbles.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.

   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de unidades extraíbles**.

7. En la lista desplegable **Modo de cifrado**, seleccione la acción por defecto que deberá realizar Kaspersky Endpoint Security en todos los discos extraíbles que estén conectados a equipos del grupo de administración seleccionado:

   - **Cifrar la unidad extraíble completa**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración de cifrado especificada para discos extraíbles, Kaspersky Endpoint Security cifrará el contenido de los discos extraíbles sector por sector. Como resultado, la aplicación cifrará no solo los archivos almacenados en los discos extraíbles sino también los sistemas de archivos de los discos extraíbles, incluidos los nombres de archivos y las estructuras de carpetas. Kaspersky Endpoint Security no vuelve a cifrar discos extraíbles que ya se hayan cifrado.

     Este escenario de cifrado se habilita gracias a la funcionalidad de cifrado de discos duros de Kaspersky Endpoint Security.

   - **Cifrar todos los archivos**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración de cifrado especificada para discos extraíbles, Kaspersky Endpoint Security cifrará todos los archivos almacenados en discos extraíbles. Kaspersky Endpoint Security no vuelve a cifra los archivos ya cifrados. La aplicación no cifra los sistemas de archivos de los discos extraíbles, como el nombre de los archivos cifrados y las estructuras de carpetas.

   - **Solo cifrar archivos nuevos**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración de cifrado especificada para discos extraíbles, Kaspersky Endpoint Security solo cifrará los archivos que se hayan agregado a discos extraíbles o que se hayan almacenado en discos extraíbles y que hayan sido modificados después de la última vez que se aplicó la directiva de Kaspersky Security Center.

   - **Descifrar la unidad extraíble completa**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración de cifrado especificada para discos extraíbles, Kaspersky Endpoint Security descifrará todos los archivos almacenados en discos extraíbles y también los sistemas de archivos de los discos extraíbles si se hubieran cifrado anteriormente.

     Esta situación de cifrado es posible gracias a la funcionalidad de cifrado de archivos y la funcionalidad de cifrado de discos duros que ofrece Kaspersky Endpoint Security.

   - **Dejar sin modificar**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración de cifrado especificada para discos extraíbles, Kaspersky Endpoint Security no cifrará ni descifrará los archivos almacenados en discos extraíbles.

8. Cree reglas de cifrado para los archivos almacenados en los discos extraíbles cuyo contenido quiera cifrar.

9. Aplique la directiva.

Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center.*

Ni bien se implementa la directiva, cuando el usuario conecta un disco extraíble o si el disco extraíble ya está conectado, Kaspersky Endpoint Security notifica al usuario que el disco extraíble está sujeto a una regla de cifrado por la cual los datos almacenados en el disco extraíble serán cifrados.

Si se especificó la regla *Dejar sin modificar* para el cifrado de datos en un disco extraíble, la aplicación no mostrará ninguna notificación al usuario.

La aplicación le advierte al usuario que el proceso de cifrado puede durar algunos minutos.

La aplicación le solicita al usuario que confirme la operación de cifrado y realiza las siguientes acciones:

- Cifra los datos de acuerdo con la configuración de la directiva si el usuario acepta el cifrado.
- Deja los datos sin cifrar si el usuario rechaza el cifrado, y restringe el acceso a los archivos del disco extraíble al modo de solo lectura.
- Deja los datos sin cifrar si el usuario ignora la solicitud de cifrado, restringe el acceso a los archivos del disco extraíble al modo de solo lectura, y vuelve a solicitarle al usuario que confirme el cifrado de datos la próxima vez que se aplique la directiva de Kaspersky Security Center o que se conecte un disco extraíble.

La directiva de Kaspersky Security Center con configuración preestablecida para el cifrado de datos en discos extraíbles se conforma para un grupo específico de equipos administrados. Por lo tanto, el resultado del cifrado de datos en discos extraíbles depende del equipo al cual esté conectado el disco extraíble.

Si el usuario inició la extracción segura de un disco extraíble durante el cifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de cifrado de datos y permite la extracción del disco extraíble antes de que finalice el descifrado.

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.

Agregar una regla de cifrado para discos extraíbles

Para añadir una regla de cifrado para discos extraíbles:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** en el árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración para el cual quiera agregar reglas de cifrado para discos extraíbles.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.

- Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de unidades extraíbles**.

7. Haga clic izquierdo sobre el botón **Agregar** y, en la lista desplegable, seleccione uno de los siguientes elementos:

   - Si quiere agregar reglas de cifrado para discos 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**.

     Se abre la ventana **Agregar dispositivos de la lista de dispositivos de confianza**.

   - Si quiere agregar reglas de cifrado para discos extraíbles que están en la lista de Kaspersky Security Center, seleccione **De la lista de dispositivos de Kaspersky Security Center**.

     Se abre la ventana **Agregar dispositivos de la lista de Kaspersky Security Center**.

8. Si seleccionó **De la lista de dispositivos de Kaspersky Security Center** en el paso anterior, especifique los filtros para mostrar dispositivos en la tabla. Para hacerlo:

   a. Especifique los valores de los siguientes parámetros: **Mostrar en la tabla los dispositivos que tengan definido lo siguiente**, **Tipo de dispositivo**, **Nombre**, **Equipo** y **Cifrado de disco de Kaspersky**.

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

9. En la columna **Tipo de dispositivo**, seleccione la casilla junto a los nombres de los discos extraíbles para los que quiera crear reglas de cifrado.

10. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione la acción que realizará Kaspersky Endpoint Security en los archivos almacenados en los discos extraíbles seleccionados.

11. Seleccione la casilla **Modo portátil** si desea que Kaspersky Endpoint Security prepare los discos extraíbles antes del cifrado, lo que permite que sea posible utilizar los archivos cifrados almacenados en esos discos en modo portátil.

    El modo portátil le permite usar archivos cifrados almacenados en discos extraíbles conectados a equipos sin funcionalidad de cifrado.

12. 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.

13. 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 los discos extraíbles:

    - Si quiere que la regla de cifrado creada anteriormente para el disco extraíble permanezca sin cambios, seleccione **Omitir**.

- Si quiere que una regla de cifrado creada anteriormente para un disco extraíble sea reemplazada por la regla nueva, seleccione **Actualizar**.

14. Haga clic en **Aceptar**.

    Las líneas que contienen los parámetros de las reglas de cifrado creadas aparecen en la tabla **Reglas personalizadas**.

15. Haga clic en **Aceptar** para guardar los cambios.

Las reglas de cifrado para discos extraíbles agregados se implementan en los discos extraíbles que están conectados a los equipos controlados por la directiva modificada de Kaspersky Security Center.

Edición de una regla de cifrado para discos extraíbles

Para modificar una regla de cifrado para un disco extraíble:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** en el árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración para el cual quiera modificar una regla de cifrado para discos extraíbles.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de unidades extraíbles**.
7. En la lista de discos extraíbles para las que se configuraron reglas de cifrado, seleccione una entrada correspondiente al disco extraíble que necesita.
8. 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**.
9. En el menú contextual del botón **Establecer una regla**, seleccione la acción que Kaspersky Endpoint Security realizará en los archivos almacenados en el disco extraíble seleccionado.
10. Haga clic en **Aceptar** para guardar los cambios.

Las reglas de cifrado para discos extraíbles modificadas se implementan en los discos extraíbles que están conectados a los equipos controlados por la directiva modificada de Kaspersky Security Center.

Habilitación del modo portátil para el acceso a archivos cifrados en discos extraíbles

Para habilitar el modo portátil para el acceso a archivos cifrados en discos 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 para el cual quiera activar el modo portátil para acceder a archivos cifrados en discos extraíbles.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de unidades extraíbles**.
7. Seleccione la casilla **Modo portátil**.

   El modo portátil está disponible para el cifrado de todos los archivos o solo de archivos nuevos.

8. Haga clic en **Aceptar**.
9. Aplique la directiva.

   Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.
10. Conecte el disco extraíble a un dispositivo en el cual se haya aplicado la directiva de Kaspersky Security Center.
11. Confirme la operación de cifrado del disco extraíble.

    Esto abre una ventana en la cual puede crear una contraseña para 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 cifra archivos en un disco extraíble según las reglas del cifrado definidas en la directiva de Kaspersky Security Center. El Administrador de archivos portátil usado para funcionar con archivos cifrados también se escribirá en el disco extraíble.

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.

Descifrado de discos extraíbles

Para descifrar discos 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 para el cual quiera configurar el descifrado de discos extraíbles.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.

   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de unidades extraíbles**.

7. Si quiere descifrar todos los archivos cifrados almacenados en los discos extraíbles, en la lista desplegable **Modo de cifrado**, seleccione **Descifrar la unidad extraíble completa**.

8. Para descifrar datos almacenados en discos extraíbles individuales, modifique las reglas de cifrado para los discos extraíbles que contienen los datos que quiera descifrar. Para hacerlo:

   a. En la lista de discos extraíbles para las que se configuraron reglas de cifrado, seleccione una entrada correspondiente al disco 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**.

9. Haga clic en **Aceptar** para guardar los cambios.

10. Aplique la directiva.

Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center.*

Después de aplicar la directiva, cuando el usuario conecta un disco extraíble o si un disco extraíble ya está conectado, Kaspersky Endpoint Security notifica al usuario que la unidad está sujeta a una regla de cifrado según la cual se descifrarán los archivos cifrados almacenados en la unidad, como así también su sistema de archivos. La aplicación le advierte al usuario que el proceso de descifrado puede durar algunos minutos.

La directiva de Kaspersky Security Center con configuración preestablecida para el cifrado de datos en discos extraíbles se conforma para un grupo específico de equipos administrados. Por lo tanto, el resultado del descifrado de datos en discos extraíbles depende del equipo al cual esté conectado el disco extraíble.

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.

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.

Cifrado de discos duros

Si Kaspersky Endpoint Security está instalado en un equipo con Microsoft Windows para estaciones de trabajo, las tecnologías Cifrado de unidad BitLocker y Cifrado de Disco de Kaspersky están disponibles para el cifrado. Si Kaspersky Endpoint Security se instala en un equipo que ejecuta Microsoft Windows para servidores de archivos, solo estará disponible la tecnología de Cifrado de unidad BitLocker.

Esta sección contiene información sobre el cifrado de discos duros e instrucciones sobre cómo configurar y realizar el cifrado de discos duros con Kaspersky Endpoint Security y con el complemento de la consola de Kaspersky Endpoint Security.

Sobre el cifrado de discos duros

Antes de comenzar el cifrado de discos duros, la aplicación ejecuta una cantidad 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 y 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 del disco duro 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. En base a esta información, la aplicación no inicia la tarea de cifrado de discos duros 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 del disco duro, ingrese `avp pbatestreset` en la línea de comando. 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 los discos duros, 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 descifrado del disco duro, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el cifrado de discos duros 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 descifrado del disco duro, el Agente de autenticación se carga cuando el sistema operativo sale del modo de hibernación. Kaspersky Endpoint Security reanuda el cifrado de discos duros 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 del disco duro, Kaspersky Endpoint Security reanuda el cifrado 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 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 escribir usando las configuraciones de teclado disponibles en el Agente de autenticación, solo se podrá acceder a los discos duros después de que se restauren con la Utilidad de Restauración o después de que se restauren el nombre y la contraseña de la cuenta del Agente de autenticación.

Kaspersky Endpoint Security es compatible con los siguientes dispositivos, lectores de tarjetas inteligentes y tarjetas inteligentes:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)

- SafeNet eToken 4100 72K Java (Smart Card)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Cifrado de discos duros usando la tecnología de Cifrado de disco de Kaspersky

Antes de cifrar discos duros en un equipo, se recomienda que se asegure de que el equipo no esté infectado. Para hacerlo, inicie la tarea de Análisis completo o la de Análisis de áreas críticas. Cifrar el disco duro de un equipo que está infectado por un rootkit puede hacer que quede inoperable.

Para cifrar discos duros usando la tecnología de 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 para el cual quiera configurar el cifrado de discos duros.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de discos duros**.

7. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **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.

8. En la lista desplegable **Modo de cifrado**, seleccione **Cifrar todos los discos duros**.

   Si tiene que excluir algunos de los discos duros del cifrado, cree una lista de dichos discos duros.

9. 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 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 quiere aplicar el cifrado al disco duro completo, desmarque la casilla **Solo cifrar el espacio de disco usado**.

     Esta función solo puede aplicarse a dispositivos no cifrados. 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.

10. Haga clic en **Aceptar** para guardar los cambios.

11. Aplique la directiva.

    Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

Cifrado de discos usando la tecnología de Cifrado de disco de BitLocker

Antes de cifrar discos duros en un equipo, se recomienda que se asegure de que el equipo no esté infectado. Para hacerlo, inicie la tarea de Análisis completo o la de Análisis de áreas críticas. Cifrar el disco duro de un equipo que está infectado por un rootkit puede hacer que quede inoperable.

El uso de la tecnología Cifrado de unidad BitLocker en equipos con un sistema operativo de servidor puede requerir la instalación del componente **Cifrado de unidad BitLocker** usando el asistente de componentes y Agregar roles.

Para cifrar discos duros usando la tecnología de Cifrado de disco de BitLocker

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 para el cual quiera configurar el cifrado de discos duros.

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

4. Seleccione la directiva correspondiente.

5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de discos duros**.

7. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **Cifrado de unidad BitLocker**.

8. En la lista desplegable **Modo de cifrado**, seleccione la opción **Cifrar todos los discos duros**.

9. Si quiere usar un teclado de pantalla táctil para ingresar la información en un entorno previo al inicio, seleccione la casilla **Permitir el uso de autenticación que requiere el ingreso del teclado previo al inicio en tabletas**.

   Se recomienda usar este parámetro solo para dispositivos que tengan herramientas de entrada de datos alternativas como un teclado USB en un entorno previo al inicio.

10. Seleccione uno de los siguientes tipos de cifrado:

    - Si quiere utilizar cifrado de hardware, seleccione la casilla **Usar cifrado de hardware**.
    - Si quiere utilizar cifrado de software, seleccione la casilla **Usar cifrado de software**.

11. 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 quiere aplicar el cifrado al disco duro completo, desmarque la casilla **Solo cifrar el espacio de disco usado**.

      Esta función solo puede aplicarse a dispositivos no cifrados. 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.

12. Seleccione un método para acceder a discos duros que se cifraron con BitLocker.

    - Si quiere usar un Módulo de plataforma segura (TPM) para almacenar claves de cifrado, seleccione la opción **Usar el módulo de plataforma segura (TPM)**.
    - Si no está utilizando un Módulo de plataforma segura (TPM) para el cifrado de discos duros, seleccione la opción **Usar contraseña** y especifique la cantidad mínima de caracteres que deberá contener la contraseña en el campo **Extensión mínima de contraseña**.

La disponibilidad de un Módulo de plataforma segura (TPM) es obligatoria para los sistemas operativos Windows 7 y Windows 2008 R2, así como para versiones anteriores.

13. Si seleccionó la opción **Usar el módulo de plataforma segura (TPM)** en el paso anterior:

    - Si quiere definir un código PIN que se le solicitará al usuario cuando intente acceder a una clave de cifrado, seleccione la casilla **Usar PIN** y, en el campo **Longitud mínima de PIN**, especifique la cantidad mínima de dígitos que deberá contener el código PIN.

    - Si desea acceder a discos duros cifrados sin un módulo de plataforma segura en el equipo usando una contraseña, seleccione la casilla **Usar la contraseña si el módulo de plataforma segura (TPM) no está disponible** y, en el campo **Extensión mínima de contraseña**, indique el número mínimo de caracteres que la contraseña debe contener.

      En este caso, se podrá acceder a las claves de cifrado usando la contraseña determinada como si estuviese seleccionada la casilla **Usar contraseña**.

      Si no está seleccionada la casilla **Usar la contraseña si el módulo de plataforma segura (TPM) no está disponible** y el módulo de plataforma segura no está disponible, no se iniciará el cifrado del disco duro.

14. Haga clic en **Aceptar** para guardar los cambios.

15. Aplique la directiva.

    Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

Después de aplicar la directiva en el equipo del cliente con Kaspersky Endpoint Security instalado, se realizarán las siguientes preguntas:

- Si se aplica la directiva de cifrado a un disco duro del sistema, la ventana del código PIN aparecerá si el módulo de plataforma segura está en uso. De lo contrario, aparecerá la ventana de solicitud de contraseña para la autorización de la precarga.

- Si el sistema operativo del equipo tiene activado el modo de compatibilidad del Estándar federal de procesamiento de la información, en Windows 8 y posteriores, el sistema operativo mostrará una ventana de solicitud de conexión del dispositivo USB para guardar el archivo de la clave de recuperación.

Si no hay acceso a claves de cifrado, el usuario puede solicitar que el administrador de la red local proporcione una clave de recuperación (si la clave de recuperación no se ha guardado anteriormente en el dispositivo USB o se ha perdido).

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 para el cual quiera crear una lista de discos duros que se deben excluir del

cifrado.

3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de discos duros**.
7. 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.
8. 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** y **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**.
9. Si quiere quitar discos duros de la tabla de exclusiones, seleccione una o varias líneas en la tabla **No cifrar los siguientes discos duros** y haga clic en el botón **Eliminar**.

   Para seleccionar varias líneas de la tabla, mantenga presionada la tecla **CTRL**.
10. Haga clic en **Aceptar** para guardar los cambios.

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 para el cual quiera configurar el descifrado de discos duros.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Cifrado de discos duros**.
7. En la lista desplegable **Tecnología de cifrado**, seleccione la tecnología con la cual se cifraron los discos duros.
8. 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.
9. Haga clic en **Aceptar** para guardar los cambios.
10. Aplique la directiva.

    Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center.*

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.

Administración del Agente de autenticación

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.

Es posible que el usuario no pueda superar la autenticación en algunas ocasiones. Por ejemplo, no es posible superar la autenticación si el usuario ha olvidado las credenciales de la cuenta del Agente de autenticación, o la contraseña del token o de la tarjeta inteligente, o cuando ha extraviado el token o la tarjeta inteligente.

Si el usuario ha olvidado las credenciales de la cuenta del Agente de autenticación o la contraseña de un token o una tarjeta inteligente, debe ponerse en contacto con el administrador de la red LAN corporativa para recuperarlas.

Si un usuario ha perdido una tarjeta inteligente o simbólica, el administrador debe agregar el archivo de un certificado electrónico de token o tarjeta inteligente al comando para crear una cuenta del Agente de autenticación. A continuación, el usuario debe completar el procedimiento de restaurar datos en los dispositivos cifrados.

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 hacerlo, debe agregar el archivo de certificado de un token o tarjeta inteligente al comando para crear una cuenta 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.

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.

  Si el certificado electrónico del token o de la tarjeta electrónica no cumple con este requisito, el complemento de administración no cargará el archivo de este certificado en el comando para crear una cuenta del Agente de autenticación y expondrá un mensaje de error.

- El parámetro `KeyUsage` que define el propósito del certificado debe tener el valor `keyEncipherment` o `dataEncipherment`.

  Si el certificado electrónico del token o de la tarjeta electrónica no cumple con este requisito, el complemento de administración cargará el archivo de este certificado en el comando para crear una cuenta del Agente de autenticación y expondrá un mensaje de advertencia.

- El certificado contiene una clave RSA con una longitud de al menos 1024 bits.

  Si el certificado electrónico del token o de la tarjeta electrónica no cumple con este requisito, el complemento de administración no cargará el archivo de este certificado en el comando para crear una cuenta del Agente de autenticación y expondrá un mensaje de error.

Edición de mensajes de ayuda del Agente de autenticación

Antes de modificar mensajes de ayuda del Agente de autenticación, revise la lista de caracteres admitidos en un entorno previo al inicio.

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 para el cual quiera modificar mensajes de ayuda del Agente de autenticación.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Configuración común de cifrado**.
7. En la sección **Plantillas**, haga clic en el botón **Ayuda**.

   Se abre la ventana **Mensajes de ayuda del Agente de autenticación**.
8. 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.
9. Modifique los mensajes de ayuda.

   Si quiere restaurar el texto original, haga clic en el botón **Predeterminado**.
10. Haga clic en **Aceptar**.
11. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.

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.

Selección del nivel de rastreo del Agente de autenticación

La aplicación registra información de servicio sobre el funcionamiento del Agente de autenticación e información acerca de las operaciones realizadas por el usuario con el Agente de autenticación en el archivo de seguimiento.

Para seleccionar el nivel de rastreo del 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. Seleccione el nivel de rastreo en la ventana de configuración del Agente de autenticación:

   - **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.

Administración de cuentas del Agente de autenticación

Las siguientes herramientas de Kaspersky Security Center están disponibles para administrar cuentas del Agente de autenticación:

- Tarea de grupo para administrar cuentas del Agente de autenticación. Esta tarea le permite administrar cuentas del Agente de autenticación para un grupo de equipos cliente.

- Tarea local de **Cifrado (administración de cuentas)**. Esta tarea le permite administrar cuentas del Agente de autenticación para equipos cliente individuales.

Para configurar los parámetros correspondientes a la tarea de administración de cuentas del Agente de autenticación:

1. Cree (Creación de una tarea local, Creación de una tarea de grupo) una tarea de administración de la cuenta del Agente de autenticación.
2. Abra la sección de **Configuración** en la ventana **Propiedades: <nombre de la tarea de administración de la cuenta del Agente de autenticación>**.
3. Agregue comandos para crear cuentas del Agente de autenticación.
4. Agregue comandos para modificar cuentas del Agente de autenticación.
5. Agregue comandos para eliminar las cuentas de usuario del Agente de autenticación.
6. Si es necesario, modifique los comandos agregados para administrar cuentas del Agente de autenticación. Para ello, seleccione un comando en la tabla **Comandos para administrar cuentas del Agente de autenticación** y haga clic en el botón **Modificar**.
7. Si es necesario, elimine los comandos agregados para administrar cuentas del Agente de autenticación. Para ello, seleccione uno o varios comandos en la tabla **Comandos para administrar cuentas del Agente de autenticación** y haga clic en el botón **Eliminar**.

   Para seleccionar varias líneas de la tabla, mantenga presionada la tecla **CTRL**.

8. Para guardar los cambios, haga clic en **Aceptar** en la ventana de propiedades de la tarea.
9. Ejecute la tarea.

Se ejecutarán los comandos de administración de cuentas del Agente de autenticación agregados a la tarea.

Cómo agregar un comando para crear una cuenta del Agente de autenticación

Para agregar un comando para crear una cuenta del Agente de autenticación:

1. Abra la sección de **Configuración** en la ventana **Propiedades: <nombre de la tarea de administración de la cuenta del Agente de autenticación>**.
2. Haga clic en el botón **Agregar** y, en la lista desplegable, seleccione **Comando de adición de cuenta**.

   Se abre la ventana **Agregar cuenta de usuario**.
3. En el campo **Agregar cuenta de usuario** de la ventana **Cuenta de Windows**, especifique el nombre de la cuenta de Microsoft Windows en función de la cual se creará la cuenta del Agente de autenticación.

   Para hacerlo, escriba el nombre de la cuenta manualmente o haga clic en el botón **Seleccionar**.
4. Si ingresó el nombre de una cuenta de Microsoft Windows manualmente, haga clic en el botón **Permitir** para determinar 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 SID de la cuenta de Microsoft Windows al agregar un comando de creación de cuenta del Agente de autenticación es una manera conveniente de asegurarse de que el nombre la cuenta de Microsoft Windows ingresada manualmente es correcto. Si la cuenta de Microsoft Windows ingresada no existe, pertenece a un dominio no confiable o no existe en el equipo para el cual se está modificando la tarea local de **Cifrado (administración de cuentas)**, la tarea de administración de cuentas del Agente de autenticación finaliza con error.

5. Seleccione la casilla **Cambiar la cuenta de usuario actual** 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 se agrega un comando de creación de cuenta del Agente de autenticación en las propiedades de una tarea local de **Cifrado (administración de cuentas)**.

6. 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.

7. Seleccione la casilla **Permitir la 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.

8. Si seleccionó la casilla **Permitir la autenticación basada en contraseña** en el paso anterior:

   a. En el campo **Contraseña**, escriba la contraseña de la cuenta del Agente de autenticación que se debe ingresar durante la autenticación para poder acceder a discos duros cifrados.

   b. En el campo **Confirmar contraseña**, confirme con la contraseña de la cuenta del Agente de autenticación ingresada en el paso anterior.

   c. Realice una de las siguientes acciones:

   - Seleccione la opción **Cambiar contraseña en la primera autenticación** si desea que la aplicación muestre una solicitud de cambio de contraseña al usuario la primera vez que pase la autenticación con la cuenta especificada en el comando.

   - De lo contrario, seleccione la opción **No solicitar cambio de contraseña**.

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.

10. Si seleccionó la casilla **Permitir la autenticación basada en certificado** en el paso anterior, haga clic en el botón **Examinar** y seleccione el archivo del certificado electrónico del token o de la tarjeta inteligente en la ventana **Seleccionar archivo de certificado**.

11. 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.

12. Realice una de las siguientes acciones:

- Seleccione la casilla **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 casilla **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.

13. En la ventana **Agregar cuenta de usuario**, haga clic en **Aceptar**.

Cómo agregar un comando para modificar una cuenta del Agente de autenticación

Para agregar un comando para modificar una cuenta del Agente de autenticación:

1. En la sección de **Configuración** de la ventana **Propiedades: <nombre de la tarea de administración de la cuenta del Agente de autenticación>**, abra el menú contextual del botón **Agregar** y seleccione el elemento **Comando de modificación de cuenta**.

   Se abre la ventana **Modificar cuenta de usuario**.

2. En el campo **Cuenta de Windows** de la ventana **Modificar cuenta de usuario**, especifique el nombre de la cuenta de usuario de Microsoft Windows que se utilizó para crear la cuenta del Agente de autenticación que quiera modificar. Para hacerlo, escriba el nombre de la cuenta manualmente o haga clic en el botón **Seleccionar**.

3. Si ingresó el nombre de una cuenta de usuario de Microsoft Windows manualmente, haga clic en el botón **Permitir** para determinar el identificador de seguridad (SID) de la cuenta de usuario.

   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 SID de la cuenta de usuario de Microsoft Windows al agregar un comando de modificación de cuenta del Agente de autenticación es una manera conveniente de asegurarse de que el nombre de la cuenta de usuario de Microsoft Windows ingresada manualmente es correcta. Si la cuenta de usuario de Microsoft Windows indicada no existe o pertenece a un dominio no confiable, la tarea de grupo para administrar cuentas del agente de autenticación finaliza con error.

4. 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.

5. Seleccione la casilla **Modificar la configuración de la autenticación por contraseña** para hacer modificables las configuraciones de autenticación basada en contraseña.

6. Seleccione la casilla **Permitir la 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.

7. Si seleccionó la casilla **Permitir la autenticación basada en contraseña** en el paso anterior:

   a. En el campo **Contraseña**, ingrese la nueva contraseña de la cuenta del Agente de autenticación.

   b. En el campo **Confirmar contraseña**, confirme con la contraseña ingresada en el paso previo.

8. 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.

9. Especifique el valor de la configuración de cambio de contraseña al autenticarse en el Agente de autenticación.

10. 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.

11. 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.

12. Si seleccionó la casilla **Permitir la autenticación basada en certificado** en el paso anterior, haga clic en el botón **Examinar** y seleccione el archivo del certificado electrónico del token o de la tarjeta inteligente en la ventana **Seleccionar archivo de certificado**.

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. En la ventana **Modificar cuenta de usuario**, haga clic en **Aceptar**.

Cómo agregar un comando para eliminar una cuenta del Agente de autenticación

Para agregar un comando para eliminar una cuenta del Agente de autenticación:

1. En la sección de **Configuración** de la ventana **Propiedades: <nombre de la tarea de administración de la cuenta del Agente de autenticación>**, abra el menú contextual del botón **Agregar** y seleccione el elemento **Comando de eliminación de cuenta**.

   Se abre la ventana **Eliminar cuenta de usuario**.

2. En el campo **Cuenta de Windows** de la ventana **Eliminar cuenta de usuario**, especifique el nombre de la cuenta de usuario de Microsoft Windows que se utilizó para crear la cuenta del Agente de autenticación que quiera eliminar. Para hacerlo, escriba el nombre de la cuenta manualmente o haga clic en el botón **Seleccionar**.

3. Si ingresó el nombre de una cuenta de usuario de Microsoft Windows manualmente, haga clic en el botón **Permitir** para determinar el identificador de seguridad (SID) de la cuenta de usuario.

   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 SID de la cuenta de usuario de Microsoft Windows al agregar un comando de eliminación de cuenta del Agente de autenticación es una manera conveniente de asegurarse de que el nombre de la cuenta de usuario de Microsoft Windows ingresada manualmente es correcta. Si la cuenta de usuario de Microsoft Windows indicada no existe o pertenece a un dominio no confiable, la tarea de grupo para administrar cuentas del agente de autenticación finaliza con error.

4. En la ventana **Eliminar cuenta de usuario**, haga clic en **Aceptar**.

Restauración de credenciales de cuentas del Agente de autenticación

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

Para restaurar el nombre de usuario y la contraseña de una cuenta del Agente de autenticación:

1. El Agente de autenticación se carga en un equipo con discos duros cifrados antes de que se cargue el sistema operativo. En la interfaz del Agente de autenticación, haga clic en el botón **Olvidé la contraseña** para iniciar el proceso de restauración del nombre de usuario y la contraseña de una cuenta del Agente de autenticación.

2. Siga las instrucciones del Agente de autenticación para obtener los las unidades de solicitud para restaurar el nombre de usuario y la contraseña del Agente de autenticación.

3. Indique el contenido de los bloques de solicitud al administrador de la red LAN de su empresa, junto con el nombre del equipo.

4. Complete las secciones de la respuesta a la solicitud de restauración del nombre de usuario y la contraseña de la cuenta del Agente de autenticación que haya generado (y le haya proporcionado) el administrador de la red LAN.

5. Ingrese una nueva contraseña para la cuenta del Agente de autenticación y confírmela.

   El nombre de usuario de la cuenta del Agente de autenticación se define utilizando las secciones de la respuesta a las solicitudes de restauración de nombre de usuario y la contraseña de la cuenta del Agente de autenticación.

Una vez ingresada y confirmada la nueva contraseña de la cuenta del Agente de autenticación, se guardará la contraseña y se le otorgará acceso a discos duros cifrados.

Cómo responder la solicitud de un usuario para restaurar credenciales de una cuenta del Agente de autenticación

Para crear y enviar al usuario las secciones de la respuesta a la solicitud de restauración del nombre de usuario y la contraseña de la cuenta 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 que incluya al equipo del usuario que solicitó la restauración del nombre de usuario y la contraseña de una cuenta del Agente de autenticación.

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

4. En la ficha **Dispositivos**, seleccione el equipo del usuario que solicitó la restauración del nombre de usuario y la contraseña de una cuenta del Agente de autenticación y haga clic con el botón derecho del mouse para abrir el menú contextual.

5. En el menú contextual, seleccione la opción **Otorgar acceso a dispositivos y datos en el modo offline**.

   Se abre la ventana **Otorgar acceso a dispositivos y datos en el modo offline**.

6. En la ventana **Otorgar acceso a dispositivos y datos en el modo offline**, seleccione la ficha **Agente de autenticación**.

7. En la sección **Algoritmo de cifrado en uso**, seleccione el tipo de algoritmo de cifrado.

8. 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.

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.

    El contenido de las secciones de la respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de una cuenta del Agente de autenticación se mostrará en el campo **Clave de acceso**.

11. Indique el contenido de los bloques de respuesta al usuario.

Visualización de detalles del cifrado de datos

Esta sección describe cómo ver los detalles del cifrado de datos.

Acerca del estado de cifrado

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 no definida*. No se ha definido una directiva de Kaspersky Security Center para el equipo.
- *Cifrado o descifrado en curso*. 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 o descifrado 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.

- *No compatible*. La funcionalidad de cifrado de datos no está disponible en el equipo.

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 pertenece el equipo 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.

   La columna **Estado de cifrado** muestra el estado de cifrado de los datos de los equipos del grupo de administración seleccionado. Este estado se conforma basándose en información sobre el cifrado de archivos de los discos locales del equipo, el cifrado de los discos duros del equipo y el cifrado de los discos extraíbles conectados al equipo.

Visualización de estadísticas de cifrado en los paneles de detalles de Kaspersky Security Center

Para ver el estado de cifrado en los paneles de detalles 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 de cifrado**.

g. Si es necesario, modifique la configuración del panel de detalles. Para hacerlo, 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 aparecen en la lista **Paneles de detalles** en 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 creados en los pasos anteriores aparece 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 discos extraíbles.

Visualización de errores de cifrado en discos locales del equipo

Para visualizar errores de cifrado en discos 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. Realice una de las siguientes acciones:

- Seleccione **Protección** en el menú contextual del equipo.
- 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 **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 **Crear 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 cifrado de datos del dispositivo almacenado**.
   - **Informe de errores de cifrado**.
   - **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.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

Administración de archivos cifrados con funcionalidad limitada de cifrado de archivos

Cuando la directiva de Kaspersky Security Center se implementa en archivos cifrados, Kaspersky Endpoint Security recibe una clave de cifrado necesaria para acceder directamente a los archivos cifrados. 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 colocan dentro de paquetes cifrados creados en un equipo con Kaspersky Endpoint Security instalado.
- Los archivos se almacenan en unidades extraíbles en las cuales se ha autorizado el modo portátil.

Acceso a archivos cifrados sin conexión con Kaspersky Security Center

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

Para acceder a archivos cifrados sin conexión con Kaspersky Security Center:

1. Intente acceder al archivo cifrado que necesita.

   Si no hay conexión con Kaspersky Security Center al intentar acceder a un archivo almacenado en un disco local del equipo, Kaspersky Endpoint Security genera un archivo con una solicitud de acceso para todos los archivos cifrados almacenados en los discos locales del equipo. Si intenta acceder a un archivo almacenado en un disco extraíble, Kaspersky Endpoint Security genera un archivo que solicita acceso a todos los archivos cifrados almacenados en el disco extraíble. Se abre la ventana **Acceso al archivo bloqueado**.

2. Envíe al administrador de red de área local el archivo que contiene la solicitud de acceso a archivos cifrados. Para ello, realice una de las siguientes acciones:

   - Para enviar por correo electrónico el archivo que solicita acceso a archivos cifrados al administrador de la red de área local, haga clic en el botón **Enviar por correo electrónico**.
   - Para guardar el archivo de solicitud de acceso a los archivos cifrados y entregárselo al administrador de la red LAN con un método diferente, haga clic en el botón **Guardar**.

3. Obtenga el archivo de clave para acceder a archivos cifrados que el administrador de la red de área local creó (y le proporcionó).

4. Active la clave para acceder a los archivos cifrados de una de las siguientes maneras:

   - En cualquier administrador de archivos, seleccione el archivo de la clave para acceder a archivos cifrados. Abra el archivo haciendo doble clic.
   - Haga lo siguiente:

     a. Abra la ventana principal de Kaspersky Endpoint Security.

     b. Haga clic en el botón .

     Se abre la ventana **Eventos**.

     c. Seleccione la ficha **Estado de acceso a archivos y dispositivos**.

     La ficha contiene una lista de todas las solicitudes de acceso a archivos cifrados.

     d. Seleccione la solicitud para la cual recibió el archivo de clave para acceder a archivos cifrados.

     e. Para cargar el archivo de clave enviado para acceder a archivos cifrados, haga clic en **Examinar**.

     Se abre el cuadro de diálogo **Seleccionar archivo de clave de acceso** estándar de Microsoft Windows.

f. En la ventana **Seleccionar archivo de clave de acceso** estándar de Microsoft Windows, seleccione el archivo proporcionado por el administrador con la extensión .kesdr y el nombre que coincida con el nombre de archivo del archivo de solicitud de acceso.

g. Haga clic en el botón **Abrir**.

h. En la ventana **Eventos**, haga clic en **Aceptar**.

Si un archivo con una solicitud de acceso a archivos cifrados se genera durante un intento de acceder a un archivo almacenado en un disco local del equipo, Kaspersky Endpoint Security otorga acceso a todos los archivos cifrados almacenados en los discos locales del equipo. Si se genera un archivo de solicitud de acceso a archivos cifrados durante un intento de acceder a un archivo almacenado en un disco extraíble, Kaspersky Endpoint Security otorga acceso a todos los archivos cifrados almacenados en el disco extraíble. Para acceder a archivos cifrados almacenados en otras unidades extraíbles, deberá obtener un archivo de clave de acceso exclusivo para cada unidad.

Otorgar acceso a archivos cifrados a los usuarios sin ninguna conexión con Kaspersky Security Center

Para otorgar acceso a archivos cifrados a los usuarios sin ninguna conexión con Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración que incluya al equipo del usuario que está solicitando el acceso a archivos cifrados.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que está solicitando el acceso a archivos cifrados y haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione la opción **Otorgar acceso a dispositivos y datos en el modo offline**.

   Se abre la ventana **Otorgar acceso a dispositivos y datos en el modo offline**.
6. En la ventana **Otorgar acceso a dispositivos y datos en el modo offline**, seleccione la ficha **Cifrado**.
7. En la ficha **Cifrado**, haga clic en el botón **Examinar**.

   Se abre el cuadro de diálogo **Seleccionar archivo de solicitud de acceso** estándar de Microsoft Windows.
8. En la ventana **Seleccionar archivo de solicitud de acceso**, especifique la ruta del archivo de solicitud que recibió del usuario y haga clic en **Abrir**.

   Kaspersky Security Center genera un archivo de clave para acceder a los archivos cifrados. Los detalles de la solicitud del usuario se muestran en la ficha **Cifrado**.
9. Realice una de las siguientes acciones:

   - Para enviar al usuario el archivo de clave de acceso generado, haga clic en el botón **Enviar por correo electrónico**.
   - Para guardar el archivo de clave de acceso correspondiente a los archivos cifrados y entregárselo al usuario por otro método, haga clic en el botón **Guardar**.

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 para el cual quiera modificar las plantillas de mensajes de solicitud de acceso a archivos cifrados.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Cifrado de datos**, seleccione la subsección **Configuración común de cifrado**.
7. En la sección **Plantillas**, haga clic en el botón **Plantillas**.

   Se abre la ventana **Plantillas**.
8. Haga lo siguiente:
   - Si quiere modificar la plantilla del mensaje del usuario, seleccione la ficha **Mensaje del usuario**. Se abre la ventana **Acceso al archivo denegado** cuando el usuario intenta acceder a un archivo cifrado, en tanto no exista ninguna clave disponible en el equipo para el acceso a archivos cifrados. Al hacer clic en el botón **Enviar por correo electrónico** en la ventana **Acceso al archivo denegado**, se crea automáticamente un mensaje del usuario. Este mensaje se envía al administrador de la red de área local corporativa junto con el archivo para solicitar acceso a archivos cifrados.
   - Si quiere modificar la plantilla del mensaje del administrador, seleccione la ficha **Mensaje del administrador**. Este mensaje se crea automáticamente al hacer clic en el botón **Enviar por correo electrónico** de la ventana **Otorgar acceso a archivos cifrados** y se envía al usuario después de que se le otorga acceso a los archivos cifrados.
9. Modifique las plantillas de mensaje.

   Puede usar el botón **Predeterminado** y la lista desplegable **Variable**.
10. Haga clic en **Aceptar**.
11. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.

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. El usuario usa la interfaz de aplicación Kaspersky Endpoint Security para crear un archivo de solicitud de acceso con la extensión kesdc y lo envía al administrador de la red LAN corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso con la extensión kesdr y 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. El usuario usa la Utilidad de restauración para crear un archivo de solicitud de acceso con la extensión fdertc y lo envía al administrador de la red LAN corporativa.
2. El administrador usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso con la extensión fdertr y 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 los datos de los dispositivos cifrados, se recomienda cancelar la directiva de cifrado de Kaspersky Security Center en el equipo donde se realizará esta operación. Esto evita que la unidad vuelva a cifrarse.

Obtención de acceso a dispositivos cifrados mediante la interfaz de la aplicación

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

Para obtener acceso a dispositivos cifrados mediante la interfaz de la aplicación:

1. Intente acceder al dispositivo cifrado que necesita.

   Se abre la ventana **El acceso a los datos está bloqueado**.

2. Envíe al administrador de la red LAN corporativa el archivo de solicitud de acceso con la extensión kesdc para el dispositivo cifrado. Para ello, realice una de las siguientes acciones:

   - Para enviar por correo electrónico al administrador de la red LAN corporativa el archivo de solicitud de acceso para el dispositivo cifrado, haga clic en el botón **Enviar por correo electrónico**.
   - Para guardar el archivo de solicitud de acceso para el dispositivo cifrado y entregárselo al administrador de la red LAN corporativa con un método diferente, haga clic en el botón **Guardar**.

   Si cierra la ventana **El acceso a los datos está bloqueado** sin guardar el archivo de solicitud de acceso o sin enviárselo al administrador de la red LAN corporativa, puede hacerlo en cualquier momento en la ventana **Eventos** en la ficha **Estado de acceso a archivos y dispositivos**. Para abrir esta ventana, haga clic en el botón de la ventana principal de la aplicación.

3. Obtenga y guarde el archivo de la clave de acceso del dispositivo cifrado que el administrador de la red LAN corporativa creó y le proporcionó.

4. Use uno de los siguientes métodos para aplicar la clave de acceso para acceder al dispositivo cifrado:

   - En cualquier administrador de archivos, busque el archivo de clave de acceso del dispositivo cifrado y haga doble clic en él para abrirlo.
   - Haga lo siguiente:

     a. Abra la ventana principal de Kaspersky Endpoint Security.

     b. Haga clic en el botón para abrir la ventana **Eventos**.

     c. Seleccione la ficha **Estado de acceso a archivos y dispositivos**.

     La ficha contiene una lista de todas las solicitudes de acceso a archivos y dispositivos cifrados.

     d. Seleccione la solicitud para la cual recibió el archivo de clave de acceso para acceder al dispositivo cifrado.

     e. Para cargar el archivo de clave de acceso recibido para acceder al dispositivo cifrado, haga clic en **Examinar**.

     Se abre el cuadro de diálogo **Seleccionar archivo de clave de acceso** estándar de Microsoft Windows.

f. En la ventana **Seleccionar archivo de clave de acceso** estándar de Microsoft Windows, seleccione el archivo proporcionado por el administrador con la extensión .kesdr y el nombre que coincida con el nombre de archivo del archivo de solicitud de acceso correspondiente para el dispositivo cifrado.

g. Haga clic en el botón **Abrir**.

h. Se abre la ventana **Estado de acceso a archivos y dispositivos**, haga clic en **Aceptar**.

Como resultado, Kaspersky Endpoint Security otorga acceso al dispositivo cifrado.

Otorgar acceso a dispositivos cifrados al usuario

Para otorgar acceso a un dispositivo cifrado al usuario:

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 del usuario que está solicitando el acceso al dispositivo cifrado.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo del usuario que está solicitando el acceso al dispositivo cifrado y haga clic con el botón derecho del mouse para abrir el menú contextual.
5. En el menú contextual, seleccione la opción **Otorgar acceso a dispositivos y datos en el modo offline**.

   Se abre la ventana **Otorgar acceso a dispositivos y datos en el modo offline**.
6. En la ventana **Otorgar acceso a dispositivos y datos en el modo offline**, seleccione la ficha **Cifrado**.
7. En la ficha **Cifrado**, haga clic en el botón **Examinar**.

   Se abre el cuadro de diálogo **Seleccionar archivo de solicitud de acceso** estándar de Microsoft Windows.
8. En la ventana **Seleccionar archivo de solicitud de acceso**, especifique la ruta al archivo de solicitud con la extensión kesdc que recibió del usuario.
9. Haga clic en el botón **Abrir**.

   Kaspersky Security Center genera un archivo de clave de acceso al dispositivo cifrado con la extensión kesdr. Los detalles de la solicitud del usuario se muestran en la ficha **Cifrado**.
10. Realice una de las siguientes acciones:

    - Para enviar al usuario el archivo de clave de acceso generado, haga clic en el botón **Enviar por correo electrónico**.
    - Para guardar el archivo de clave de acceso correspondiente al dispositivo cifrado y entregárselo al usuario por otro método, haga clic en el botón **Guardar**.

Proporcionar al usuario una clave de recuperación para el cifrado de discos duros con BitLocker

Para enviar a un usuario una clave de recuperación para un disco duro del sistema que se cifró usando BitLocker:

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 del usuario que está solicitando el acceso al disco cifrado.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En la ficha **Dispositivos**, seleccione el equipo que pertenece al usuario que está solicitando acceso al disco cifrado.
5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Otorgar acceso a dispositivos y datos en el modo offline**.

   Se abre la ventana **Otorgar acceso a dispositivos y datos en el modo offline**.
6. En la ventana **Otorgar acceso a dispositivos y datos en el modo offline**, seleccione la ficha **Acceder a un disco de sistema protegido por 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.
8. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.

Para enviar a un usuario una clave de recuperación para un disco duro que no sea de sistema y que se cifró usando BitLocker:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Cifrado y protección de datos** → **Dispositivos cifrados**.

   El espacio de trabajo muestra una lista de dispositivos cifrados.
3. En el espacio de trabajo, seleccione el dispositivo cifrado al cual tiene que restaurar el acceso.
4. Haga clic con el botón derecho del mouse para mostrar el menú contextual y seleccione **Obtener clave de acceso al dispositivo cifrado especificado**.

   Se abre la ventana **Restaurar acceso a un dispositivo cifrado con BitLocker**.
5. 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.
6. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.

Creación del archivo ejecutable de la Utilidad de Restauración

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

Para crear el archivo ejecutable de la Utilidad de Restauración:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón del ángulo inferior izquierdo de la ventana principal de la aplicación para abrir la ventana de **Soporte**.
3. En la ventana **Soporte**, haga clic en el botón **Restaurar dispositivo cifrado**.

   Se inicia la Utilidad de restauración de dispositivos cifrados.
4. Haga clic en el botón **Crear Utilidad de Restauración independiente** en la ventana de la Utilidad de Restauración.

   Se abre la ventana **Creando Utilidad de Restauración independiente**.
5. En la ventana **Guardar en**, escriba manualmente la ruta de la carpeta para guardar el archivo ejecutable de la Utilidad de Restauración o haga clic en el botón **Examinar**.
6. Haga clic en **Aceptar** en la ventana **Creando Utilidad de Restauración independiente**.

   El archivo ejecutable de la Utilidad de Restauración (fdert.exe) se guarda en la carpeta seleccionada.

Restauración de datos de dispositivos cifrados con la Utilidad de restauración

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

Para restaurar el acceso a dispositivos cifrados con la Utilidad de Restauración:

1. Ejecute la Utilidad de Restauración de una de las siguientes maneras:

   - Haga clic en el botón de la ventana principal de Kaspersky Endpoint Security para abrir la ventana de **Soporte** y seleccione el botón **Restaurar dispositivo cifrado**.
   - Ejecute el archivo ejecutable fdert.exe 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. 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 del dispositivo puede acelerar el proceso de recopilar la información necesaria para desbloquear o descifrar el dispositivo.

5. Haga clic en el botón **Desbloquear** o **Descifrar** según los resultados de diagnóstico.

   Se abre la ventana **Configuración de desbloqueo de dispositivos** o **Configuración de descifrado de dispositivos**.

6. Si desea restaurar datos usando una cuenta del Agente de autenticación:

   a. Seleccione la opción **Usar la configuración de la cuenta del Agente de autenticación**.

   b. En los campos **Nombre** y **Contraseña**, especifique las credenciales de la cuenta 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.

7. Si desea usar una clave de acceso para restaurar los datos:

   a. Seleccione la opción **Especificar manualmente la clave de acceso del dispositivo**.

   b. Haga clic en el botón **Recibir clave de acceso**.

   c. Se abre la ventana **Recibir clave de acceso del dispositivo**.

   d. Haga clic en el botón **Guardar** y seleccione la carpeta en la cual desea guardar el archivo de solicitud de acceso con la extensión fdertc.

   e. 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.

   f. Obtenga y guarde el archivo de la clave de acceso que el administrador de la red LAN corporativa creó y le proporcionó.

   g. Haga clic en el botón **Cargar** y seleccione el archivo de clave de acceso con la extensión fdertr en la ventana que se abre.

8. Si está descifrando un dispositivo, también debe especificar el resto de la configuración de descifrado en la ventana **Configuración de descifrado de dispositivos**. Para hacerlo:

   - Especifique el área para descifrar:

     - Si desea descifrar todo el dispositivo, seleccione la opción **Descifrar todo el dispositivo**.

- Si desea descifrar una parte de los datos de un dispositivo, seleccione la opción **Descifrar áreas individuales del dispositivo** y use los campos **Inicio** y **Fin** para especificar los límites del área del descifrado.

- 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 en el archivo después del descifrado**.

  - Si desea guardar los datos descifrados por separado de los datos cifrados originales, seleccione la casilla de selección **Guardar datos en el archivo después del descifrado** y el botón **Examinar** para especificar la ruta donde desea guardar los datos.

9. Haga clic en **Aceptar**.

Se inicia el proceso de desbloqueo o descifrado del dispositivo.

Respondiendo a una solicitud del usuario de restaurar datos en dispositivos cifrados

Para crear un archivo de clave para acceder a un dispositivo cifrado y proporcionárselo a un usuario:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el árbol de la Consola de administración, seleccione la carpeta **Adicional** → **Cifrado y protección de datos** → **Dispositivos cifrados**.

3. En el espacio de trabajo, seleccione el dispositivo cifrado para el cual desea crear un archivo de clave de acceso y, en el dispositivo del menú contextual, seleccione **Obtener clave de acceso al dispositivo cifrado especificado**.

   Si no está seguro de para qué equipo se generó el archivo de solicitud de acceso, en el árbol de la Consola de administración, seleccione el **Cifrado** → **Adicional** de datos y, en el espacio de trabajo, haga clic en el vínculo **Obtener la clave del dispositivo de cifrado**.

   Se abre la ventana **Permitir acceso al dispositivo**.

4. Seleccione el algoritmo del cifrado en uso. Para ello, seleccione una de las siguientes opciones:

   - **AES256**, si Kaspersky Endpoint Security se ha instalado desde un paquete de distribución localizado en la carpeta aes256 del equipo donde se cifró el dispositivo;

   - **AES56**, si Kaspersky Endpoint Security se ha instalado desde un paquete de distribución localizado en la carpeta aes56 del equipo donde se cifró el dispositivo;

5. Haga clic en el botón **Examinar**.

   Se abre el cuadro de diálogo **Seleccionar archivo de solicitud de acceso** estándar de Microsoft Windows.

6. En la ventana **Seleccionar archivo de solicitud de acceso**, especifique la ruta al archivo de solicitud con la extensión fdertc que recibió del usuario.

7. Haga clic en el botón **Abrir**.

Kaspersky Security Center genera un archivo de clave del acceso con la extensión fdertr para acceder al dispositivo cifrado.

8. Realice una de las siguientes acciones:

   - Para enviar al usuario el archivo de clave de acceso generado, haga clic en el botón **Enviar por correo electrónico**.
   - Para guardar el archivo de clave de acceso correspondiente al dispositivo cifrado y entregárselo al usuario por otro método, haga clic en el botón **Guardar**.

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.

Se otorgará el acceso a los datos en las mismas condiciones que antes de la falla del sistema operativo.

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).

Protección de la red

Esta sección contiene información sobre la supervisión del tráfico de red e instrucciones sobre cómo configurar los parámetros de los puertos de red supervisados.

Acerca de la protección de la red

Durante el funcionamiento de Kaspersky Endpoint Security, diversos componentes como el Antivirus de correo electrónico, el Antivirus de Internet y el Antivirus MI supervisan las transmisiones de datos enviadas a través de protocolos específicos y que pasan por puertos TCP y UDP abiertos específicos de su equipo. Por ejemplo: el Antivirus de correo electrónico analiza los datos que se transmiten por medio de SMTP, mientras que el Antivirus de Internet analiza los datos transmitidos mediante HTTP y FTP.

Kaspersky Endpoint Security divide los puertos TCP y UDP del sistema operativo en varios grupos, según el grado de probabilidad de que se vean vulnerados. Algunos puertos de red se reservan para servicios que pueden ser vulnerables. Se le recomienda que controle estos puertos con mayor atención, dado que la probabilidad de que sufran ataques es mayor. 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. Dichos puertos y aplicaciones recibirán atención especial de los componentes Antivirus de correo electrónico, Antivirus de Internet y Antivirus MI cuando estos supervisan el tráfico de red.

Configuración de los parámetros de la supervisión del tráfico de red

Puede realizar las siguientes acciones para establecer la configuración de los parámetros de la supervisión del tráfico de red:

- Habilitar la supervisión de todos los puertos de red.
- Crear una lista de puertos de red supervisados.
- Crear una lista de aplicaciones para las que se supervisarán todos los puertos de red.

Habilitación de la supervisión de todos los puertos de red

Para activar la supervisión de todos los puertos de red:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.
   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Puertos supervisados**, seleccione **Supervisar todos los puertos de red**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Creación de una lista de puertos de red supervisados

Para crear una lista de puertos de red supervisados:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Puertos supervisados**, seleccione **Supervisar solo los puertos seleccionados**.
4. 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.
5. En la lista de puertos de red, realice lo siguiente:

   - Seleccione las casillas junto a los puertos de red que desee incluir en la lista de puertos de red supervisados.

     Por defecto, se seleccionan las casillas que se encuentran junto a todos los puertos de red que están incluidos en la ventana **Puertos de red**.
   - Desactive las casillas junto a los puertos de red que desee excluir de la lista de puertos de red supervisados.
6. Si no se muestra un puerto de red en la lista de puertos de red, agréguelo haciendo lo siguiente:

   a. En la lista de puertos de red, haga clic en el vínculo **Agregar** para abrir la ventana **Puerto de red**.

   b. Escriba el número de puerto de red en el campo **Puerto**.

   c. Escriba el nombre del puerto de red en el campo **Descripción**.

   d. Haga clic en **Aceptar**.

   La ventana **Puerto de red** se cierra. El puerto de red recién agregado se muestra al final de la lista de puertos de red.
7. En la ventana **Puertos de red**, haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

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 dichas conexiones, seleccione la casilla **Supervisar todos los puertos de red** en la sección **Puertos supervisados** o configure la supervisión de todos los puertos para aplicaciones que establezcan la conexión 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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Puertos supervisados**, seleccione **Supervisar solo los puertos seleccionados**.
4. Haga clic en el botón **Configuración**.

   Se abre la ventana **Puertos de red**.
5. Seleccione la casilla **Supervisar todos los puertos de las aplicaciones especificadas**.
6. En la lista de aplicaciones debajo de la casilla **Supervisar todos los puertos de las aplicaciones especificadas**, haga lo siguiente:

   - Seleccione las casillas junto a los nombres de las aplicaciones para las que desea que se supervisen los puertos.

     Por defecto, se seleccionan las casillas que se encuentran junto a todas las aplicaciones que están incluidas en la ventana **Puertos de red**.

   - Desactive las casillas junto a los nombres de las aplicaciones para las cuales no desea que se supervisen los puertos.
7. Si una aplicación no está incluida en la lista de aplicaciones, agréguela del siguiente modo:

   a. Haga clic en el vínculo **Agregar** de la lista de aplicaciones y abra el menú contextual.

   b. En el menú contextual, seleccione la forma para agregar la aplicación a la lista de aplicaciones:

      - Para seleccionar una aplicación de la lista de aplicaciones que están instaladas en el equipo, seleccione el comando **Aplicaciones**. Se abre la ventana **Seleccionar aplicación**, en donde puede especificar el nombre de la aplicación.

      - Para especificar la ubicación del archivo ejecutable de la aplicación, seleccione el comando **Examinar**. Se abre la ventana **Abrir** estándar de Microsoft Windows, en donde puede especificar el nombre del archivo ejecutable de la aplicación.

      La ventana **Aplicación** se abre después de seleccionar la aplicación.

   c. En el campo **Nombre**, escriba un nombre para la aplicación seleccionada.

   d. Haga clic en **Aceptar**.

      Se cierra la ventana **Aplicación**. La aplicación que agregó aparece al final de la lista de aplicaciones.
8. En la ventana **Puertos de red**, haga clic en **Aceptar**.

9. Para guardar los cambios, haga clic en el botón **Guardar**.

Actualización de bases de datos y módulos de software de la aplicación

Esta sección contiene información acerca de las actualizaciones de las bases de datos y de los módulos de la aplicación (también denominadas "actualizaciones") e instrucciones sobre cómo configurar parámetros de actualización.

Acerca de actualizaciones de las bases de datos y de los módulos 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 ajustar la configuración de la conexión.

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 **Actualización**, en la sección **Tareas** de la ficha **Protección y control** de la ventana principal de la aplicación.

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.

Acerca de los orígenes de actualizaciones

Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security.

Como origen de actualizaciones, puede utilizar el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky o una carpeta local o de red dispuesta para tal fin.

Actualizar configuración de parámetros

Puede realizar las siguientes acciones para definir la configuración de actualización:

- Agregar nuevos orígenes de actualizaciones.

  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.

  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.

  > Si selecciona un recurso ubicado fuera de la red LAN como origen de actualizaciones, será necesaria una conexión a Internet para obtener la actualización.

- Seleccionar la región del servidor de actualizaciones de Kaspersky.

  Si utiliza servidores de actualizaciones de Kaspersky como un origen de actualizaciones, puede seleccionar la ubicación del servidor de actualizaciones de Kaspersky que se utiliza para descargar el paquete de actualización. Kaspersky posee servidores de actualización en varios países. Utilizar los servidores de actualización de Kaspersky más cercanos ayuda a reducir el tiempo empleado para recuperar un paquete de actualización.

  Por defecto, la aplicación utiliza información sobre la región actual del registro del sistema operativo.

- Configurar la actualización de Kaspersky Endpoint Security desde una carpeta compartida.

  Para economizar tráfico web, puede configurar las actualizaciones de Kaspersky Endpoint Security para que los equipos en su LAN reciban actualizaciones desde una carpeta compartida. Para esto, uno de los equipos en su red LAN recibe un paquete de actualización actualizado del servidor de Kaspersky Security Center o de los servidores de actualizaciones de Kaspersky y, luego, copia el paquete de actualización recuperado a una carpeta compartida. A continuación, otros equipos en la LAN pueden recibir el paquete de actualización desde esta carpeta compartida.

- Seleccionar el 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.

- Configurar la tarea de actualización para que se ejecute con los permisos de una cuenta de usuario diferente.

Adición de un origen de actualizaciones

Para agregar un origen de actualizaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.
   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Origen**.
   Se abre la ficha **Origen** de la ventana **Actualizar**.
4. En la ficha **Origen**, haga clic en el botón **Agregar**.
   Se abre la ventana **Seleccionar origen de actualización**.
5. En la ventana **Seleccionar origen de actualización**, seleccione una carpeta con el paquete de actualización o escriba la ruta completa de la carpeta en el campo **Origen**.
6. Haga clic en **Aceptar**.
7. En la ventana **Actualizar**, haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

Selección de la región del servidor de actualizaciones

Para seleccionar la región del servidor de actualizaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.
   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Origen**.
   Se abre la ficha **Origen** de la ventana **Actualizar**.
4. En la ficha **Origen**, diríjase a la sección **Configuración regional** y seleccione **Seleccionar de la lista**.
5. En la lista desplegable, seleccione el país más cercano a su ubicación actual.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de actualizaciones desde una carpeta compartida

La configuración de actualizaciones de Kaspersky Endpoint Security desde una carpeta compartida consta de los siguientes pasos:

1. Habilitación de la copia de un paquete de actualización a una carpeta compartida en uno de los equipos en la red de área local.

2. Configuración de actualizaciones de Kaspersky Endpoint Security desde una carpeta compartida especificada a los equipos restantes en la red de área local.

Para habilitar la copia del paquete de actualización a la carpeta compartida:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.

   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.

3. En la sección **Adicional**, seleccione la casilla **Copiar las actualizaciones en la carpeta**.

4. Especifique la ruta a la carpeta compartida donde se va a colocar el paquete de actualización. Puede hacer esto de las siguientes maneras:

   - Indique la ruta a la carpeta compartida en el campo en la casilla **Copiar las actualizaciones en la carpeta**.

   - Haga clic en el botón **Examinar**. Luego, en la ventana **Seleccionar carpeta** que se abre, seleccione la carpeta necesaria y haga clic en **Aceptar**.

5. Para guardar los cambios, haga clic en el botón **Guardar**.

Para configurar la actualización de Kaspersky Endpoint Security desde una carpeta compartida:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.

   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.

3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Origen**.

   Se abre la ficha **Origen** de la ventana **Actualizar**.

4. En la ficha **Origen**, haga clic en el botón **Agregar**.

   Se abre la ventana **Seleccionar origen de actualización**.

5. En la ventana **Seleccionar origen de actualización**, seleccione la carpeta compartida que contiene el paquete de actualización o escriba la ruta completa de la carpeta compartida en el campo **Origen**.

6. Haga clic en **Aceptar**.

7. En la ficha **Origen**, desactive las casillas junto a los nombres de los orígenes de actualizaciones que no ha especificado como la carpeta compartida.

8. Haga clic en **Aceptar**.

9. Para guardar los cambios, haga clic en el botón **Guardar**.

Selección del modo de ejecución de la tarea de actualización

Para seleccionar el modo de ejecución de la tarea de actualización:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.

   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.

3. Haga clic en el botón **Modo de ejecución**.

   Se abre la ficha **Modo de ejecución** en la ventana **Actualizar**.

4. En la sección **Modo de ejecución**, seleccione una de las siguientes opciones para iniciar una 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**.

5. Realice una de las siguientes acciones:

   - Si ha seleccionado la opción **Automático** o **Manual**, vaya al paso 6 de las instrucciones.

   - Si ha seleccionado la opción **Mediante programación**, especifique la configuración de la programación de ejecución de la tarea de actualización. Para hacerlo:

     a. En la lista desplegable **Frecuencia**, especifique cuándo se debe iniciar la tarea de actualización. Seleccione una de las siguientes opciones: **Minutos**, **Horas**, **Días**, **Cada semana**, **En el momento especificado**, **Cada mes** o **Después del inicio de la aplicación**.

     b. Según el elemento seleccionado en la lista desplegable **Frecuencia**, especifique los valores para la configuración que define el momento de inicio de la tarea de actualización.

     c. 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 el elemento **Después del inicio de la aplicación** está seleccionado en la lista desplegable **Frecuencia**, el campo **Posponer la ejecución después del inicio de la aplicación durante** no está disponible.

d. Si desea que Kaspersky Endpoint Security ejecute las tareas de actualización omitidas lo antes posible, seleccione la casilla **Ejecutar tareas omitidas**.

Si la opción **Horas**, **Minutos** o **Después del inicio de la aplicación** está seleccionada en la lista desplegable **Frecuencia**, la casilla **Ejecutar tareas omitidas** no está disponible.

6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

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 por no tener los permisos de un usuario de servidor proxy autorizado. 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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.
   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Modo de ejecución**.
   Se abre la ficha **Modo de ejecución** en la ventana **Actualizar**.
4. En la ficha **Modo de ejecución**, en la sección **Usuario**, seleccione la casilla **Ejecutar la tarea como**.
5. En el campo **Nombre**, ingrese el nombre de la cuenta de usuario cuyos derechos son necesarios para acceder al origen de actualizaciones.
6. En el campo **Contraseña**, escriba la contraseña del usuario cuyos permisos son necesarios para acceder al origen de actualizaciones.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de las actualizaciones de los módulos de la aplicación

Para configurar las actualizaciones de los módulos de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.

   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.
3. En la sección **Adicional**, realice una de las siguientes acciones:

   - Seleccione la casilla **Descargar actualizaciones de módulos de la aplicación** si quiere que la aplicación incluya las actualizaciones de los módulos de aplicación en los paquetes de actualización.
   - De lo contrario, desmarque la casilla **Descargar actualizaciones de módulos de la aplicación**.
4. Si se seleccionó **Descargar actualizaciones de módulos de la aplicación** en el paso anterior, especifique las condiciones en las cuales la aplicación instalará las actualizaciones de los módulo de la aplicación:

   - Seleccione la opción **Instalar actualizaciones críticas y aprobadas** si quiere que la aplicación instale las actualizaciones críticas de los módulos de la aplicación en forma automática, y otras actualizaciones luego de que se haya aprobado su instalación en forma local a través de la interfaz de la aplicación o por medio de Kaspersky Security Center.
   - Seleccione la opción **Instalar solo actualizaciones aprobadas** si quiere que la aplicación instale las actualizaciones de los módulos de la aplicación luego de que se haya aprobado su instalación en forma local a través de la interfaz de la aplicación o por medio de Kaspersky Security Center.
5. Para guardar los cambios, haga clic en el botón **Guardar**.

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 descargar un paquete de actualización de los servidores de Kaspersky, se requiere una conexión a Internet.

Para iniciar o detener una tarea de actualización:

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

   Se abre la ventana **Tareas**.
2. Haga clic en la sección con el nombre de la tarea de actualización.

   La sección seleccionada se amplía.
3. Realice una de las siguientes acciones:

   - Si desea iniciar la tarea de actualización, seleccione **Iniciar** en el menú.

El estado del progreso de la tarea que se muestra debajo del nombre de la tarea de actualización cambia a *En ejecución*.

- Si desea detener la tarea de actualización, seleccione **Detener** en el menú.

  El estado del progreso de la tarea que se muestra debajo del nombre de la tarea de actualización cambia a *Detenido*.

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

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. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Tareas**.

   Se abre la sección **Tareas**.
4. Haga clic con el botón derecho para mostrar el menú contextual de la tarea **Actualizar**.
5. Seleccione **Revertir la actualización**.

Configuración de parámetros del servidor proxy

Para configurar los parámetros del servidor proxy:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Actualizar**.
   En la parte derecha de la ventana, se muestra la Configuración de actualización de la aplicación.
3. En la sección **Servidor proxy**, haga clic en el botón **Configuración**.
   Se abre la ventana **Configuración del servidor proxy**.
4. En la ventana **Configuración del servidor proxy**, seleccione la casilla **Usar servidor proxy**.
5. Especifique la configuración del servidor proxy.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

También puede configurar los parámetros del servidor proxy en la ventana principal de la aplicación, en la ficha **Configuración**, en la sección **Configuración avanzada**.

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.

En esta sección se describen las características específicas y la configuración de tareas de análisis, niveles de seguridad, métodos y tecnologías de análisis e instrucciones sobre el manejo de archivos que Kaspersky Endpoint Security no procesó durante el análisis antivirus.

Acerca de las tareas de análisis

Para encontrar virus y otros tipos de malware, y comprobar la integridad de los módulos de la aplicación, Kaspersky Endpoint Security incluye las siguientes tareas:

- **Análisis completo**. Análisis detallado de todo el equipo. Por defecto, 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
- **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.
- **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
  - Buzón de correo de Outlook
  - Todos los discos duros, los discos extraíbles y de red
  - Cualquier archivo seleccionado
- **Comprobación de integridad**. Kaspersky Endpoint Security comprueba si los módulos de la aplicación presentan fallas o modificaciones.

Las tareas Análisis completo y Análisis de áreas críticas son algo diferentes de las otras. Para estas tareas, no se recomienda modificar el alcance del análisis.

Una vez iniciadas las tareas de análisis, su progreso se muestra en el campo adyacente al nombre de la tarea de análisis en ejecución, en la sección **Tareas** de la ficha **Protección y Control** de la ventana principal de Kaspersky Endpoint Security.

La información sobre los eventos y resultados del análisis, que se han producido durante la ejecución de las tareas de análisis, se registra en el informe de Kaspersky Endpoint Security.

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. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Tareas**.

   Se abre la sección **Tareas**.
4. Haga clic con el botón derecho para mostrar el menú contextual de la línea con el nombre de la tarea de análisis.

   Se abre un menú con las acciones de la tarea de análisis.
5. Realice una de las siguientes acciones:

   - Si desea iniciar la tarea de análisis, seleccione **Iniciar el análisis** en el menú.

     El estado del progreso de la tarea, que se muestra a la derecha del botón con el nombre de esta tarea de análisis, cambia a *En ejecución*.
   - Si desea detener la tarea de análisis, seleccione **Detener el análisis** en el menú.

     El estado del progreso de la tarea, que se muestra a la derecha del botón con el nombre de esta tarea de análisis, cambia a *Detenido*.

Configuración de los parámetros de una tarea de análisis

Para configurar los parámetros de una tarea de análisis, puede hacer lo siguiente:

- Modificar el nivel de seguridad.

  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.
- Cambiar la acción que realiza Kaspersky Endpoint Security si detecta un archivo infectado.
- Modificar el alcance del análisis.

  Puede ampliar o reducir el alcance del análisis agregando o eliminando objetos, o cambiando el tipo de archivos que se analizarán.
- Optimizar el análisis.

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 activar el uso de las tecnologías iChecker y iSwift. Estas tecnologías optimizan la velocidad de análisis de archivos al excluir archivos que no se modificaron desde el último análisis.

- Configurar el análisis de archivos compuestos.
- Configurar los métodos de análisis.

  Kaspersky Endpoint Security utiliza usa una técnica de 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 análisis de firmas está siempre habilitado.

  Para aumentar la efectividad de la protección, puede utilizar el análisis heurístico. Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de objetos en el sistema operativo. El análisis heurístico puede detectar objetos maliciosos sobre los cuales no existen registros en las bases de datos de Kaspersky Endpoint Security.

- Seleccionar el modo de ejecución de 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 para después del inicio de la aplicación si seleccionó el modo de ejecución de la tarea de actualización **Mediante programación** y el tiempo de inicio de Kaspersky Endpoint Security coincide con la programación de la ejecución de la tarea de análisis. La tarea de análisis solo se puede ejecutar una vez transcurrido el intervalo de tiempo especificado después del inicio de Kaspersky Endpoint Security.

- Configurar la tarea de análisis para que se ejecute con una cuenta de usuario diferente.
- Especificar la configuración del análisis de unidades extraíbles cuando se conectan.

Modificación del nivel de seguridad

Para realizar tareas de análisis, Kaspersky Endpoint Security utiliza varias combinaciones de parámetros. Estas combinaciones de parámetros guardadas en la aplicación se llaman *niveles de seguridad*. Existen tres niveles de seguridad predeterminados: **Alto**, **Recomendado** y **Bajo**. Se considera que la configuración del nivel de seguridad **Recomendado** es óptima. Es el nivel recomendado por los expertos de Kaspersky.

Para cambiar un nivel de seguridad:

1. En la ventana principal de la aplicación, haga clic en el botón **Configuración**.
2. En la parte izquierda de la ventana, en la sección **Tareas**, seleccione la subsección con el nombre de la tarea de análisis deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. En la sección **Nivel de seguridad**, realice una de las siguientes acciones:

   - Si desea aplicar uno de los niveles de seguridad predeterminados (**Alto**, **Recomendado** o **Bajo**), selecciónelo con el control deslizante.

- Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** y, en la ventana que se abre, especifique la configuración con el nombre de la tarea de análisis.

  Después de configurar un nivel personalizado de seguridad, el nombre del nivel de seguridad que aparece en la sección **Nivel de seguridad** cambia a **Personalizado**.

- Si desea cambiar el nivel de seguridad al nivel **Recomendado**, haga clic en el botón **Predeterminado**.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de la acción que se llevará a cabo en archivos infectados

Para modificar la acción que se llevará a cabo en archivos infectados:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Acción al detectar una amenaza**, seleccione la opción que desee:

   - **Seleccionar acción automáticamente**.

   - **Realizar acción**.

4. Si seleccionó la opción **Realizar acción** en el paso anterior, seleccione las siguientes casillas:

   - Seleccione la casilla **Desinfectar** si desea que Kaspersky Endpoint Security desinfecte objetos en los que se hayan detectado amenazas.

     Incluso si esta opción está seleccionada, Kaspersky Endpoint Security realiza la acción **Eliminar** en los archivos que son parte de la aplicación Tienda Windows.

   - Seleccione la casilla **Eliminar** si desea que Kaspersky Endpoint Security elimine objetos en los que se hayan detectado amenazas.

   - Seleccione las casillas **Desinfectar** y **Eliminar** si desea que Kaspersky Endpoint Security intente desinfectar objetos en los que se hayan detectado amenazas y eliminar los objetos que no se puedan desinfectar.

   - Desmarque las casillas **Desinfectar** y **Eliminar** si desea que Kaspersky Endpoint Security no tome ninguna medida con respecto a los objetos en los que se hayan detectado amenazas y que, en cambio, simplemente notifique al usuario sobre el resultado del análisis de estos objetos.

5. Para guardar los cambios, haga clic en el botón **Guardar**.

Generar una lista de objetos para analizar

Para generar una lista de objetos para analizar, puede usar uno de los dos métodos siguientes:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

> Este método solo está disponible para las tareas **Análisis completo** y **Análisis de áreas críticas**. La lista de objetos para analizar en la tarea **Análisis personalizado** solo se puede crear en la ficha **Protección y control**.

Para crear una lista de objetos para analizar en la ficha Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Tareas**.

   Se abre la sección **Tareas**.
4. Haga clic con el botón derecho del mouse para abrir el menú contextual de la línea que contiene el nombre de la tarea y seleccione **Alcance del análisis**.

   Se abre la ventana **Alcance del análisis**.
5. Si quiere agregar un objeto nuevo al alcance del análisis:

   a. Haga clic en el botón **Agregar**.

      Se abre la ventana **Seleccionar alcance del análisis**.

   b. Seleccione el objeto y haga clic en **Agregar**.

      Todos los objetos seleccionados en la ventana **Seleccionar alcance del análisis** se muestran en la lista **Alcance del análisis**.

   c. Haga clic en **Aceptar**.
6. Si quiere cambiar la ruta a un objeto en el alcance del análisis:

   a. Seleccione el objeto en el alcance del análisis.

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

      Se abre la ventana **Seleccionar alcance del análisis**.

   c. Escriba la ruta nueva al objeto en el alcance del análisis.

   d. Haga clic en **Aceptar**.
7. Si quiere quitar un objeto del alcance del análisis:

   a. Seleccione el objeto que quiera quitar del alcance del análisis.

      Para seleccionar múltiples objetos, mantenga presionada la tecla **CTRL**.

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

      Se abre una ventana para confirmar la eliminación.

   c. Haga clic en **Sí** en la ventana de confirmación de la eliminación.

No puede quitar ni modificar objetos que estén incluidos en el alcance del análisis predeterminado.

8. Para excluir un objeto del alcance del análisis, desmarque la casilla adyacente al objeto en la ventana **Alcance del análisis**.

   El objeto permanecerá en la lista de objetos del alcance del análisis, pero no se lo analizará al ejecutar la tarea de análisis.

9. Haga clic en **Aceptar**.

10. Para guardar los cambios, haga clic en el botón **Guardar**.

Para crear una lista de objetos para analizar desde la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis necesaria: **Análisis completo** o **Análisis de áreas críticas**.

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. Haga clic en el botón **Alcance del análisis**.

   Se abre la ventana **Alcance del análisis**.

4. Cree una lista de objetos para analizar siguiendo los pasos 5 a 10 de las instrucciones anteriores.

Selección del tipo de archivos para analizar

Puede usar los dos métodos siguientes para seleccionar el tipo de archivos para analizar:

- Ficha **Protección y control** de la ventana principal de la aplicación.
- Desde la ventana de configuración de la aplicación.

Este método solo está disponible para las tareas **Análisis completo** y **Análisis de áreas críticas**. Los tipos de archivos para analizar con la tarea **Análisis personalizado** solo se pueden seleccionar en la ficha **Protección y control**.

Para seleccionar el tipo de archivos para analizar en la ficha Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.

2. Seleccione la ficha **Protección y control**.

3. Haga clic en la sección **Tareas**.

   Se abre la sección **Tareas**.

4. Haga clic con el botón derecho del mouse para abrir el menú contextual de la línea que contiene el nombre de la tarea y seleccione **Configuración**.

   Se abrirá una ventana con el nombre de la tarea de análisis seleccionada.

5. En la ventana con el nombre de la tarea de análisis seleccionada, seleccione la ficha **Alcance**.

6. En la sección **Tipos de archivos**, especifique el tipo de archivos que desea analizar cuando se ejecute la tarea de análisis seleccionada:

   - Si desea analizar todos los archivos, seleccione **Todos los archivos**.
   - Si desea analizar archivos con los formatos más vulnerables a infecciones, seleccione **Archivos analizados según su formato**.
   - Si quiere analizar archivos con las extensiones habitualmente más vulnerables a infecciones, seleccione **Archivos analizados según su extensión**.

   Cuando seleccione el tipo de archivos por analizar, tenga presenta la siguiente información:

   - Para algunos formatos de archivos (por ejemplo, TXT), hay una baja probabilidad de intrusión de código malicioso y su posterior activación. Además, otros formatos contienen o pueden contener código ejecutable (por ejemplo, .exe, .dll y .doc). El riesgo de que el código malicioso ingrese en estos archivos y se active es alto.
   - Un intruso puede enviar un virus u otro programa malicioso al equipo en un archivo ejecutable al que se le ha cambiado el nombre con la extensión .txt. 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, el Antivirus de archivos analiza el encabezado del archivo independientemente de la extensión. Si este análisis revela que el archivo tiene formato EXE, la aplicación lo analiza.

7. En la ventana que contiene el nombre de la tarea de análisis, haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Para seleccionar el tipo de archivos para analizar desde la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis necesaria: **Análisis completo** o **Análisis de áreas críticas**.

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abrirá una ventana con el nombre de la tarea de análisis seleccionada.

4. En la ventana con el nombre de la tarea de análisis seleccionada, seleccione la ficha **Alcance**.

5. Complete los pasos 5 a 7 de las instrucciones anteriores.

Optimización del análisis de archivos

Para optimizar el análisis de archivos:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abrirá una ventana con el nombre de la tarea de análisis seleccionada.

4. En la ventana que se abre, seleccione la ficha **Alcance**.

5. En la sección **Optimización del análisis**, realice las siguientes acciones:

   - Seleccione la casilla **Analizar solo archivos nuevos y modificados**.
   - Seleccione la casilla **Omitir archivos que se analicen por más de** y especifique la duración del análisis para un único archivo (en segundos).

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abrirá una ventana con el nombre de la tarea de análisis seleccionada.

4. En la ventana que se abre, seleccione la ficha **Alcance**.

5. 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.

6. Si se desmarca la casilla **Analizar solo archivos nuevos y modificados** en la sección **Optimización del análisis**, haga clic en el vínculo **todos/nuevos** adyacente al nombre del tipo de archivo compuesto si quiere especificar, para cada tipo de archivo compuesto, si se analizarán todos los archivos de este tipo o solo los nuevos archivos de este tipo.

   Cuando hace clic en el vínculo, el valor de ese vínculo cambia.

   Si la casilla **Analizar solo archivos nuevos y modificados** está seleccionada, se analizan solamente los archivos nuevos.

7. Haga clic en el botón **Adicional**.

Se abre la ventana **Archivos compuestos**.

8. En la sección **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.

9. Haga clic en **Aceptar**.
10. En la ventana con el nombre de la tarea de análisis, haga clic en **Aceptar**.
11. Para guardar los cambios, haga clic en el botón **Guardar**.

Uso de métodos de análisis

Para utilizar métodos de análisis:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abrirá una ventana con el nombre de la tarea de análisis seleccionada.
4. En la ventana que se abre, seleccione la ficha **Adicional**.
5. Si desea que la aplicación utilice el análisis heurístico cuando ejecute la tarea de análisis, en la sección **Métodos de análisis**, seleccione la casilla **Análisis heurístico**. Luego, utilice el control deslizante para definir el nivel del análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis profundo**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Uso de tecnologías de análisis

Para utilizar tecnologías de análisis:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea de análisis deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Nivel de seguridad**, haga clic en **Configuración**.

   Se abrirá una ventana con el nombre de la tarea de análisis seleccionada.

4. En la ventana que se abre, seleccione la ficha **Adicional**.

5. En la sección **Tecnologías de análisis**, seleccione las casillas junto a los nombres de las tecnologías que desea utilizar durante el análisis.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Seleccionar el modo de ejecución para la tarea de análisis

Para seleccionar el modo de ejecución de la tarea de análisis:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. Haga clic en el botón **Modo de ejecución**.

   Se abre una ventana con las propiedades de la tarea seleccionada en la ficha **Modo de ejecución**.

4. En la sección **Modo de ejecución**, seleccione el modo de ejecución de la tarea: **Manual** o **Mediante programación**.

5. Si seleccionó la opción **Mediante programación**, especifique la configuración de la programación. Para hacerlo:

   a. En la lista desplegable **Frecuencia**, seleccione la frecuencia de ejecución de la tarea (**Minutos**, **Horas**, **Días**, **Cada semana**, **En el momento especificado**, **Cada mes**o **Después del inicio de la aplicación**, **Después de cada actualización**).

   b. Según la frecuencia seleccionada, defina configuraciones avanzadas que especifiquen la programación de ejecución de la tarea.

   c. Si desea que Kaspersky Endpoint Security inicie las tareas de análisis ignoradas lo antes posible, seleccione la casilla **Ejecutar tareas omitidas**.

   > Si en la lista desplegable de **Frecuencia** se seleccionó el elemento **Minutos**, **Horas**, **Después del inicio de la aplicación** o **Después de cada actualización**, la casilla **Ejecutar tareas omitidas** no está disponible.

   a. 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**.

Esta opción de programación permite conservar recursos del equipo.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione la subsección con el nombre de la tarea deseada (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

   En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. Haga clic en el botón **Modo de ejecución**.

   Se abre una ventana con las propiedades de la tarea seleccionada en la ficha **Modo de ejecución**.

4. En la ficha **Modo de ejecución**, en la sección **Usuario**, seleccione la casilla **Ejecutar la tarea como**.

5. En el campo **Nombre**, ingrese el nombre de la cuenta de usuario cuyos derechos sean necesarios para iniciar la tarea de análisis.

6. En el campo **Contraseña**, escriba la contraseña del usuario cuyos permisos sean necesarios para iniciar la tarea de análisis.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Análisis de discos extraíbles cuando se conectan al equipo

Algunos programas maliciosos aprovechan las vulnerabilidades del sistema operativo para replicarse a través de redes de área local y discos extraíbles. Kaspersky Endpoint Security le permite analizar los discos extraíbles en busca de virus y otras clases de malware cuando se conectan al equipo.

Para configurar el análisis de los discos extraíbles cuando se conectan:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, seleccione la sección **Tareas programadas**.

   La configuración de la tarea se muestra en la parte derecha de la ventana.

3. En la sección **Analizar unidades extraíbles al conectarlas**, en la lista desplegable **Acción al conectarse una unidad extraíble**, seleccione la acción requerida:

   - **No analizar**
   - **Análisis detallado**

     En este modo, Kaspersky Endpoint Security analiza todos los archivos presentes en el disco extraíble, incluidos los que se encuentran dentro de objetos compuestos.

   - **Análisis rápido**

     En este modo, Kaspersky Endpoint Security analiza archivos potencialmente infectables y no descomprime objetos compuestos.

4. Si desea que Kaspersky Endpoint Security analice solamente los discos extraíbles con un tamaño que no exceda el valor especificado, seleccione la casilla **Tamaño máximo de la unidad extraíble** y especifique un valor en megabytes en el campo adyacente.

5. Para guardar los cambios, haga clic en el botón **Guardar**.

Manejo de archivos no procesados

Esta sección contiene instrucciones sobre el manejo de archivos infectados y probablemente infectados que Kaspersky Endpoint Security no procesó mientras analizaba el equipo en busca de virus y otras amenazas.

Acerca de los archivos no procesados

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 archivos no procesados.

Un archivo infectado se considera *procesado* si Kaspersky Endpoint Security realiza una de las siguientes acciones en 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.

Un archivo infectado se considera *sin procesar* si Kaspersky Endpoint Security, por cualquier motivo, no realizó una acción en este archivo infectado de acuerdo con la configuración de la aplicación especificada mientras analiza 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.

Puede iniciar manualmente una tarea de análisis personalizado para los archivos de la lista de archivos no procesados luego de la actualización de bases de datos y los módulos de la aplicación. Es posible que el estado del archivo cambie después del análisis. Puede realizar las acciones necesarias en los archivos, según su estado.

Por ejemplo, puede realizar las siguientes acciones:

- Eliminar archivos con el estado *Infectado*.
- Restaurar archivos infectados que contienen información importante y restaurar archivos marcados como *Desinfectados* o *No infectados*.
- Llevar a la Cuarentena los archivos con el estado *Probablemente infectado*.

Administración de la lista de archivos no procesados

La lista de archivos no procesados aparece en forma de tabla.

Puede realizar las siguientes operaciones con archivos sin procesar:

- Ver la lista de archivos no procesados.
- Analizar los archivos no procesados utilizando la versión actual de las bases de datos y los módulos de Kaspersky Endpoint Security.
- Restaurar archivos de la lista de archivos no procesados a sus carpetas originales o a una carpeta diferente de su preferencia (cuando no se pueda escribir la carpeta original).
- Eliminar archivos de la lista de archivos no procesados.
- Abrir la carpeta donde se encontraba el archivo sin procesar originalmente.

También puede realizar las siguientes acciones mientras administra los datos de la tabla:

- Filtrar eventos de archivos no procesados por el valor de columna o las condiciones de filtros personalizadas.
- Usar la función de búsqueda de eventos de archivos no procesados.
- Ordenar eventos de archivos no procesados.
- Cambiar el orden y el conjunto de columnas que se muestran en la lista de archivos no procesados.
- Agrupar eventos de archivos no procesados.

Puede copiar eventos de archivos no procesados seleccionados al portapapeles, si es necesario.

Inicio de una tarea de análisis personalizado de archivos no procesados

Puede iniciar manualmente una tarea de Análisis personalizado de los archivos no procesados. Puede iniciar el análisis si, por ejemplo, el último análisis se interrumpió por alguna razón o si desea que Kaspersky Endpoint Security vuelva a analizar archivos sin procesar después de la actualización más reciente de bases de datos y módulos de aplicación.

Para iniciar un análisis personalizado de archivos no procesados:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Archivos sin procesar**.
4. En la tabla de la ficha **Archivos sin procesar**, seleccione uno o más eventos asociados con los archivos que quiera analizar.

   Para seleccionar múltiples eventos, debe seleccionarlos mientras mantiene presionada la tecla **CTRL**.
5. Inicie la tarea de análisis personalizado de una de las siguientes formas:
   - Haga clic en el botón **Volver a analizar**.
   - Haga clic con el botón derecho del mouse para mostrar el menú contextual y seleccione **Volver a analizar**.

Eliminación de archivos de la lista de archivos no procesados

Para eliminar archivos de la lista de archivos no procesados:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Archivos sin procesar**.
4. En la tabla de la ficha **Archivos sin procesar**, seleccione uno o más eventos asociados con los archivos que quiera eliminar.

   Para seleccionar múltiples eventos, debe seleccionarlos mientras mantiene presionada la tecla **CTRL**.
5. Elimine archivos de una de las siguientes maneras:
   - Haga clic en el botón **Eliminar**.
   - Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Eliminar**.

Análisis de vulnerabilidades

Esta sección contiene información sobre los detalles y la configuración de la tarea del Análisis de vulnerabilidades, e instrucciones sobre cómo administrar la lista de vulnerabilidades detectadas por Kaspersky Endpoint Security mientras se ejecuta la tarea del Análisis de vulnerabilidades.

Visualización de información acerca de vulnerabilidades de aplicaciones en ejecución

La información sobre vulnerabilidades de aplicaciones en ejecución está disponible si Kaspersky Endpoint Security está instalado en un equipo en el que se ejecuta Microsoft Windows para estaciones de trabajo. Esta información no está disponible si Kaspersky Endpoint Security está instalado en un equipo en el que se ejecuta Microsoft Windows para servidores de archivos.

Para ver información sobre las vulnerabilidades de las aplicaciones que se están ejecutando:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Abra la sección **Control del endpoint**.
4. Haga clic en el botón **Monitor de aplicaciones**.

   Se abre la ventana **Control de privilegios de aplicaciones** en la ficha **Monitor de aplicaciones**. En la tabla **Monitor de actividad de la aplicación** se muestra un resumen de la información sobre la actividad de las aplicaciones que se están ejecutando en el sistema operativo. La gravedad de la vulnerabilidad de las aplicaciones que se están ejecutando, determinado por el componente Monitor de vulnerabilidades, se muestra en la columna **Gravedad de la vulnerabilidad**.

Acerca de la tarea del Análisis de vulnerabilidades

Las vulnerabilidades del sistema operativo pueden ser causadas, por ejemplo, por errores de programación o diseño, contraseñas débiles o actividad de malware. Al analizar las vulnerabilidades, la aplicación analiza el sistema operativo y busca anomalías y parámetros dañados de aplicaciones de Microsoft u otros proveedores.

El análisis de vulnerabilidades realiza el diagnóstico de seguridad del sistema operativo y detecta las funciones de software que los intrusos pueden usar para propagar objetos maliciosos y obtener acceso a información personal.

Una vez iniciada la tarea del Análisis de vulnerabilidades, su progreso se muestra en el campo adyacente al nombre de la tarea del **Análisis de vulnerabilidades** en la sección **Tareas** de la ficha **Protección y control** de la ventana principal de Kaspersky Endpoint Security.

Los resultados de la tarea del Análisis de vulnerabilidades se registran en informes.

Inicio o detención de la tarea del Análisis de vulnerabilidades

Independientemente del modo de ejecución seleccionado para la tarea Análisis de vulnerabilidades, puede iniciar o detener la tarea en cualquier momento.

Para iniciar o detener la tarea Análisis de vulnerabilidades:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Haga clic en la sección **Tareas**.

   Se abre la sección **Tareas**.
4. Haga clic con el botón derecho del mouse para mostrar el menú contextual de la línea con el nombre de la tarea Análisis de vulnerabilidades.

   Se abre un menú de operaciones de la tarea Análisis de vulnerabilidades.
5. Realice una de las siguientes acciones:

   - Para iniciar la tarea Análisis de vulnerabilidades, seleccione **Iniciar el análisis** en el menú.

     El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de la tarea Análisis de vulnerabilidades cambia a *En ejecución*.

   - Para detener la tarea Análisis de vulnerabilidades, seleccione **Detener el análisis** en el menú.

     El estado del progreso de la tarea, que se muestra a la derecha del botón con el nombre de la tarea Análisis de vulnerabilidades cambia a *Detenido*.

Configuración de los parámetros del Análisis de vulnerabilidades

Para configurarla los parámetros del Análisis de vulnerabilidades, puede hacer lo siguiente:

- Crear el alcance del Análisis de vulnerabilidades.

  Puede expandir o contraer el alcance del análisis si agrega o quita aplicaciones que deban analizarse en busca de vulnerabilidades.

- Seleccionar el modo de ejecución para la tarea del Análisis de vulnerabilidades.

  Si no es posible ejecutar la tarea por alguna razón (por ejemplo: el equipo estaba apagado en ese momento), puede configurar la tarea omitida para que se ejecute automáticamente tan pronto como sea posible.

- Configurar la tarea para que se ejecute con los derechos de una cuenta de 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 derechos adecuados en la configuración de la tarea y ejecutarla con la cuenta de este usuario.

Creación del alcance del análisis de vulnerabilidades

El alcance del análisis de vulnerabilidades es el proveedor de software o la ruta de la carpeta en la que se instaló el software (por ejemplo, todas las aplicaciones de Microsoft instaladas en la carpeta Archivos de programa).

Para crear un alcance del análisis de vulnerabilidades, realice lo siguiente:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Análisis de vulnerabilidades**.
   En la parte derecha de la ventana, se muestra la configuración de la tarea Análisis de vulnerabilidades.
3. En la sección **Alcance del análisis**:
   a. Para que Kaspersky Endpoint Security busque vulnerabilidades en las aplicaciones de Microsoft instaladas en el equipo, seleccione la casilla **Microsoft**.
   b. Para que Kaspersky Endpoint Security busque vulnerabilidades en todas las aplicaciones instaladas en el equipo que no sean de Microsoft, seleccione la casilla **Otros proveedores**.
   c. En la ventana **Área de análisis de vulnerabilidades adicional**, haga clic en el botón **Configuración**.
   Se abre la ventana **Alcance del análisis de vulnerabilidades**.
   d. Cree el alcance del análisis de vulnerabilidades. Para hacerlo, utilice los botones **Agregar** y **Eliminar**.
   e. En la ventana **Alcance del análisis de vulnerabilidades**, haga clic en **Aceptar**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Selección del modo de ejecución para la tarea del Análisis de vulnerabilidades

Para seleccionar el modo de ejecución de la tarea del Análisis de vulnerabilidades:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Análisis de vulnerabilidades**.
   En la parte derecha de la ventana, se muestra la configuración de la tarea Análisis de vulnerabilidades.
3. Haga clic en el botón **Modo de ejecución**.
   Se abre la ficha **Modo de ejecución** de la ventana **Análisis de vulnerabilidades**.
4. En la sección **Modo de ejecución**, seleccione una de las siguientes opciones de modo de ejecución para iniciar la tarea Análisis de vulnerabilidades:
   - Si desea iniciar la tarea Análisis de vulnerabilidades manualmente, seleccione **Manual**.
   - Si desea configurar una programación de inicio de la tarea Análisis de vulnerabilidades, seleccione **Mediante programación**.
5. Realice una de las siguientes acciones:
   - Si seleccionó la opción **Manual**, vaya al paso 6 de estas instrucciones.
   - Si seleccionó la opción **Mediante programación**, especifique la configuración de inicio de la tarea Análisis de vulnerabilidades. Para hacerlo:

a. En la lista desplegable **Frecuencia**, especifique cuándo se debe iniciar la tarea Análisis de vulnerabilidades. Seleccione una de las siguientes opciones: **Días**, **Cada semana**, **En el momento especificado**, **Cada mes**, **Después del inicio de la aplicación** o **Después de cada actualización**.

b. Según el elemento seleccionado en la lista desplegable **Frecuencia**, especifique los valores para la configuración que define el momento de inicio de la tarea Análisis de vulnerabilidades.

c. Si desea que Kaspersky Endpoint Security ejecute lo antes posible las tareas Análisis de vulnerabilidades omitidas, seleccione la casilla **Ejecutar tareas omitidas**.

> Si en la lista desplegable **Frecuencia** se seleccionaron las opciones **Después del inicio de la aplicación** o **Después de cada actualización**, la casilla **Ejecutar tareas omitidas** no está disponible.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Inicio de la tarea del Análisis de vulnerabilidades utilizando los derechos de una cuenta de usuario distinta

Por defecto, la tarea Análisis de vulnerabilidades se inicia con la cuenta que el usuario usa para iniciar sesión en el sistema operativo. Sin embargo, es posible que deba iniciar la tarea Análisis de vulnerabilidades con una cuenta de usuario distinta. Puede especificar un usuario con estos permisos en la configuración de la tarea Análisis de vulnerabilidades e iniciar dicha tarea con la cuenta de este usuario.

Para configurar el inicio de la tarea Análisis de vulnerabilidades con otra cuenta de usuario:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Análisis de vulnerabilidades**.

   En la parte derecha de la ventana, se muestra la configuración de la tarea Análisis de vulnerabilidades.

3. Haga clic en el botón **Modo de ejecución**.

   Se abre la ficha **Modo de ejecución** de la ventana **Análisis de vulnerabilidades**.

4. En la ficha **Modo de ejecución**, en la sección **Usuario**, seleccione la casilla **Ejecutar la tarea como**.

5. En el campo **Nombre**, escriba el nombre de la cuenta del usuario cuyos permisos son necesarios para iniciar la tarea Análisis de vulnerabilidades.

6. En el campo **Contraseña**, escriba la contraseña del usuario cuyos permisos son necesarios para iniciar la tarea Análisis de vulnerabilidades.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Administración de la lista de vulnerabilidades

Mientras administra la lista de vulnerabilidades, puede realizar las siguientes acciones:

- Ver la lista de vulnerabilidades.
- Iniciar la tarea Análisis de vulnerabilidades luego de actualizar las bases de datos y los módulos de la aplicación.
- Ver información detallada sobre la vulnerabilidad y las recomendaciones para su reparación en una sección separada.
- Ocultar entradas seleccionadas en la lista de vulnerabilidades.
- Filtrar la lista de vulnerabilidades por nivel de importancia.
- Filtrar la lista de vulnerabilidades por los valores de estado *Reparado* y *Oculto*.

También puede realizar las siguientes acciones mientras administra los datos de la tabla:

- Filtrar la lista de vulnerabilidades por valores de columna o por condiciones de filtros personalizadas.
- Usar la función de búsqueda de vulnerabilidades.
- Ordenar las entradas en la lista de vulnerabilidades.
- Cambiar el orden y la organización de las columnas que se muestran en la lista de vulnerabilidades.
- Agrupar las entradas en la lista de vulnerabilidades.

Acerca de la lista de vulnerabilidades

Kaspersky Endpoint Security registra los resultados de la tarea del Análisis de vulnerabilidades en la lista de vulnerabilidades.

Luego de que usted revise vulnerabilidades específicas y ejecute las acciones recomendadas para repararlas, Kaspersky Endpoint Security cambiará el estado de las vulnerabilidades a *Reparadas*.

Si usted no desea mostrar las entradas sobre vulnerabilidades específicas en la lista de vulnerabilidades, puede elegir ocultar dichas entradas. Kaspersky Endpoint Security asigna a dichas vulnerabilidades el estado *Oculto*.

La lista de vulnerabilidades aparece en forma de tabla. Cada fila de la tabla contiene la siguiente información:

- Un icono que indica el nivel de gravedad de la vulnerabilidad. Existen los siguientes niveles de gravedad de las vulnerabilidades:
  - Icono . **Crítico**. Este nivel de gravedad se aplica a las vulnerabilidades altamente peligrosas que deben repararse sin demora. Los intrusos aprovechan activamente las vulnerabilidades de este nivel para infectar el sistema operativo del equipo o acceder a los datos personales del usuario. Kaspersky recomienda que tome todas las medidas necesarias de inmediato para corregir las vulnerabilidades del nivel de gravedad “crítico”.
  - Icono . **Importantes**. Este nivel de gravedad se aplica a las vulnerabilidades importantes que deben repararse enseguida. Los intrusos pueden aprovecharse activamente de las vulnerabilidades de este nivel. En este momento los intrusos no se aprovechan activamente de las vulnerabilidades del nivel de gravedad “importante”. Kaspersky recomienda que tome todas las medidas necesarias de inmediato para corregir las vulnerabilidades del nivel de gravedad “importante”.

- Icono . **Advertencia**. Este nivel de gravedad se aplica a las vulnerabilidades cuya reparación puede posponerse. No obstante, dichas vulnerabilidades pueden suponer una amenaza para la seguridad del equipo en el futuro.

- Id. de la vulnerabilidad.
- Nombre de la aplicación en la que se detectó la vulnerabilidad.
- Breve descripción de la vulnerabilidad.
- Información sobre el fabricante del software, tal como se indica en la firma digital.
- Resultado de acciones realizadas para reparar la vulnerabilidad.

Volver a iniciar la tarea Análisis de vulnerabilidades

Para actualizar información sobre vulnerabilidades previamente detectadas, puede volver a iniciar la tarea Análisis de vulnerabilidades. Es posible que tenga que reiniciar la tarea de análisis si el análisis de vulnerabilidades se interrumpiera por algún motivo o si desea analizar el equipo en busca de vulnerabilidades después de la última actualización de bases de datos y módulos de la aplicación.

Para volver a iniciar la tarea Análisis de vulnerabilidades:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Vulnerabilidades**.

   La ficha **Vulnerabilidades** contiene una lista de vulnerabilidades que Kaspersky Endpoint Security ha detectado durante la tarea Análisis de vulnerabilidades.
4. En la esquina inferior derecha de la ventana **Depósitos**, haga clic en el botón **Volver a analizar**.

Kaspersky Endpoint Security actualiza información detallada sobre vulnerabilidades en la lista de vulnerabilidades.

El estado de una vulnerabilidad que ha sido reparada por la instalación de una revisión propuesta no cambia después de otro análisis de vulnerabilidades.

Reparación de una vulnerabilidad

Puede reparar una vulnerabilidad si instala una actualización de sistema operativo, cambia la configuración de la aplicación o instala una revisión de la aplicación.

Es posible que las vulnerabilidades detectadas no correspondan a las aplicaciones instaladas, sino a sus copias. Una revisión puede reparar una vulnerabilidad solo si la aplicación está instalada.

Para reparar una vulnerabilidad:

1. Abra la ventana principal de la aplicación.

2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.

3. En la ventana **Depósitos**, seleccione la ficha **Vulnerabilidades**.

   La ficha **Vulnerabilidades** contiene una lista de vulnerabilidades que Kaspersky Endpoint Security ha detectado durante la tarea Análisis de vulnerabilidades.

4. En la lista de vulnerabilidades, seleccione la entrada que corresponde a la vulnerabilidad relevante.

   Se abre una sección con información sobre esta vulnerabilidad y recomendaciones sobre cómo repararla al final de la lista de vulnerabilidades.

   La siguiente información está disponible para cada vulnerabilidad seleccionada:

   - Nombre de la aplicación en la que se detectó la vulnerabilidad.
   - Versión de la aplicación en la que se detectó la vulnerabilidad.
   - Nivel de gravedad de una vulnerabilidad.
   - Id. de la vulnerabilidad.
   - Fecha y hora de la detección de la última vulnerabilidad.
   - Recomendación para reparar la vulnerabilidad (por ejemplo, un vínculo a un sitio web con una actualización de sistema operativo o con una revisión de la aplicación).
   - Vínculo a un sitio web con la descripción de la vulnerabilidad.

5. Para ver una descripción detallada de la vulnerabilidad, haga clic en el vínculo **Información adicional** para abrir una página web con la descripción de la amenaza asociada con la vulnerabilidad seleccionada. En el sitio web www.secunia.com puede descargar la actualización necesaria para la versión actual de la aplicación e instalarla.

6. Seleccione una de las siguientes formas de reparar una vulnerabilidad:

   - Si hay una o más revisiones disponibles para la aplicación, instale la revisión necesaria siguiendo las instrucciones que se proporcionan junto al nombre de la revisión.
   - Si hay una actualización del sistema operativo disponible, instale la actualización necesaria siguiendo las instrucciones que se proporcionan junto al nombre de la actualización.

   La vulnerabilidad se repara luego de instalar la revisión o actualización. Kaspersky Endpoint Security asigna a la vulnerabilidad un estado que indica que la vulnerabilidad está reparada. La entrada sobre la vulnerabilidad reparada se muestra en color gris en la lista de vulnerabilidades.

7. Si no se proporciona información sobre cómo reparar la vulnerabilidad en la parte inferior de la ventana, puede iniciar nuevamente la tarea Análisis de vulnerabilidades después de actualizar las bases de datos y los módulos de Kaspersky Endpoint Security. Como Kaspersky Endpoint Security analiza el sistema en busca de vulnerabilidades mediante la comparación con una base de datos de vulnerabilidades, es posible que aparezca una entrada sobre una vulnerabilidad reparada luego de actualizar la aplicación.

Ocultar entradas en la lista de vulnerabilidades

Puede ocultar una entrada de vulnerabilidad seleccionada. Kaspersky Endpoint Security asigna el estado *Oculto* a entradas seleccionadas en la lista de vulnerabilidades y marcadas como ocultas. Luego puede filtrar la lista de vulnerabilidades conforme al valor del estado *Oculto*.

Para ocultar entradas en la lista de vulnerabilidades:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Vulnerabilidades**.

   La ficha **Vulnerabilidades** contiene una lista de vulnerabilidades que Kaspersky Endpoint Security ha detectado durante la tarea Análisis de vulnerabilidades.
4. En la lista de vulnerabilidades, seleccione la entrada correspondiente a la vulnerabilidad que desea ocultar.

   Se abre una sección con información sobre esta vulnerabilidad y recomendaciones sobre cómo repararla al final de la lista de vulnerabilidades.
5. Haga clic en el botón **Ocultar**.

   Kaspersky Endpoint Security asigna el estado *Oculto* a la vulnerabilidad seleccionada. Las entradas sobre las vulnerabilidades en estado *Oculto* se pasan al final de la lista de vulnerabilidades y aparecen en gris.
6. Para ocultar la entrada correspondiente a una vulnerabilidad en la lista de vulnerabilidades, seleccione la casilla **Oculto** en la parte superior de la lista.

Filtrado de la lista de vulnerabilidades por nivel de gravedad

Para filtrar la lista de vulnerabilidades por nivel de gravedad:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Vulnerabilidades**.

   La ficha **Vulnerabilidades** contiene una lista de vulnerabilidades que Kaspersky Endpoint Security ha detectado durante la tarea Análisis de vulnerabilidades. Aparecen tres iconos del nivel de gravedad (Advertencia, Importante, Crítico) de la vulnerabilidad en la parte superior de la lista de vulnerabilidades en la fila **Mostrar gravedad**. Si hace clic en estos iconos, puede filtrar la lista de vulnerabilidades por nivel de gravedad.
4. Haga clic en uno, dos o tres de los iconos del nivel de gravedad de la vulnerabilidad. Las vulnerabilidades que coincidan con los niveles de gravedad seleccionados aparecen en la lista. Para dejar de mostrar vulnerabilidades que coincidan con un nivel de gravedad específico en la lista, vuelva a hacer clic en el icono del nivel de gravedad pertinente. Si no se selecciona ningún nivel de gravedad, la lista de vulnerabilidades aparece vacía.

Las condiciones de filtrado de las entradas de vulnerabilidad especificadas se guardan luego de cerrar la ventana **Depósitos**.

Filtrado de la lista de vulnerabilidades por los valores de estado Reparado y Oculto

Para filtrar la lista de vulnerabilidades por los valores de estado Reparado y Oculto:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Vulnerabilidades**.

   La ficha **Vulnerabilidades** contiene una lista de vulnerabilidades que Kaspersky Endpoint Security ha detectado durante la tarea Análisis de vulnerabilidades.
4. Las casillas que representan el estado de las vulnerabilidades se muestran junto a la opción de configuración **Mostrar vulnerabilidades**. Para filtrar la lista de vulnerabilidades por el estado *Reparada*, realice una de las siguientes acciones:

   - Para mostrar las entradas sobre vulnerabilidades reparadas en la lista de vulnerabilidades, seleccione la casilla **Reparada**. Las entradas sobre vulnerabilidades reparadas se muestran en color gris en la lista de vulnerabilidades.
   - Para ocultar las entradas sobre vulnerabilidades reparadas en la lista de vulnerabilidades, desactive la casilla **Reparada**.
5. Para filtrar la lista de vulnerabilidades por el estado *Oculto*, realice una de las siguientes acciones:

   - Para mostrar las entradas sobre vulnerabilidades ocultas en la lista de vulnerabilidades, seleccione la casilla **Oculto**. Las entradas sobre vulnerabilidades ocultas se muestran en color gris en la lista de vulnerabilidades.
   - Para ocultar las entradas sobre vulnerabilidades ocultas en la lista de vulnerabilidades, desactive la casilla **Oculto**.

Las condiciones de filtrado de las entradas de vulnerabilidad especificadas no se guardarán luego de cerrar la ventana **Depósitos**.

Comprobación de la integridad de los módulos de la aplicación

Esta sección contiene información sobre los detalles y la configuración de la tarea de comprobación de la integridad.

Acerca de la tarea de Comprobación de la 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.

Una vez iniciada la tarea de comprobación de la integridad, su progreso se muestra en el campo adyacente al nombre de la tarea en la sección **Tareas** de la ficha **Protección y control** de la ventana principal de Kaspersky Endpoint Security.

Los resultados de la tarea de comprobación de la integridad se registran en informes.

Inicio o detención de una tarea de comprobación de la integridad

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

Para iniciar o detener una tarea de comprobación de la integridad:

1. Abra la ventana principal de la aplicación.
2. Seleccione la ficha **Protección y control**.
3. Abra la sección **Tareas**.
4. Haga clic con el botón derecho del mouse para mostrar el menú contextual de la línea con el nombre de la tarea de comprobación de la integridad.
5. Realice una de las siguientes acciones:
   - Para iniciar la tarea de comprobación de la integridad, seleccione **Iniciar el análisis** en el menú contextual.

     El estado del progreso de la tarea, que se muestra a la derecha del botón con el nombre de esta tarea, pasa a *En ejecución*.
   - Si quiere detener la tarea de comprobación de la integridad, seleccione **Detener el análisis** en el menú contextual.

     El estado del progreso de la tarea, que se muestra a la derecha del botón con el nombre de esta tarea, pasa a *detenida*.

Selección del modo de ejecución para la tarea de comprobación de la integridad

Para seleccionar el modo de ejecución para la tarea de comprobación de la integridad:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Tareas programadas**, seleccione **Comprobación de integridad**.

   En la parte derecha de la ventana, se muestra la configuración de la tarea de comprobación de la integridad.
3. En la sección **Modo de ejecución**, elija una de las siguientes opciones:

   - Si quiere iniciar la tarea de comprobación de la integridad manualmente, seleccione **Manual**.
   - Si quiere configurar la programación del inicio de la tarea de comprobación de la integridad, seleccione **Mediante programación**.
4. Si seleccionó la opción **Mediante programación** en el paso anterior, especifique la configuración de la programación de ejecución de la tarea. Para hacerlo:

   a. En la lista desplegable **Frecuencia**, especifique cuándo se debe iniciar la tarea de comprobación de la integridad. Seleccione una de las siguientes opciones: **Minutos**, **Horas**, **Días**, **Cada semana**, **En el momento especificado**, **Cada mes** o **Después del inicio de la aplicación**.

   b. Según el elemento seleccionado en la lista desplegable **Frecuencia**, especifique los valores para la configuración que define cuándo se iniciará la tarea.

   c. Si quiere que Kaspersky Endpoint Security ejecute lo antes posible las tareas de comprobación de la integridad omitidas, seleccione la casilla **Ejecutar tareas omitidas**.

   > Si se selecciona el elemento **Después del inicio de la aplicación**, **Minutos** u **Horas** en la lista desplegable **Frecuencia**, la casilla **Ejecutar tareas omitidas** no estará disponible.

   d. 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**.

   Esta opción de programación permite conservar recursos del equipo.
5. Haga clic en **Aceptar**.
6. Para guardar los cambios, haga clic en el botón **Guardar**.

Administración de informes

Esta sección describe cómo puede configurar los parámetros de Informes y administrar los Informes.

Acerca de los 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 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 del informe se presentan en forma de una tabla que contiene una lista de eventos. Cada línea de la tabla contiene información sobre un evento separado. 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 atributos adicionales, debe presionar el botón ⊞ adyacente al nombre del gráfico. Los eventos registrados durante el funcionamiento de los distintos componentes o la ejecución de diversas tareas 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.
- Informe sobre el funcionamiento de un componente o la ejecución de una tarea de Kaspersky Endpoint Security.
- Informe de **Cifrado**. 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**. Icono . Eventos formales que normalmente no contienen información importante.
- **Advertencias**. Icono . Eventos que requieren atención dado que reflejan situaciones importantes relacionadas con el funcionamiento de Kaspersky Endpoint Security.
- **Eventos críticos**. Icono . 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.
- Mostrar y ocultar eventos agrupados por 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. Kaspersky Endpoint Security elimina todas las entradas de los informes seleccionados desde la entrada más antigua hasta el presente.

Si Kaspersky Endpoint Security se está ejecutando bajo la administración de Kaspersky Security Center, la información sobre eventos se puede transmitir al Servidor de administración de Kaspersky Security Center. Para obtener más información sobre la administración de informes en Kaspersky Security Center, consulte la sección de Ayuda de Kaspersky Security Center.

Configuración de los parámetros de informes

Puede configurar los parámetros de informes de las siguientes maneras:

- Configurar el plazo de almacenamiento máximo de los 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. Puede cancelar la restricción basada en el tiempo o modificar la duración máxima de almacenamiento de informes.

- Configurar el 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. Puede cancelar la restricción del tamaño del archivo del informe o definir un valor diferente.

Configuración de la duración máxima del almacenamiento de informes

Para modificar la duración máxima del almacenamiento de informes:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.
3. En la parte derecha de la ventana, en la sección **Parámetros de informes**, realice una de las siguientes acciones:
   - Para limitar la duración del almacenamiento de informes, active la casilla **Conservar informes como máximo**. En el campo junto a la casilla **Conservar informes como máximo**, especifique la duración máxima

del almacenamiento de informes.

Por defecto, el plazo máximo de almacenamiento de informes es de 30 días.

- Para cancelar el límite de la duración del almacenamiento de informes, desactive el botón **Conservar informes como máximo**.

El límite de la duración del almacenamiento de informes está habilitado por defecto.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del tamaño máximo del archivo del informe

Para configurar el tamaño máximo del archivo del informe:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.
3. En la parte derecha de la ventana, en la sección **Parámetros de informes**, realice una de las siguientes acciones:
   - Para limitar el tamaño del archivo del informe, seleccione la casilla **Tamaño máximo de archivo**. En el campo a la derecha de la casilla **Tamaño máximo de archivo**, especifique el tamaño máximo del archivo del informe.

     El tamaño máximo por defecto del archivo del informe es de 1024 MB.
   - Para eliminar la restricción sobre el tamaño del archivo del informe, desactive la casilla **Tamaño máximo de archivo**.

   El límite de tamaño del archivo de informe está habilitado por defecto.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Visualización de informes

Para visualizar informes:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Informes** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Informes**.
3. Para generar el informe Todos los componentes de protección, a la izquierda de la ventana **Informes**, seleccione el elemento **Todos los componentes de protección** en la lista de componentes y tareas.

   Se muestra el informe Todos los componentes de protección en la parte derecha de la ventana, que contiene una lista de eventos sobre la operación de todos los componentes de Kaspersky Endpoint Security.
4. Para generar un informe sobre el funcionamiento de un componente o de una tarea, a la izquierda de la ventana **Informes**, en la lista de componentes y tareas, seleccione un componente o una 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.

Por defecto, los eventos del informe se disponen en orden ascendente según los valores de la columna **Fecha de evento**.

Visualización de información de eventos en un informe

Puede visualizar un resumen detallado de cada evento en el informe.

Para visualizar un resumen detallado de un evento en el informe:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Informes** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Informes**.
3. En la parte izquierda de la ventana, seleccione el informe relevante sobre el componente o la tarea.

   Los eventos incluidos en el alcance del informe se presentan en la tabla de la parte derecha de la ventana. Para encontrar eventos específicos en el informe, use las funciones de filtro, búsqueda y orden.
4. Seleccione el evento relevante en el informe.

Se presenta una sección con el resumen del evento en la parte inferior de la ventana.

Almacenamiento de informes en archivos

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. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Informes** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Informes**.
3. Realice una de las siguientes acciones:

   - Para generar el informe "Todos los componentes de protección", seleccione el elemento **Todos los componentes de protección** en la lista de componentes y tareas.

     Se muestra el informe "Todos los componentes de protección" en la parte derecha de la ventana, que contiene una lista de eventos sobre la operación de todos los componentes de protección.

   - Para generar un informe sobre la operación de un componente o una tarea en particular, seleccione el componente o la tarea en la lista de componentes y tareas.

     Se muestra un informe en la parte derecha de la ventana, que contiene una lista de eventos sobre la operación del componente o la tarea que se seleccionó.
4. 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

5. Haga clic en el botón **Guardar informe** en la parte derecha de la ventana.

   Se abre un menú contextual.

6. En el menú contextual, seleccione el cifrado para guardar el archivo de informe: **Guardar como ANSI** o **Guardar como Unicode**.

   Se abre la ventana **Guardar como** estándar de Microsoft Office.

7. En la ventana **Guardar como**, especifique la carpeta de destino para el archivo de informe.
8. En el campo **Nombre de archivo**, escriba el nombre del archivo de informe.
9. En el campo **Tipo de archivo**, seleccione el formato de archivo de informe necesario: TXT o CSV.
10. Haga clic en el botón **Guardar**.

Borrado de informes

Para eliminar información de los informes:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.
3. En la parte derecha de la ventana, en la sección **Parámetros de informes** , haga clic en el botón **Eliminar informes**.

   Se abre la ventana **Borrado de informes**.

4. Seleccione las casillas junto a los informes de los cuales desea eliminar información.

   - **Todos los informes**.
   - **Informe general de protección**. Contiene información sobre la operación de los siguientes componentes de Kaspersky Endpoint Security:
     - Antivirus de archivos
     - Antivirus de correo electrónico.
     - Antivirus de Internet.
     - Antivirus MI.
     - System Watcher.
     - Firewall.

- Bloqueador de ataques de red.
- Prevención de ataques BadUSB

- **Informe de tareas de análisis**. Contiene información sobre las tareas de análisis completadas:
  - Análisis completo
  - Análisis de áreas críticas
  - Análisis personalizado
  - Comprobación de integridad.
- **Informe de tareas de actualización**. Contiene información sobre las tareas de actualización completadas:
- **Informe de Firewall**. Contiene información sobre la operación de Firewall.
- **Informe de componentes de control**. Contiene información sobre la operación de los siguientes componentes de Kaspersky Endpoint Security:
  - Control de Inicio de las Aplicaciones.
  - Control de Privilegios de Aplicaciones.
  - Monitor de vulnerabilidades.
  - Control de dispositivos.
  - Control web.
- **Informe de cifrado de datos**.

5. Haga clic en **Aceptar**.

Servicio de notificación

Esta sección contiene información sobre el servicio de notificación que alerta al usuario sobre eventos en el funcionamiento de Kaspersky Endpoint Security; además, contiene instrucciones sobre cómo configurar los parámetros de notificación.

Acerca de las notificaciones de Kaspersky Endpoint Security

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, las notificaciones pueden informar sobre una actualización correcta de la base de datos y de módulos de la aplicación, o registrar errores de componentes que es necesario remediar.

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.

Configuración del servicio de notificación

Puede realizar las siguientes acciones para configurar el servicio de notificación:

- Configurar los parámetros de los registros de eventos donde Kaspersky Endpoint Security registra los eventos.
- Configure cómo se muestran las notificaciones en pantalla.
- Configurar la entrega de notificaciones por correo.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.

   En la parte derecha de la ventana se muestran los parámetros de los informes y el almacenamiento.
3. En la sección **Notificaciones**, haga clic en el botón **Configuración**.

   Se abre la ventana **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.
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. Seleccione las casillas opuestas a los eventos relevantes en las columnas **Guardar en registro local** y **Guardar en registro de eventos de Windows**.

   Los eventos cuyas casillas estén seleccionadas en la columna **Guardar en registro local** se muestran en el área de **Registros de aplicaciones y servicios** de la 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, haga clic en **Inicio** → **Panel de control** → **Administración** → **Visor de eventos**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de la visualización y el envío de notificaciones

Para configurar la visualización y el envío de notificaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.

   En la parte derecha de la ventana se muestran los parámetros de los informes y el almacenamiento.
3. En la sección **Notificaciones**, haga clic en el botón **Configuración**.

   Se abre la ventana **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.
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 el botón **Parámetros de notificaciones por correo electrónico**.

   Se abrirá la ventana **Parámetros de notificaciones por correo electrónico**.

8. Seleccione la casilla **Enviar notificaciones de eventos** para activar el envío de notificaciones sobre los eventos de Kaspersky Endpoint Security seleccionados en la columna **Notificar por correo electrónico**.

9. Especifique los parámetros de envío de notificaciones por correo electrónico.

10. Haga clic en **Aceptar**.

11. En la ventana **Parámetros de notificaciones por correo electrónico**, haga clic en **Aceptar**.

12. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración de la visualización de advertencias acerca del estado de la aplicación en el área de notificación

Para configurar la visualización de advertencias acerca del estado de la aplicación en el área de notificación:

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

2. En la parte izquierda de la ventana, en la sección **Configuración general**, seleccione **Interfaz**.

   Los parámetros de la interfaz de Kaspersky Endpoint Security se indican en la parte derecha de la ventana

3. En la sección **Advertencias**, 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. Para guardar los cambios, haga clic en el botón **Guardar**.

Cuando se registren eventos asociados con las categorías seleccionadas, el icono de la aplicación en el área de notificación pasará a error occurred o a reinicio necesario, en función de la gravedad de la advertencia.

Administración de la Cuarentena y Copia de seguridad

Esta sección describe cómo puede configurar y administrar la Cuarentena y Copia de seguridad.

Acerca de la Cuarentena y Copia de seguridad

La *Cuarentena* es una lista de archivos probablemente infectados. Los *Archivos probablemente infectados* son archivos que pueden contener virus y otras amenazas o sus variedades.

Cuando Kaspersky Endpoint Security pone en cuarentena un archivo probablemente infectado, no copia el archivo sino que lo mueve: la aplicación elimina el archivo del disco duro o del mensaje de correo electrónico y lo guarda en un almacenamiento especial de datos. Los archivos puestos en Cuarentena se guardan con un formato especial que no representa una amenaza.

Kaspersky Endpoint Security puede detectar y poner en cuarentena un archivo probablemente infectado al ejecutar un análisis antivirus y también durante el funcionamiento de los componentes Antivirus de archivos, Antivirus de correo electrónico y System Watcher.

Kaspersky Endpoint Security coloca los archivos en Cuarentena en los siguientes casos:

- El código del archivo se parece a un malware conocido, pero parcialmente modificado, o tiene una estructura similar a la del malware, pero no está registrado en la base de datos de Kaspersky Endpoint Security. En este caso, el archivo se pone en Cuarentena después de que el Antivirus de archivos y el Antivirus de correo electrónico hayan realizado un análisis heurístico o durante un análisis antivirus. En raras ocasiones, el análisis heurístico genera falsos positivos.

- La secuencia de las operaciones que realiza un archivo es peligrosa. En este caso, el archivo se coloca en cuarentena después de que el componente System Watcher analizó su comportamiento.

El *Depósito de Copia de seguridad* es una lista de copias de seguridad de los archivos que se eliminaron o modificaron durante el proceso de desinfección. *Copia de seguridad* es una copia de un archivo creada en el primer intento de desinfectar o eliminar este archivo. Las copias de seguridad de archivos se almacenan con un formato especial que no representa una amenaza.

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 la copia desinfectada del archivo a su carpeta original.

Es posible que después de actualizar otra base de datos o módulo de software de la aplicación, Kaspersky Endpoint Security pueda identificar definitivamente las amenazas y neutralizarlas. Por lo tanto, se recomienda analizar los archivos en cuarentena después de cada actualización de bases de datos y de módulos de software de la aplicación.

Configuración de los parámetros de la Cuarentena y Copia de seguridad

El almacenamiento de datos consiste en la Cuarentena y Copia de seguridad. Puede configurar los parámetros de la Cuarentena y Copia de seguridad de la siguiente manera:

- Configure el plazo de almacenamiento máximo para archivos en cuarentena y copias de archivos en copia de seguridad.

El plazo de almacenamiento máximo predeterminado para archivos en cuarentena y copias de archivos en copia de seguridad es de 30 días. Cuando caduque el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos del almacenamiento de datos. Puede cancelar la restricción basada en el tiempo o modificar el plazo de almacenamiento de archivos máximo.

- Puede configurar el tamaño máximo de la Cuarentena y Copia de Seguridad.

  Por defecto, el tamaño máximo de la copia de seguridad y los elementos en cuarentena es de 100 MB. Cuando el almacenamiento de datos alcanza su límite, Kaspersky Endpoint Security elimina automáticamente los archivos más antiguos de la Cuarentena y de la Copia de seguridad para que no se supere el tamaño máximo de datos. Puede cancelar el límite de tamaño de la copia de seguridad o los elementos en cuarentena o cambiar el tamaño máximo.

Configuración del plazo de almacenamiento máximo para archivos en Cuarentena y copias de archivos en Copia de seguridad

Para configurar el plazo de almacenamiento máximo para archivos en Cuarentena y para copias de archivos en Copia de seguridad:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.
3. Realice una de las siguientes acciones:
   - Para limitar el plazo de almacenamiento en la Cuarentena y Copia de Seguridad, en la parte derecha de la ventana, en la sección **Configuración de Cuarentena y Copias de seguridad**, seleccione la casilla **Guardar objetos no más de**. En el campo a la derecha de la casilla **Guardar objetos no más de**, especifique el plazo máximo de almacenamiento para archivos en Cuarentena y para copias de archivos en Copia de seguridad. Por defecto, el plazo de almacenamiento para archivos en Cuarentena y para copias de archivos en Copia de seguridad se limita a 30 días.
   - Para cancelar el límite del plazo de almacenamiento en la Cuarentena y Copia de Seguridad, en la parte derecha de la ventana, en la sección **Configuración de Cuarentena y Copias de seguridad**, seleccione la casilla **Guardar objetos no más de**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Configuración del tamaño máximo de la Cuarentena y Copia de seguridad

Para configurar el tamaño máximo de las copias de seguridad y de los elementos en cuarentena:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.
3. Realice una de las siguientes acciones:
   - Si desea limitar el tamaño total de Cuarentena y Copia de seguridad, seleccione la casilla **Tamaño máximo de almacenamiento** en la parte derecha de la ventana en la sección **Configuración de Cuarentena y**

Copias de seguridad y especifique el tamaño máximo de Cuarentena y Copia de seguridad en el campo que se encuentra a la derecha de la casilla **Tamaño máximo del almacenamiento**.

De forma predeterminada, el tamaño máximo del almacenamiento para los datos que comprenden el directorio de la Cuarentena y las copias de seguridad de los archivos es de 100 MB.

- Si desea eliminar el límite del tamaño de Cuarentena y Copia de seguridad, desmarque la casilla **Tamaño máximo de almacenamiento** en la parte derecha de la ventana en la sección **Configuración de Cuarentena y Copias de seguridad**.

El tamaño de Cuarentena y Copia de seguridad es ilimitado de forma predeterminada.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Administración de la Cuarentena

Una vez transcurrido el plazo de almacenamiento establecido en la configuración de la aplicación, Kaspersky Endpoint Security elimina automáticamente los archivos de la Cuarentena con cualquier estado.

Las siguientes operaciones de archivo están disponibles cuando se administra la Cuarentena:

- Ver los archivos puestos en cuarentena por Kaspersky Endpoint Security.
- Analizar los archivos probablemente infectados utilizando la versión actual de las bases de datos y los módulos de Kaspersky Endpoint Security.
- Restaurar todos los archivos en cuarentena a sus carpetas originales.
- Eliminar archivos de la cuarentena.
- Abrir las carpetas donde se encontraban los archivos originalmente.

El conjunto de archivos en cuarentena se presenta en forma de tabla.

También puede realizar las siguientes acciones mientras administra los datos de la tabla:

- Filtrar archivos puestos en cuarentena según columnas y condiciones con filtros personalizados.
- Usar la función de búsqueda de archivo en cuarentena.
- Ordenar archivos en cuarentena.
- Cambiar el orden y el conjunto de columnas que se muestran en la tabla de archivos en cuarentena.

Puede copiar eventos de cuarentena seleccionados al portapapeles. Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.

Habilitación y deshabilitación del análisis de archivos en cuarentena después de una actualización

Si Kaspersky Endpoint Security detecta signos de infección al analizar un archivo pero no puede determinar qué programas maliciosos específicos lo han infectado, Kaspersky Endpoint Security pone este archivo en Cuarentena. Es posible que Kaspersky Endpoint Security identifique definitivamente las amenazas y las neutralice después de la actualización de las bases de datos y los módulos de la aplicación. Puede habilitar el análisis automático de archivos en cuarentena después de cada actualización de las bases de datos y los módulos de la aplicación.

Se recomienda analizar con regularidad los archivos en cuarentena. El análisis puede cambiar los estados de archivos. Algunos archivos pueden desinfectarse y restaurarse a su ubicación original para que pueda seguir usándolos.

Para habilitar el análisis de archivos en cuarentena después de las actualizaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y depósitos**.

   En la parte derecha de la ventana, se muestra la configuración de la administración de Informes y depósitos.
3. En la sección **Configuración de Cuarentena y Copias de seguridad**, realice una de las siguientes acciones:
   - Para habilitar el análisis de archivos en cuarentena después de cada actualización de Kaspersky Endpoint Security, active la casilla **Volver a analizar la Cuarentena después de actualizar**.
   - Para deshabilitar el análisis de archivos en cuarentena después de cada actualización de Kaspersky Endpoint Security, desactive la casilla **Volver a analizar la Cuarentena después de actualizar**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Inicio de una tarea de análisis personalizado de los archivos en cuarentena

Después de la actualización de las bases de datos y de los módulos de software de la aplicación, Kaspersky Endpoint Security puede identificar definitivamente las amenazas de los archivos en cuarentena y neutralizarlas. Si la aplicación no está configurada para analizar automáticamente archivos en cuarentena luego de cada actualización de bases de datos y módulos de la aplicación, puede iniciar manualmente una tarea de análisis personalizado de archivos en cuarentena.

Para iniciar una tarea de análisis personalizado de archivos en cuarentena:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.

   Se abre la ficha **Cuarentena** de la ventana **Depósitos**.
3. En la ficha **Cuarentena**, seleccione uno o más archivos probablemente infectados que quiera analizar.

   Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.
4. Inicie la tarea de análisis personalizado de una de las siguientes formas:
   - Haga clic en el botón **Volver a analizar**.
   - Haga clic con el botón derecho del mouse para mostrar el menú contextual y seleccione **Volver a analizar**.

Cuando finalice el análisis, aparecerá una notificación con la cantidad de archivos analizados y la cantidad de amenazas detectadas.

Restauración de archivos en cuarentena

Para restaurar los archivos desde la Cuarentena:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.

   Se abre la ficha **Cuarentena** de la ventana **Depósitos**.
3. Si desea restaurar todos los archivos en cuarentena, seleccione **Restaurar todo** en el menú contextual de cualquier archivo.

   Kaspersky Endpoint Security restaura todos los archivos de Cuarentena a sus carpetas originales.
4. Para restaurar uno o más archivos en cuarentena:

   a. En la ficha **Cuarentena**, seleccione uno o más archivos que quiera restaurar desde la Cuarentena.

   Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.

   b. Restaure archivos de una de las siguientes maneras:

   - Haga clic en el botón **Restaurar**.
   - Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Restaurar**.

Kaspersky Endpoint Security restaura los archivos seleccionados a sus carpetas originales.

Eliminación de archivos de la cuarentena

Para eliminar archivos desde la Cuarentena:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.

   Se abre la ficha **Cuarentena** de la ventana **Depósitos**.
3. Si desea eliminar todos los archivos en cuarentena, seleccione **Eliminar todo** en el menú contextual de cualquier archivo.

   Kaspersky Endpoint Security elimina todos los archivos de la Cuarentena.
4. Para eliminar uno o más archivos en cuarentena:

   a. En la tabla de la ficha **Cuarentena**, seleccione uno o más archivos probablemente infectados que quiera eliminar de la Cuarentena.

Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.

b. Elimine archivos de una de las siguientes maneras:

- Haga clic en el botón **Eliminar**.
- Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Eliminar**.

Kaspersky Endpoint Security elimina los archivos seleccionados de la Cuarentena.

Administración del Depósito de copias de seguridad

Si se detecta código malicioso en el archivo, Kaspersky Endpoint Security bloquea el archivo, coloca una copia en la copia de seguridad e intenta desinfectarlo. Si se lleva a cabo una desinfección de un archivo, el estado de la copia de seguridad del archivo cambia a *Desinfectado*. El archivo queda disponible en su carpeta original. Si no se puede desinfectar un archivo, Kaspersky Endpoint Security lo elimina de su carpeta original. Puede restaurar el archivo de su copia de seguridad a su carpeta original.

Después de detectar código malicioso en un archivo que es parte de la aplicación Tienda Windows, Kaspersky Endpoint Security inmediatamente elimina el archivo sin pasar una copia a la 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*).

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 la copia de seguridad cualquier copia de un archivo.

El conjunto de copias de seguridad de los archivos se presenta en forma de tabla.

Mientras administra el Depósito de copias de seguridad, puede realizar las siguientes acciones con las copias de seguridad de archivos:

- Ver el conjunto de copias de seguridad de archivos.
- Restaurar los archivos de copias de seguridad a sus carpetas originales.
- Eliminar copias de seguridad de archivos desde el Depósito de copias de seguridad.

También puede realizar las siguientes acciones mientras administra los datos de la tabla:

- Filtrar las copias de seguridad por columna, incluso por condiciones de filtros personalizadas.
- Usar la función de búsqueda de copia de seguridad.
- Ordenar copias de seguridad.
- Cambiar el orden y el conjunto de columnas que se muestran en la tabla de copias de seguridad.

Puede copiar los eventos de copia de seguridad seleccionados al portapapeles. Para seleccionar varios archivos del Depósito de copias de seguridad, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.

Restauración de archivos desde el Depósito de copias de seguridad

Para restaurar los archivos desde el Depósito de copias de seguridad:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Copia de Seguridad**.
4. Si desea restaurar todos los archivos desde el Depósito de copias de seguridad, seleccione **Restaurar todo** en el menú contextual de cualquier archivo.

   Kaspersky Endpoint Security restaura todos los archivos desde sus copias de seguridad hasta sus carpetas originales.
5. Para restaurar uno o más archivos desde el Depósito de copias de seguridad:

   a. En la tabla de la ficha **Depósito de copias de seguridad**, seleccione uno o más archivos del Depósito de copias de seguridad.

   Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.

   b. Restaure archivos de una de las siguientes maneras:

   - Haga clic en el botón **Restaurar**.
   - Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Restaurar**.

Kaspersky Endpoint Security restaura archivos desde las copias de seguridad seleccionadas a sus carpetas originales.

Eliminar copias de seguridad de archivos desde el Depósito de copias de seguridad

Para eliminar copias de seguridad de archivos desde el Depósito de copias de seguridad:

1. Abra la ventana principal de la aplicación.
2. Haga clic en el vínculo **Cuarentena** en la parte superior de la ventana principal de la aplicación para abrir la ventana **Depósitos**.
3. En la ventana **Depósitos**, seleccione la ficha **Copia de Seguridad**.

4. Si desea eliminar todos los archivos desde Copia de seguridad, realice una de las siguientes acciones:

   - En el menú contextual de cualquier archivo, seleccione **Eliminar todo**.
   - Haga clic en el botón **Vaciar depósito**.

   Kaspersky Endpoint Security elimina todas las copias de seguridad de archivos del Depósito de copias de seguridad.

5. Si quiere eliminar uno o más archivos del Depósito de copias de seguridad:

   a. En la tabla de la ficha **Depósito de copias de seguridad**, seleccione uno o más archivos del Depósito de copias de seguridad.

      Para seleccionar varios archivos del Depósito de copias de seguridad, haga clic con el botón derecho del mouse para abrir el menú contextual de cualquier archivo y elija **Seleccionar todo**. Para desmarcar los archivos que no quiera analizar, hágales clic mientras mantiene presionada la tecla **CTRL**.

   b. Elimine archivos de una de las siguientes maneras:

      - Haga clic en el botón **Eliminar**.
      - Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Eliminar**.

   Kaspersky Endpoint Security elimina todas las copias de seguridad de archivos seleccionadas del Depósito de copias de seguridad.

Configuraciones avanzadas de la aplicación

Esta sección describe los parámetros de las Configuraciones avanzadas de Kaspersky Endpoint Security y cómo se las puede configurar.

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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.

   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Administrar configuración**, haga clic en el botón **Guardar**.

   Se abre la ventana **Seleccione un archivo de configuración** estándar de Microsoft Windows.
4. Especifique la ruta en la cual quiera 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. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.

   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Administrar configuración**, haga clic en el botón **Cargar**.

   Se abre la ventana **Seleccione un archivo de configuración** estándar de Microsoft Windows.
4. Especifique la ruta 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.

Zona de confianza

Esta sección contiene información sobre la zona de confianza e instrucciones para configurar las exclusiones de escaneo y para crear una lista de aplicaciones de confianza.

Acerca de la zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo. En otras palabras, es un conjunto de exclusiones de escaneo.

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.

Puede excluir del análisis los siguientes objetos:

- Archivos con ciertos formatos
- Archivos seleccionados por una máscara
- Archivos seleccionados
- Carpetas
- Procesos de aplicaciones

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. Si bien no tienen ninguna función maliciosa, tales aplicaciones se pueden utilizar como un componente auxiliar del malware. Ejemplos de tales aplicaciones incluyen herramientas administrativas remotas, clientes IRC, servidores FTP, diversas utilidades para la suspensión u ocultamiento de procesos, registradores de pulsaciones, decodificadores de contraseñas y marcadores automáticos. Dichas aplicaciones no se categorizan como virus. 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 virus de Kaspersky en www.securelist.com/threats/riskware.

Kaspersky Endpoint Security puede bloquear estas aplicaciones. Para prevenir que se bloqueen, puede configurar la exclusión del análisis para las aplicaciones en uso. Para esto, agregue el nombre o la máscara de nombre de la amenaza enumerada en la Enciclopedia del virus de Kaspersky 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 enumera en la Enciclopedia del virus 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. Por defecto, Kaspersky Endpoint Security analiza objetos abiertos, ejecutados o guardados por cualquier proceso de programa y controla la actividad de todas las aplicaciones y el tráfico de red que estos generan. Kaspersky Endpoint Security excluye del análisis a las aplicaciones incluidas en 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 crear una exclusión 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.

Para crear una exclusión de análisis:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración general**, seleccione **Exclusiones**.

   La configuración de las exclusiones se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

   Se abre la ventana **Zona de confianza** en la ficha **Exclusiones de análisis**.
4. Haga clic en el botón **Agregar**.

   Se abre la ventana **Exclusión de análisis**. En esta ventana, puede crear una exclusión de análisis con el o los criterios de la sección **Propiedades**.
5. 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.

   La máscara del nombre de archivo o carpeta puede contener el asterisco (*) en reemplazo de cualquier número de caracteres del nombre de archivo.

   A modo de ejemplo, puede usar máscaras para agregar las siguientes rutas:

   - Rutas a los archivos de cualquier carpeta:
     - La máscara `*.exe` comprende 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 todas las rutas a archivos almacenados en la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
     - La máscara "C:\dir*" comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
     - La máscara "C:\dir\" comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
     - La máscara "C:\dir*.exe" comprende las rutas a todos los archivos de extensión EXE almacenados en C:\dir\, pero no a los de las subcarpetas de C:\dir\.

- La máscara "C:\dir\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 todas las rutas a archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
  - La máscara "dir*" comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
  - La máscara "dir\" comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
  - La máscara "dir*.exe" comprende las rutas a todos los archivos de extensión EXE almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
  - La máscara "dir\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.

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**.

6. 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. Ingrese el nombre del objeto o la máscara del nombre según la clasificación de la Enciclopedia de virus de Kaspersky.

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**.

7. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

8. 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.

9. En la ventana **Exclusión de análisis**, haga clic en **Aceptar**.

   La exclusión de análisis que agregó aparece en la tabla de la ficha **Exclusiones de análisis** de la ventana **Zona de confianza**. Los parámetros configurados de esta exclusión de análisis aparecen en la sección **Descripción de la exclusión de escaneo**.

10. En la ventana **Zona de confianza**, haga clic en **Aceptar**.

11. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificar una exclusión de escaneo

Para modificar una exclusión de escaneo:

1. Abra la ventana de configuración de la aplicación.

2. Seleccione la sección **Protección antivirus** de la izquierda.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.

3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

   Se abre la ventana **Zona de confianza** en la ficha **Exclusiones de análisis**.

4. Seleccione la exclusión de escaneo que desea modificar en la lista.

5. Cambie la configuración de la exclusión de escaneo con uno de los métodos siguientes:

   - Haga clic en el botón **Modificar**.

     Se abre la ventana **Exclusiones de análisis**.

   - Abra la ventana para modificar el parámetro necesario haciendo clic en el vínculo del campo **Descripción de la exclusión de escaneo**.

6. Si hizo clic en el botón **Modificar** en el paso anterior, haga clic en **Aceptar** en la ventana **Exclusión de análisis**.

   Los parámetros modificados de esta exclusión de escaneo aparecen en la sección **Descripción de la exclusión de escaneo**.

7. En la ventana **Zona de confianza**, haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

Eliminar una exclusión de escaneo

Para eliminar una exclusión de escaneo:

1. Abra la ventana de configuración de la aplicación.

2. Seleccione la sección **Protección antivirus** de la izquierda.
   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
   Se abre la ventana **Zona de confianza** en la ficha **Exclusiones de análisis**.
4. Seleccione la exclusión de escaneo que necesite en la lista de exclusiones de escaneo.
5. Haga clic en el botón **Eliminar**.
   La exclusión de escaneo eliminada desaparece de la lista.
6. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Activar y desactivar una exclusión de escaneo

Para activar y desactivar una exclusión de escaneo:

1. Abra la ventana de configuración de la aplicación.
2. Seleccione la sección **Protección antivirus** de la izquierda.
   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
   Se abre la ventana **Zona de confianza** en la ficha **Exclusiones de análisis**.
4. Seleccione la exclusión que necesite en la lista de exclusiones de escaneo.
5. Realice una de las siguientes acciones:
   - Para habilitar una exclusión de escaneo, seleccione la casilla adyacente al nombre de la exclusión de escaneo.
   - Para deshabilitar una exclusión de escaneo, desmarque la casilla adyacente al nombre de la exclusión de escaneo.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios, haga clic en el botón **Guardar**.

Modificación de la lista de aplicaciones de confianza

Para modificar la lista de aplicaciones de confianza:

1. Abra la ventana de configuración de la aplicación.
2. Seleccione la sección **Protección antivirus** de la izquierda.
   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.

3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

   Se abre la ventana **Zona de confianza**.

4. En la ventana **Zona de confianza**, seleccione la ficha **Aplicaciones de confianza**.

5. Para agregar una aplicación a la lista de aplicaciones de confianza:

   a. Haga clic en el botón **Agregar**.

   b. En el menú contextual que se abre, realice una de las siguientes acciones:

   - Si quiere encontrar la aplicación en la lista de aplicaciones instaladas en el equipo, seleccione el elemento **Aplicaciones** en el menú.

     Se abre la ventana **Seleccionar aplicación**.

   - Si quiere especificar la ruta del archivo ejecutable de la aplicación relevante, seleccione **Examinar**.

     Se abre la ventana estándar **Abrir archivo** en Microsoft Windows.

   c. Puede seleccionar la aplicación de las siguientes maneras:

   - Si seleccionó **Aplicaciones** en el paso anterior, seleccione la aplicación en la lista de aplicaciones instaladas en el equipo y haga clic en **Aceptar** en la ventana **Seleccionar aplicación**.

   - Si seleccionó **Examinar** en el paso anterior, especifique la ruta del archivo ejecutable de la aplicación relevante y haga clic en el botón **Abrir** en la ventana **Abrir** estándar de Microsoft Windows.

   Con estas acciones, se abre la ventana **Exclusiones de análisis para la aplicación**.

   a. Seleccione las casillas que se encuentran frente a las reglas de la zona de confianza relevantes para la aplicación seleccionada:

   - **No analizar archivos abiertos**.
   - **No supervisar la actividad de la aplicación**.
   - **No heredar restricciones del proceso principal (aplicación)**.
   - **No supervisar la actividad de las aplicaciones secundarias**.
   - **No bloquear la interacción con la interfaz de la aplicación**.
   - **No analizar el tráfico de red**.

   b. En la ventana **Exclusiones de análisis para la aplicación**, haga clic en **Aceptar**.

   La aplicación de confianza que agregó aparece en la lista de aplicaciones de confianza.

6. Para modificar la configuración de una aplicación de confianza:

   a. Seleccione una aplicación de confianza de la lista.

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

   c. Se abre la ventana **Exclusiones de análisis para la aplicación**.

d. Seleccione o desmarque las casillas que se encuentran frente a las reglas de la zona de confianza relevantes para la aplicación seleccionada:

> Si no se selecciona ninguna regla de zona de confianza en la ventana **Exclusiones de análisis para la aplicación**, la aplicación de confianza se incluye en el análisis. En este caso, no se quita la aplicación de confianza de la lista de aplicaciones de confianza, pero sí se desmarca su casilla.

e. En la ventana **Exclusiones de análisis para la aplicación**, haga clic en **Aceptar**.

7. Para quitar una aplicación de confianza de la lista:

a. Seleccione una aplicación de confianza de la lista.

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

8. En la ventana **Zona de confianza**, haga clic en **Aceptar**.

9. Para guardar los cambios, haga clic en el botón **Guardar**.

Activación y desactivación de reglas de la zona de confianza para una aplicación en la lista de aplicaciones de confianza

Para activar o desactivar la acción de las reglas de la zona de confianza aplicadas a una aplicación de la lista de aplicaciones de confianza:

1. Abra la ventana de configuración de la aplicación.

2. Seleccione la sección **Protección antivirus** de la izquierda.
   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.

3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
   Se abre la ventana **Zona de confianza**.

4. En la ventana **Zona de confianza**, seleccione la ficha **Aplicaciones de confianza**.

5. En la lista de aplicaciones de confianza, seleccione la aplicación de confianza necesaria.

6. Realice una de las siguientes acciones:

   - Para excluir una aplicación de confianza del análisis de Kaspersky Endpoint Security, seleccione la casilla junto al nombre de la aplicación.

   - Para incluir una aplicación de confianza en el análisis de Kaspersky Endpoint Security, desactive la casilla junto al nombre de la aplicación.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios, haga clic en el botón **Guardar**.

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. Abra la ventana de configuración de la aplicación.
2. Seleccione la sección **Protección antivirus** de la izquierda.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

   Se abre la ventana **Zona de confianza**.
4. En la ventana **Zona de confianza**, seleccione la ficha **Almacén de confianza de certificados del sistema**.
5. Seleccione la casilla **Usar el almacén de confianza de certificados del sistema**.
6. En la lista desplegable **Almacén de confianza de certificados del sistema**, seleccione el almacén del sistema de Kaspersky Endpoint Security que debe considerarse de confianza.
7. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
8. Para guardar los cambios, haga clic en el botón **Guardar**.

Autoprotección de Kaspersky Endpoint Security

Esta sección describe los mecanismos de autoprotección y protección de control remoto de Kaspersky Endpoint Security y brinda instrucciones para configurar los parámetros de estos mecanismos.

Acerca de la Autoprotección de Kaspersky Endpoint Security

Kaspersky Internet Security protege el equipo contra programas maliciosos, incluido el malware que intente bloquear el funcionamiento de Kaspersky Endpoint Security o, incluso, eliminarlo del equipo.

La estabilidad del sistema de seguridad del equipo se garantiza mediante mecanismos de autoprotección y de protección de control remoto de Kaspersky Endpoint Security.

El mecanismo *Autoprotección* impide la modificación o eliminación de los archivos de aplicaciones que se encuentran en el disco duro, de los procesos de la memoria y de las entradas en el registro del sistema.

El mecanismo *Protección de control remoto* bloquea todos los intentos de controlar los servicios de las aplicaciones desde un equipo remoto.

En equipos que se ejecutan en sistemas operativos de 64 bits, solo la Autoprotección de Kaspersky Endpoint Security está disponible para impedir que se modifiquen y se eliminen los archivos de aplicación que se encuentran en el disco duro y las entradas en el registro del sistema.

Habilitación y deshabilitación de la Autoprotección

El mecanismo de Autoprotección de Kaspersky Endpoint Security está habilitado por defecto. Si es necesario, puede deshabilitar la Autoprotección.

Para habilitar o deshabilitar la Autoprotección:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:
   - Para habilitar el mecanismo de Autoprotección, seleccione la casilla **Habilitar Autoprotección**.
   - Para deshabilitar el mecanismo de Autoprotección, desmarque la casilla **Habilitar Autoprotección**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Habilitación o deshabilitación de la Protección de control remoto

El mecanismo Protección de control remoto está habilitado por defecto. Si es necesario, puede deshabilitar el mecanismo Protección de control remoto.

Para habilitar o deshabilitar el mecanismo Protección de control remoto:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:
   - Para habilitar el mecanismo Protección de control remoto, active la opción **Deshabilitar administración externa del servicio del sistema**.
   - Para deshabilitar el mecanismo Protección de control remoto, desactive la opción **Deshabilitar administración externa del servicio del sistema**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Compatibilidad con aplicaciones de administración remota

Ocasionalmente, puede necesitar usar una aplicación de administración remota mientras está habilitada la protección de control externo.

Para habilitar el funcionamiento de aplicaciones de administración remota:

1. Abra la ventana de configuración de la aplicación.
2. Seleccione la sección **Protección antivirus** de la izquierda.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

   Se abre la ventana **Zona de confianza**.
4. En la ventana **Zona de confianza**, seleccione la ficha **Aplicaciones de confianza**.
5. Haga clic en el botón **Agregar**.
6. En el menú contextual que se abre, realice una de las siguientes acciones:

   - Para encontrar la aplicación de administración remota en la lista de aplicaciones instaladas en el equipo, seleccione el elemento **Aplicaciones**.

     Se abre la ventana **Seleccionar aplicación**.
   - Para especificar la ruta de acceso al archivo ejecutable de la aplicación de administración remota, seleccione **Examinar**.

     Se abre la ventana estándar **Abrir archivo** en Microsoft Windows.
7. Puede seleccionar la aplicación de las siguientes maneras:

   - Si seleccionó **Aplicaciones** en el paso anterior, seleccione la aplicación en la lista de aplicaciones instaladas en el equipo y haga clic en **Aceptar** en la ventana **Seleccionar aplicación**.
   - Si seleccionó **Examinar** en el paso anterior, especifique la ruta del archivo ejecutable de la aplicación relevante y haga clic en el botón **Abrir** en la ventana **Abrir** estándar de Microsoft Windows.

   Con estas acciones, se abre la ventana **Exclusiones de análisis para la aplicación**.
8. Seleccione la casilla **No supervisar la actividad de la aplicación**.
9. En la ventana **Exclusiones de análisis para la aplicación**, haga clic en **Aceptar**.

   La aplicación de confianza que agregó aparece en la lista de aplicaciones de confianza.
10. Para guardar los cambios, haga clic en el botón **Guardar**.

Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones

Esta sección contiene información acerca del rendimiento de Kaspersky Endpoint Security y la compatibilidad con otras aplicaciones, así como pautas para la selección de los tipos de objetos detectables y el modo de funcionamiento de Kaspersky Endpoint Security.

Acerca del rendimiento de Kaspersky Endpoint Security y la 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 Análisis de vulnerabilidades
- 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

Los programas maliciosos actuales son capaces de penetrar los niveles más bajos del sistema operativo, lo que hace prácticamente imposible que se puedan eliminar. Después de detectar actividad maliciosa en el sistema operativo, Kaspersky Endpoint Security realiza un procedimiento de desinfección amplio en el que se utiliza una tecnología de desinfección avanzada especial. La *tecnología de desinfección avanzada* se orienta a purgar el sistema operativo de los programas maliciosos que ya hayan comenzado sus procesos en la memoria RAM y evita que Kaspersky Endpoint Security los elimine utilizando otros métodos. 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.

No se puede contar con una solicitud de reinicio en un equipo con Microsoft Windows para servidores de archivos debido a las características específicas de Kaspersky Endpoint Security para servidores de archivos. 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 desinfectar una infección activa en un servidor de archivos, habilite la tecnología de desinfección avanzada para servidores de archivos e inicie una tarea de grupo *Análisis antivirus* en una hora conveniente para los usuarios de los servidores de archivos.

Selección de tipos de objetos detectables

Para seleccionar los tipos de objetos detectables:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Objetos**, haga clic en el botón **Configuración**.

   Se abre la ventana **Objetos para detectar**.
4. Seleccione las casillas junto a los tipos de objetos que desea que Kaspersky Endpoint Security detecte:

- **Herramientas maliciosas**
- **Adware**
- **Marcadores automáticos**
- **Otro**
- **Archivos empaquetados potencialmente peligrosos**
- **Archivos de empaquetado múltiple**

5. Haga clic en **Aceptar**.

   Se cierra la ventana **Objetos para detectar**. En la sección **Objetos**, los tipos de objetos seleccionados se enumeran en **Está activada la detección de los siguientes tipos de objeto**.

6. Para guardar los cambios, haga clic en el botón **Guardar**.

Activación o desactivación de la tecnología de desinfección avanzada para estaciones de trabajo

Para activar o desactivar la tecnología de desinfección avanzada para estaciones de trabajo:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.

   La configuración de la Protección antivirus se muestra en la parte derecha de la ventana.

3. En la parte derecha de la ventana, realice una de las siguientes acciones:

   - Seleccione la casilla **Habilitar la tecnología de desinfección avanzada** para habilitar la tecnología de desinfección avanzada.
   - Anule la selección de la casilla **Habilitar la tecnología de desinfección avanzada** para deshabilitar la tecnología de desinfección avanzada.

4. Para guardar los cambios, haga clic en el botón **Guardar**.

Cuando se inicia la tarea de desinfección avanzada a través de Kaspersky Security Center, la mayoría de las funciones del sistema operativo no están disponibles para el usuario. La estación de trabajo se reinicia una vez completada la tarea.

Activación o desactivación de la tecnología de desinfección avanzada para servidores de archivos

Para habilitar la tecnología de desinfección avanzada para servidores de archivos, realice una de las siguientes acciones:

- Active la tecnología de desinfección avanzada en las propiedades de la directiva activa de Kaspersky Security Center. Para hacerlo:

  a. Abra la sección **Configuración de protección general** en la ventana de propiedades de la directiva.

  b. Seleccione la casilla **Habilitar la tecnología de desinfección avanzada**.

  c. Para guardar los cambios, haga clic en **Aceptar** en la ventana de propiedades de la directiva.

- En las propiedades de la tarea de grupo Análisis antivirus de Kaspersky Security Center, seleccione la casilla **Ejecutar desinfección avanzada inmediatamente**.

Para desactivar la tecnología de desinfección avanzada para servidores de archivos, realice lo siguiente:

- Active la tecnología de desinfección avanzada en las propiedades de la directiva de Kaspersky Security Center. Para hacerlo:

  a. Abra la sección **Configuración de protección general** en la ventana de propiedades de la directiva.

  b. Anule la selección de la casilla **Habilitar la tecnología de desinfección avanzada**.

  c. Para guardar los cambios, haga clic en **Aceptar** en la ventana de propiedades de la directiva.

- En las propiedades de la tarea de grupo Análisis antivirus de Kaspersky Security Center, anule la selección de la casilla **Ejecutar desinfección avanzada inmediatamente**.

Activación o desactivación del modo de ahorro de energía

Para activar o desactivar el modo de ahorro de energía:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.
   Se abre la ventana **Modo de funcionamiento**.
4. En la ventana **Modo de funcionamiento**, realice las siguientes acciones:

   - Para activar el modo de ahorro de energía, seleccione la casilla **Posponer las tareas programadas cuando el equipo funciona con carga de batería**.
     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 Análisis de vulnerabilidades
- Tarea de Comprobación de integridad

- Si quiere desactivar el modo de ahorro de energía, desmarque la casilla **Posponer las tareas programadas cuando el equipo funciona con carga de batería**. En este caso, Kaspersky Endpoint Security realiza las tareas programadas independientemente de cuál sea la fuente de alimentación del equipo.

5. Para guardar los cambios, haga clic en el botón **Guardar**.

Activación o desactivación de la dispensación de recursos para otras aplicaciones

Para activar o desactivar la dispensación de recursos para otras aplicaciones:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.

   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.

   Se abre la ventana **Modo de funcionamiento**.
4. En la ventana **Modo de funcionamiento**, realice las siguientes acciones:

   - Si quiere activar el modo en el que se dispensan recursos para otras aplicaciones, seleccione la casilla **Conceder 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 Análisis de vulnerabilidades
     - Tarea de Comprobación de integridad
   - Si quiere desactivar el modo en el que se dispensan recursos para otras aplicaciones, desmarque la casilla **Conceder recursos a otras aplicaciones**. En este caso, Kaspersky Endpoint Security realiza las tareas programadas independientemente del funcionamiento de otras aplicaciones.

   Por defecto, la aplicación está configurada para dispensar recursos para otras aplicaciones.
5. Para guardar los cambios, haga clic en el botón **Guardar**.

Protección con contraseña

Esta sección contiene información acerca de la restricción del acceso a Kaspersky Endpoint Security mediante una contraseña.

Acerca de la restricción del acceso a Kaspersky Endpoint Security

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.

Puede restringir el acceso a Kaspersky Endpoint Security si configura un nombre de usuario y una contraseña, y especifica las operaciones para las cuales la aplicación solicitará estas credenciales:

Cuando se actualiza una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, se preserva la contraseña (si se la definió). Para editar la configuración de la protección de la contraseña por primera vez, use el nombre de usuario predeterminado KLAdmin.

Activación y desactivación de la protección con contraseña

Recomendamos ser cautelosos al usar una contraseña para restringir el acceso a la aplicación. Si olvida la contraseña, póngase en contacto con el Servicio de soporte técnico de Kaspersky con el fin de recibir instrucciones para desactivar la protección con contraseña.

Para activar la protección con contraseña:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración general**, seleccione **Interfaz**.

   Los parámetros de la interfaz de Kaspersky Endpoint Security se indican en la parte derecha de la ventana
3. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección con contraseña**.
4. Seleccione la casilla **Habilitar la protección con contraseña**.
5. En el campo **Nombre de usuario**, escriba el nombre de usuario que se debe especificar en la ventana **Control de contraseña** cuando se realizan las siguientes operaciones protegidas con contraseña.
6. En el campo **Nueva contraseña**, escriba una contraseña para acceder a la aplicación.
7. Confirme la contraseña en el campo **Confirmar contraseña**.
8. Si quiere restringir el acceso para todas las operaciones con la aplicación, en la sección **Alcance de la contraseña**, haga clic en el botón **Seleccionar todo**.

9. Si quiere restringir selectivamente el acceso del usuario, en la sección **Alcance de la contraseña**, seleccione las casillas que se encuentran al lado de los nombres de las operaciones relevantes:

   - **Configurar los parámetros de la aplicación**.
   - **Salir de la aplicación**.
   - **Desactivar componentes de protección**.
   - **Desactivar componentes de control**.
   - **Eliminar una clave**.
   - **Eliminar, modificar o restaurar la aplicación**.
   - **Restaurar el acceso a los datos de unidades cifradas**.
   - **Ver informes**.

10. Haga clic en el botón **Aceptar**.

    La aplicación verifica las contraseñas ingresadas. Si las contraseñas coinciden, la aplicación aplica la contraseña. Si las contraseñas no coinciden, la aplicación le solicita que confirme la contraseña nuevamente en el campo **Confirmar contraseña**.

11. Para guardar los cambios, haga clic en el botón **Guardar** en la ventana de configuración de la aplicación.

Después de que se habilite la protección con contraseña, la aplicación solicitará una contraseña cada vez que se realice una operación incluida en el alcance de la contraseña. Si no quiere que la aplicación le solicite la contraseña cada vez que intente realizar nuevamente una operación protegida con contraseña durante la sesión actual, puede seleccionar la casilla **Guardar contraseña para esta sesión** en la ventana **Control de contraseña**.

Cuando se desmarque la casilla **Guardar contraseña para esta sesión**, la aplicación le solicitará la contraseña cada vez que intente realizar una operación protegida con contraseña.

Para desactivar la protección con contraseña:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración general**, seleccione **Interfaz**.

   Los parámetros de la interfaz de Kaspersky Endpoint Security se indican en la parte derecha de la ventana
3. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección con contraseña**.
4. Desactive la casilla **Habilitar la protección con contraseña**.

   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.
5. Haga clic en el botón **Aceptar**.
6. Para guardar los cambios, haga clic en el botón **Guardar** en la ventana de configuración de la aplicación.

Se abre la ventana **Control de contraseña**.

7. Ingrese el nombre de usuario en el campo **Nombre de usuario**.
8. Escriba la contraseña de acceso para Kaspersky Endpoint Security en el campo **Contraseña**.
9. Haga clic en **Aceptar**.

Modificación de la contraseña de acceso a Kaspersky Endpoint Security

Para cambiar la contraseña de acceso a Kaspersky Endpoint Security:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
3. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
   Se abre la ventana **Protección con contraseña**.
4. Ingrese el nombre de usuario en el campo **Nombre de usuario**.
5. En el campo **Nueva contraseña**, introduzca una nueva contraseña para acceder a la aplicación.
6. En el campo **Confirmar contraseña**, vuelva a introducir la nueva contraseña.
7. Haga clic en **Aceptar**.
   La aplicación verifica las contraseñas ingresadas. Si las contraseñas coinciden, la aplicación emplea la nueva contraseña y cierra la ventana **Protección con contraseña**. Si las contraseñas no coinciden, la aplicación le solicita que confirme la contraseña nuevamente en el campo **Confirmar contraseña**.
8. Para guardar los cambios, haga clic en el botón **Guardar** en la ventana de configuración de la aplicación.

Acerca del uso de una contraseña temporaria

Cuando trabajen en equipos cliente administrados por una directiva de Kaspersky Security Center, es posible que los usuarios tengan que realizar operaciones con Kaspersky Endpoint Security que están protegidas con contraseña al nivel de la directiva. Si la protección con contraseña está activada, solo el administrador de Kaspersky Security Center puede realizar las operaciones especificadas en el alcance de la contraseña. Sin embargo, si se ha interrumpido la conexión con Kaspersky Security Center (por ejemplo, cuando el usuario está fuera de la red corporativa), las funciones para trabajar con la interfaz local de Kaspersky Security Center están limitadas.

Para proporcionar a un usuario la posibilidad de realizar las operaciones necesarias sin darle la contraseña que se define en la configuración de la directiva, el administrador de Kaspersky Security Center puede crear una contraseña temporaria. Una contraseña temporaria tiene un período de validez limitado y un alcance de acciones limitado. Una vez que el usuario ingresa la contraseña temporaria en la interfaz local de la aplicación, las operaciones permitidas por el administrador de Kaspersky Security Center se vuelven disponibles.

Cuando la contraseña temporaria caduca, Kaspersky Endpoint Security continúa funcionando de acuerdo con la configuración de la directiva de Kaspersky Security Center. El usuario ya no puede acceder a las operaciones protegidas con contraseña al nivel de la directiva.

Creación de una contraseña temporaria usando la Consola de administración de Kaspersky Security Center

Para crear una contraseña temporaria y enviársela a un usuario:

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 del usuario que está solicitando la contraseña temporaria.
3. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
4. En el menú contextual del equipo que pertenece al usuario que solicita la contraseña temporaria, seleccione **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del equipo>**.
5. En la ventana **Propiedades: <Nombre del equipo>**, seleccione la sección **Aplicaciones**.
6. Seleccione Kaspersky Endpoint Security Service Pack 2 para Windows y abra la ventana de propiedades de la aplicación con uno de los siguientes métodos:

   - Haga clic en el botón **Propiedades** al pie de la pantalla.
   - En el menú contextual de la aplicación, seleccione **Propiedades**.

   Se abre la ventana **Configuración de la aplicación "<Nombre de la aplicación>"**.
7. En la ventana **Configuración de la aplicación "<Nombre de la aplicación>"**, diríjase a la sección **Configuración avanzada** y seleccione la subsección **Configuración de la aplicación**.
8. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección con contraseña**.
9. En la ventana **Protección con contraseña**, diríjase a la sección **Contraseña temporal** y haga clic en el botón **Configuración**.

   > Este botón está disponible si la protección con contraseña está activada para Kaspersky Security Center en la directiva de Kaspersky Security Center que se está ejecutando en el equipo.

   Se abre la ventana **Crear contraseña temporal**.
10. En el campo **Fecha de caducidad**, especifique la fecha en la que el usuario ya no podrá utilizar la contraseña temporaria.

    En esta fecha, la contraseña temporaria ya no será válida. Se deberá crear una contraseña temporaria nueva para proporcionar acceso para realizar operaciones en la interfaz local de Kaspersky Endpoint Security.
11. En la tabla **Alcance de la contraseña temporaria**, seleccione las casillas que se encuentran frente a las operaciones que deben estar disponibles para el usuario mientras la contraseña temporaria sea válida.
12. Haga clic en el botón **Crear**.

Se abre la ventana **Contraseña temporal** con una contraseña cifrada.

13. Copie la contraseña y las instrucciones para aplicarla y envíeselas al usuario.

Aplicación de una contraseña temporaria en la interfaz de Kaspersky Endpoint Security

Estas instrucciones son para usuarios de equipos cliente con Kaspersky Endpoint Security instalado.

Para aplicar una contraseña temporaria:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.

   La configuración de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Protección con contraseña**, haga clic en el botón **Contraseña temporal**.

   Se abre la ventana **Contraseña temporal**.
4. Seleccione la casilla **Habilitar contraseña temporal**.
5. En el campo de entrada de datos, especifique la contraseña que recibió del administrador de Kaspersky Security Center.
6. Haga clic en **Aceptar** para guardar los cambios.

Una vez aplicada la contraseña temporaria, se podrá acceder a las operaciones especificadas por el administrador de Kaspersky Security Center. En la ventana **Contraseña temporal** se muestra la fecha de caducidad de la contraseña temporaria y las operaciones permitidas.

Administración remota de la aplicación a través de Kaspersky Security Center

Esta sección describe la administración de Kaspersky Endpoint Security mediante Kaspersky Security Center.

Acerca de la administración de la aplicación a través de Kaspersky Security Center

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

Para obtener información adicional sobre la administración de la aplicación mediante Kaspersky Security Center que no se proporciona en este documento, consulte la *Guía del administrador de Kaspersky Security Center*.

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

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.

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

Puede usar un complemento de administración para cambiar los siguientes elementos:

- Directivas
- Perfiles de directivas
- Tareas de grupo
- Tareas locales
- Configuración local de Kaspersky Endpoint Security

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.

Si se abre algún componente, el complemento de administración comprueba su información de compatibilidad. Si la versión del complemento de administración es igual o superior a la especificada en la información de compatibilidad, puede cambiar la configuración de este componente. De lo contario, no podrá usar el complemento de administración para cambiar la configuración del componente seleccionado. Se recomienda actualizar el complemento de administración.

Modificación de la configuración ya definida usando una versión posterior del complemento de administración

Puede usar una versión posterior del complemento de administración para cambiar toda la configuración ya definida y configurar parámetros nuevos que no estaban presentes en la versión del complemento de la administración que usaba antes.

Para los parámetros nuevos, una versión posterior del complemento de administración asigna los valores predeterminados cuando se guarda una directiva, un perfil de directivas o una tarea por primera vez.

Una vez que haya cambiado la configuración de una directiva, de un perfil de directivas o de una tarea de grupo con una versión posterior del complemento de administración, estos componentes ya no estarán disponibles en versiones anteriores del complemento de administración. La configuración local de Kaspersky Endpoint Security y los parámetros de las tareas locales seguirán disponibles en el complemento de administración de versiones anteriores.

Inicio y detención de Kaspersky Endpoint Security en un equipo cliente

Para iniciar o detener la aplicación en un equipo cliente:

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**.

   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 lo siguiente:

   - Para iniciar la aplicación, haga clic en el botón que se encuentra a la derecha de la lista de aplicaciones de Kaspersky o realice lo siguiente:

     a. Seleccione **Propiedades** en el menú contextual de Kaspersky Endpoint Security o haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.

     Se abre la ventana **Configuración de Kaspersky Endpoint Security para Windows**.

b. En la sección **General**, haga clic en el botón **Iniciar**, que encontrará en la parte derecha de la ventana.

- Para detener la aplicación, haga clic en el botón a la derecha de la lista de aplicaciones de Kaspersky o realice lo siguiente:

  a. Seleccione **Propiedades** en el menú contextual de Kaspersky Endpoint Security o haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.

  Se abre la ventana **Configuración de Kaspersky Endpoint Security para Windows**.

  b. En la sección **General**, haga clic en el botón **Detener**, que encontrará en la parte derecha de la ventana.

Configuración de los parámetros de Kaspersky Endpoint Security

Para configurar los parámetros de Kaspersky Endpoint Security:

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 la aplicación Kaspersky Endpoint Security 10 para Windows.
8. Realice una de las siguientes acciones:

   - Seleccione **Propiedades** en el menú contextual de Kaspersky Endpoint Security 10 para Windows.
   - 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 10 para Windows**.
9. En la sección **Configuración avanzada**, configure los parámetros correspondientes a Kaspersky Endpoint Security, además de la configuración de los informes y el almacenamiento.

   Las otras secciones de la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows** son las mismas que en las secciones de la aplicación estándar de Kaspersky Security Center. En la *Guía del administrador de Kaspersky Security Center* se ofrece una descripción de estas secciones.

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 avanzada**.

10. Para guardar los cambios, en la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows**, haga clic en **Aceptar**.

Administración de tareas

Esta sección describe cómo administrar tareas para Kaspersky Endpoint Security. Consulte la *Guía del administrador de Kaspersky Security Center* para obtener los detalles sobre la administración de tareas mediante Kaspersky Security Center.

Acerca de las tareas para Kaspersky Endpoint Security

Kaspersky Security Center controla la actividad de las aplicaciones de Kaspersky en equipos cliente por medio de diversas tareas. Las tareas sirven para implementar las principales funciones administrativas, como la instalación de claves, el análisis del equipo y las actualizaciones de las bases de datos y los módulos de software de la aplicación.

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 un conjunto de equipos que no pertenecen a grupos de administración

  Las tareas para conjuntos de equipos que no pertenecen a grupos de administración se aplican solamente a los equipos cliente especificados en la configuración de las tareas. Si se agregan nuevos equipos cliente a un conjunto de equipos para el cual hay una tarea configurada, esta tarea no se aplica a los nuevos equipos. Para aplicar la tarea a estos equipos, debe crear una nueva tarea o editar la configuración de la tarea existente.

Para administrar en forma remota Kaspersky Endpoint Security, puede usar las siguientes tareas de cualquiera de los tipos enumerados:

- **Añadir clave**. Kaspersky Endpoint Security agrega una clave para la activación de la aplicación, incluida una clave adicional.
- **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.
- **Inventario**. Kaspersky Endpoint Security recibe información sobre todos los archivos ejecutables de aplicaciones almacenados en los equipos.

  Puede activar el inventario de módulos DLL y archivos de script. En este caso, Kaspersky Security Center recibirá información sobre los módulos DLL cargados en un equipo con Kaspersky Endpoint Security instalado, y sobre archivos que contengan scripts.

  Activar el inventario de módulos DLL y archivos de script aumenta considerablemente la duración de la tarea del inventario y el tamaño de la base de datos.

Si el componente Control de aplicaciones no está instalado en un equipo con Kaspersky Endpoint Security instalado, la tarea del inventario en este equipo devolverá un error.

- **Actualización**. Kaspersky Endpoint Security actualiza sus bases de datos y sus módulos de la aplicación conforme a los parámetros de actualización configurados.
- **Revertir la última actualización**. Kaspersky Endpoint Security revierte la última actualización de bases de datos y módulos.
- **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.
- **Comprobación de integridad**. Kaspersky Endpoint Security recibe datos sobre el conjunto de módulos de la aplicación instalados en el equipo cliente y analiza la firma digital de cada módulo.
- **Administrar cuentas del Agente de autenticación**. Al realizar esta tarea, Kaspersky Endpoint Security genera comandos para eliminar, agregar o modificar cuentas del Agente de autenticación.

Puede realizar las siguientes acciones con las tareas:

- Iniciar, detener, suspender y reanudar tareas.
- Crear nuevas tareas.
- Editar la configuración de tareas.

Los permisos de acceso a las configuraciones de las tareas de Kaspersky Endpoint Security (leer, escribir, ejecutar) se definen para cada usuario que tiene acceso a el Servidor de administración de Kaspersky Security Center a través de las configuraciones de acceso a 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.

Configuración del modo de administración de tareas

Para configurar el modo en el que se trabajará con tareas en la interfaz local de Kaspersky Endpoint Security:

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 para el cual quiera configurar el modo en el que se trabajará con tareas en la interfaz local de Kasperskey Endpoint Security.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.
6. En la sección **Configuración avanzada**, seleccione la subsección **Configuración de la aplicación**.

7. En la sección **Modo de funcionamiento**:

   - Si quiere permitir que los usuarios trabajen con tareas locales en la interfaz y la línea de comandos de Kaspersky Endpoint Security, seleccione la casilla **Permitir el uso de tareas locales**.

     Si se desmarca la casilla, las funciones de tareas locales se detienen. En este modo, las tareas locales no se ejecutan según la programación. Tampoco estarán disponibles las tareas locales para iniciar y modificar en la interfaz local del Kaspersky Endpoint Security, y cuando se trabaje con la línea de comandos.

   - Si quiere permitir que los usuarios vean la lista de tareas de grupo, seleccione la casila **Permitir que las tareas grupales se visualicen**.

   - Si quiere permitir que los usuarios modifiquen la configuración de tareas de grupo, seleccione la casila **Permitir la administración de tareas de grupo**.

8. Haga clic en **Aceptar** para guardar los cambios.

9. Aplique la directiva.

   Para obtener más información sobre la aplicación de la directiva de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center.*

Creación de una tarea local

Para crear una tarea local:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta 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 para el cual quiera crear una tarea local.

5. Realice una de las siguientes acciones:

   - En el menú contextual del equipo cliente, seleccione la opción **Todas las tareas** Crear tarea.

   - En el menú contextual del equipo cliente, seleccione **Propiedades** y, en la ventana **Propiedades: <Nombre del equipo>** que se abre, haga clic en el botón **Agregar** de la ficha **Tareas**.

   - En la lista desplegable **Realizar acción**, seleccione **Crear tarea**.

   Se inicia el Asistente de tareas.

6. Siga las instrucciones del Asistente de tareas.

Creación de una tarea de grupo

Para crear una tarea de grupo:

1. Abra la Consola de administración de Kaspersky Security Center.
2. Realice una de las siguientes acciones:
   - Seleccione la carpeta **Dispositivos administrados** en el árbol de la Consola de administración para crear una tarea de grupo para todos los equipos administrados por Kaspersky Security Center.
   - 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 **Tareas**.
4. Haga clic en el botón **Crear tarea**.
   Se inicia el Asistente de tareas.
5. Siga las instrucciones del Asistente de tareas.

Creación de una tarea para la selección de dispositivo

Para crear una tarea para la selección del dispositivo, realice lo siguiente:

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 **Crear tarea**.
   Se inicia el Asistente de tareas.
4. Siga las instrucciones del Asistente de tareas.
5. En la ventana **Seleccionar dispositivos a los que se asignará la tarea** del Asistente, haga clic en el botón **Asignar tarea a un conjunto de dispositivos**.
6. En la siguiente ventana del Asistente, haga clic en el botón **Seleccionar**.
   Se abre la ventana **Selección de dispositivos**.
7. Seleccione los dispositivos necesarios.
8. En la ventana **Selección de dispositivos**, haga clic en **Sin inconvenientes**.
9. Siga las instrucciones del Asistente de tareas.

Inicio, detención, suspensión y reanudación de una tarea

Si la aplicación Kaspersky Endpoint Security se está ejecutando en un equipo cliente, puede iniciar, detener, suspender y reanudar una tarea en este equipo cliente por medio de Kaspersky Security Center. Cuando se suspende Kaspersky Endpoint Security, se suspenden las tareas en ejecución y se vuelve imposible iniciar, detener, suspender o reanudar una tarea a través de Kaspersky Security Center.

Para iniciar, detener, suspender o reanudar una tarea local:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta 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 que quiera iniciar, detener, suspender o reanudar una tarea local.
5. Haga clic con el botón derecho del mouse para mostrar el menú contextual del equipo cliente y seleccione **Propiedades**.

   Se abre la ventana de las propiedades del equipo cliente.
6. Seleccione la sección **Tareas**.

   Aparece una lista de tareas locales en la parte derecha de la ventana.
7. Seleccione la tarea local que desea iniciar, detener, suspender o reanudar.
8. Realice la acción necesaria sobre la tarea usando uno de los métodos siguientes:

   - Haga clic con el botón derecho del mouse para abrir el menú contextual de la tarea local y seleccione **Ejecutar** / **Detener** / **Suspender** / **Reanudar**.
   - Para iniciar o detener una tarea local, haga clic en el botón / a la derecha de la lista de tareas locales.
   - Haga lo siguiente:

     a. Haga clic en el botón **Propiedades** que se encuentra debajo de la lista de tareas locales o seleccione **Propiedades** en el menú contextual de la tarea.

     Se abre la ventana **Propiedades: <Nombre de la tarea>**.

     b. En la ficha **General**, haga clic en uno de los siguientes botones: **Ejecutar** / **Detener** / **Suspender** / **Reanudar**.

Para iniciar, detener, pausar o reanudar una tarea de grupo:

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 para el cual quiera iniciar, detener, suspender o reanudar una tarea de grupo.
3. En el espacio de trabajo, seleccione la ficha **Tareas**.

   Las tareas de grupo se muestran en la parte derecha de la ventana.
4. Seleccione la tarea de grupo que quiera iniciar, detener, suspender o reanudar.

5. Realice la acción necesaria sobre la tarea usando uno de los métodos siguientes:

   - En el menú contextual de la tarea de grupo, seleccione **Ejecutar** / **Detener** / **Suspender** / **Reanudar**.
   - Para iniciar o detener una tarea de grupo, haga clic en el botón / que se encuentra en la parte derecha de la ventana.
   - Haga lo siguiente:

     a. En la parte derecha del espacio de trabajo de la Consola de administración, haga clic en el vínculo **Configuración de la tarea**, o seleccione **Propiedades** en el menú contextual de la tarea.

     Se abre la ventana **Propiedades: <Nombre de la tarea>**.

     b. En la ficha **General**, haga clic en uno de los siguientes botones: **Ejecutar** / **Detener** / **Suspender** / **Reanudar**.

Para iniciar, detener, suspender o reanudar una tarea para un conjunto de equipos:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Tareas** del árbol de la Consola de administración, seleccione la tarea para el conjunto de equipos que quiera iniciar, detener, suspender o reanudar.
3. Realice una de las siguientes acciones:

   - En el menú contextual de la tarea, seleccione **Ejecutar** / **Detener** / **Suspender** / **Reanudar**.
   - Para iniciar o detener la tarea correspondiente a equipos específicos, haga clic en el botón / que se encuentra en la parte derecha de la ventana.
   - Haga lo siguiente:

     a. En la parte derecha del espacio de trabajo de la Consola de administración, haga clic en el vínculo **Configuración de la tarea**, o seleccione **Propiedades** en el menú contextual de la tarea.

     Se abre la ventana **Propiedades: <Nombre de la tarea>**.

     b. En la ficha **General**, haga clic en uno de los siguientes botones: **Ejecutar** / **Detener** / **Suspender** / **Reanudar**.

Edición de la configuración de tareas

Para editar la configuración de una tarea local:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta 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 un equipo para el cual quiera configurar los parámetros de la aplicación.

5. Haga clic con el botón derecho del mouse para mostrar el menú contextual del equipo cliente y seleccione **Propiedades**.

   Se abre la ventana de las propiedades del equipo cliente.

6. Seleccione la sección **Tareas**.

   Aparece una lista de tareas locales en la parte derecha de la ventana.

7. Seleccione la tarea local necesaria en la lista de tareas locales.

8. Haga clic en el botón **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre de la tarea local>**.

9. En la ventana **Propiedades:<Nombre de la tarea local>**, seleccione la sección de **Configuración**.

10. Edite las opciones de configuración de la tarea local.

11. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la tarea local>**, haga clic en **Aceptar**.

12. Para guardar los cambios, en la ventana **Propiedades: <Nombre del equipo>**, haga clic en **Aceptar**.

Para editar la configuración de una tarea de grupo:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados**, abra la carpeta con el nombre del grupo de administración en cuestión.

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

   Las tareas de grupo se muestran en el espacio de trabajo de la Consola de administración.

4. Seleccione la tarea de grupo necesaria.

5. Haga clic con el botón derecho del mouse para mostrar el menú contextual de la tarea de grupo y seleccione **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre de la tarea de grupo>**.

6. En la ventana **Propiedades:<Nombre de la tarea de grupo>**, seleccione la sección de **Configuración**.

7. Edite las opciones de configuración de la tarea de grupo.

8. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la tarea de grupo>**, haga clic en **Aceptar**.

Para editar los parámetros de una tarea correspondiente a un conjunto de equipos:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En la carpeta **Tareas** del árbol de la Consola de administración, seleccione la tarea para el conjunto de equipos cuyos parámetros quiera editar.

3. Haga clic con el botón derecho del mouse para mostrar el menú contextual de la tarea para una selección de equipos y seleccione **Propiedades**.

   Se abre la ventana **Propiedades**:**<Nombre de la tarea para una selección de equipos>**.

4. En la ventana **Propiedades: <Nombre de la tarea para el conjunto de equipos>**, seleccione la sección de **Configuración**.

5. Modifique los parámetros de la tarea correspondiente al conjunto de equipos.

6. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la tarea para el conjunto de equipos>**, haga clic en **Aceptar**.

Salvo por la sección de **Configuración**, todas las secciones presentes en la ventana de propiedades de la tarea son idénticas a las que se utilizan en Kaspersky Security Center. Para ver una descripción detallada de las secciones, consulte la ayuda de Kaspersky Security Center. La sección **Configuración** contiene los parámetros específicos de Kaspersky Endpoint Security para Windows. Su contenido depende de la tarea seleccionada o del tipo de tarea.

Administración de directivas

Esta sección analiza la creación y configuración de directivas para Kaspersky Endpoint Security. Para obtener información más detallada sobre cómo administrar Kaspersky Endpoint Security utilizando directivas de Kaspersky Security Center, consulte la *Guía del administrador de Kaspersky Security Center*.

Acerca de las directivas

Puede utilizar directivas para aplicar configuraciones idénticas de Kaspersky Endpoint Security en todos los equipos cliente dentro de un grupo de administración.

Puede modificar en forma local los valores de los parámetros especificados por una directiva para equipos individuales en un grupo de administración usando Kaspersky Endpoint Security. Puede cambiar en forma local solamente los parámetros cuya modificación no esté prohibida por la directiva.

La capacidad de cambiar la configuración de la aplicación en el equipo del cliente está determinada por el estado del "candado" de dicha configuración en las propiedades de la directiva:

- Una "candado" cerrado () significa lo siguiente:

  - Kaspersky Security Center bloquea los cambios de la configuración relacionada con este candado desde la interfaz de Kaspersky Endpoint Security en los equipos de cliente. En todos los equipos cliente, Kaspersky Endpoint Security usa los mismos valores de configuración; es decir, los valores especificados en las propiedades de la directiva.

  - Kaspersky Security Center bloquea los cambios de la configuración relacionada con este candado en las propiedades de las directivas para grupos de administración anidados y servidores de administración secundarios en los cuales está habilitada la función **Heredar la configuración de la directiva primaria**. Se utilizan los valores de esta configuración que se definen en la directiva de nivel superior.

- Un "candado" cerrado () significa lo siguiente:

  - Kaspersky Security Center habilita los cambios de la configuración relacionada con este candado desde la interfaz de Kaspersky Endpoint Security en los equipos de cliente. Kaspersky Endpoint Security funciona según los valores locales de esta configuración si el componente está habilitado en cada equipo cliente.

  - Kaspersky Security Center habilita los cambios de la configuración relacionada con este candado en las propiedades de las directivas para grupos de administración anidados y servidores de administración

secundarios en los cuales está habilitada la función **Heredar la configuración de la directiva primaria**. Los valores de esta configuración no dependen de lo que se especifica en las propiedades de la directiva de nivel superior.

Luego de que una directiva se aplica por primera vez, la configuración local de la aplicación cambia de acuerdo con la configuración de la directiva.

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.

Se individualizan los siguientes alcances funcionales de Kaspersky Endpoint Security:

- Protección básica contra amenazas. El alcance funcional incluye los componentes protección contra amenazas de archivos, protección contra amenazas de correo, protección contra amenazas web, protección contra Amenazas de red, firewall y tarea de análisis.
- Control de aplicaciones. El alcance funcional incluye el componente Control de aplicaciones.
- Control de dispositivos. El alcance funcional incluye el componente Control de Dispositivos.
- Cifrado. El alcance incluye los componentes del cifrado de archivos y el cifrado de disco completo.
- Zona de confianza. El alcance funcional incluye la Zona de confianza.
- Control web. El alcance funcional incluye el componente Control Web.
- Protección avanzada contra amenazas. El alcance funcional incluye la configuración de KSN y los componentes Detección de comportamientos, Prevención de exploits, Prevención contra intrusos y Motor de reparación.
- Funcionalidad básica. Este alcance funcional incluye las configuraciones generales de la aplicación que no están especificadas en otros alcances funcionales, incluyendo: licencia, tareas de inventario, tareas de actualización de bases de datos y módulos de la aplicación, Autoprotección, configuración avanzada de la aplicación, Informes y depósitos, configuración de protección por contraseña y configuración de la interfaz de la aplicación.

Con una directiva puede realizar las siguientes operaciones:

- Crear una directiva.
- Editar la configuración de la directiva.

  Si la cuenta de usuario desde la que accedió al Servidor de administración no tiene los permisos para editar la configuración de ciertos alcances funcionales, dicha configuración no estará disponible para su edición.

- Eliminar una directiva.
- Cambiar el estado de una directiva.

Para obtener información sobre el uso de directivas no relacionadas con la interacción con Kaspersky Endpoint Security, consulte la ayuda de Kaspersky Security Center.

Creación de una directiva

Para crear una directiva:

1. Abra la Consola de administración de Kaspersky Security Center.
2. Realice una de las siguientes acciones:
   - Seleccione la carpeta **Dispositivos administrados** en el árbol de la Consola de administración si quiere crear una directiva para todos los equipos administrados por Kaspersky Security Center.
   - 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. Realice una de las siguientes acciones:
   - Haga clic en el botón **Crear directiva**.
   - Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Crear** Directiva.

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

Edición de la configuración de directivas

Para editar la configuración de directivas:

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 relevante para el cual quiera modificar la configuración de directivas.
3. En el espacio de trabajo, seleccione la ficha **Directivas**.
4. Seleccione la directiva correspondiente.
5. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - En el menú contextual de la directiva, seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva** que se encuentra en la parte derecha del espacio de trabajo de la Consola de administración.

   La configuración de directivas de Kaspersky Endpoint Security 10 para Windows incluye la configuración de los componentes y la configuración de la aplicación. En las secciones de **Protección antivirus** y **Control del endpoint** de la ventana **Propiedades: <Nombre de la directiva>** se muestra la configuración de los componentes de protección y control, en la sección **Cifrado de datos** se muestra la configuración de cifrado para archivos y carpetas y en la sección **Configuración avanzada** se muestra la configuración de la aplicación.

Para habilitar la visualización de la configuración del cifrado de datos y de la configuración de los componentes en la configuración de directivas, debe seleccionar las casillas correspondientes en la ventana **Configuración de la interfaz** de Kaspersky Security Center.

6. Modifique la configuración de directivas.

7. Para guardar los cambios, en la ventana **Propiedades: <Nombre de la directiva>** haga clic en **Aceptar**.

Selección de los parámetros que se visualizarán en la directiva de Kaspersky Security Center

Para seleccionar los parámetros que se visualizarán en la directiva de Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.

2. En el menú contextual del nodo **Servidor de administración – <Nombre del equipo>** del árbol de la Consola de administración, seleccione Ver → **Configuración de la interfaz**.

   Se abre la ventana **Configuración de la interfaz**.

3. En la ventana **Configuración de la Interfaz**, seleccione las casillas que se encuentran frente a la configuración que se tiene que mostrar en la configuración de creación de directivas de Kaspersky Security Center y en las propiedades de las directivas:

   - Seleccione la casilla **Mostrar componentes de control de Endpoint** para permitir que se muestre la configuración de los componentes de control en la ventana del Asistente para nuevas directivas de Kaspersky Security Center y en las propiedades de las directivas.

   - Seleccione la casilla **Mostrar cifrado y protección de datos** para permitir que se muestre la configuración del cifrado de datos en la ventana del Asistente para nuevas directivas de Kaspersky Security Center y en las propiedades de las directivas.

4. Haga clic en **Aceptar**.

Envío de mensajes de usuarios al servidor de Kaspersky Security Center

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.

- El Control de Inicio de las 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 Inicio de las 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:

- Si no se está ejecutando una directiva de Kaspersky Security Center en el equipo que tiene Kaspersky Security Center instalado, el mensaje de un 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.

- Si se está ejecutando una directiva de Kaspersky Security Center en el equipo que tiene Kaspersky Security Center instalado, se envía el mensaje estándar al Servidor de administración de Kaspersky Security Center.

  En este caso, los mensajes del usuario podrán visualizarse en el almacenamiento de eventos de Kaspersky Security Center. 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.

Visualización de mensajes de usuarios en el almacenamiento de eventos de Kaspersky Security Center

Los componentes de Control de Inicio de las Aplicaciones, Control de dispositivos y Control Web permiten que los usuarios de una red LAN con equipos que tienen Kaspersky Endpoint Security instalado envíen mensajes al administrador.

Un usuario puede enviar mensajes al administrador de dos maneras:

- Como un evento en el almacenamiento de eventos de Kaspersky Security Center.

  El evento del usuario se envía al almacenamiento de eventos de Kaspersky Security Center si la aplicación Kaspersky Endpoint Security instalada en el equipo del usuario funciona según una directiva activa.

- Como mensaje de correo electrónico.

  La información del usuario se envía por correo electrónico si la aplicación Kaspersky Endpoint Security instalada en el equipo del usuario no está ejecutando una directiva o está ejecutando una directiva de ausencia de la oficina.

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 para enviar al administrador.

5. Abra la ventana **Configuración del evento** de una de las siguientes formas:

   - Haga clic con el botón derecho en el evento. En el menú contextual que se abre, seleccione **Propiedades**.

   - 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.

Participación en Kaspersky Security Network

Esta sección incluye información sobre la participación en Kaspersky Security Network e instrucciones sobre cómo habilitar o deshabilitar el uso de Kaspersky Security Network.

Acerca de la participación en 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 recibir dicha información.

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.

Según la ubicación de la infraestructura, hay un servicio de KSN global (la infraestructura está alojada en servidores de Kaspersky) y un servicio de KSN Privada.

Luego de cambiar la licencia, envíe los detalles de su nueva clave al proveedor del servicio a fin de poder utilizar KSN Privada. En caso contrario, no será posible el intercambio de datos con KSN Privada.

Gracias a quienes participan en KSN, Kaspersky puede recibir rápidamente información sobre los distintos tipos de amenazas y sus orígenes, desarrollar soluciones para neutralizar estos riesgos y reducir la cantidad de falsas alarmas que muestran los componentes de la aplicación.

Al utilizar el modo KSN ampliado, la aplicación envía automáticamente sus estadísticas operativas resultantes a KSN. La aplicación también puede enviar ciertos archivos (o partes de archivos) que los piratas informáticos podrían usar para dañar el equipo o los datos a Kaspersky para profundizar su análisis.

Para más detalles sobre la información estadística que se genera al usar KSN, sobre el envío de esa información a Kaspersky y sobre su almacenamiento y destrucción, consulte la Declaración de Kaspersky Security Network y el sitio web de Kaspersky. El archivo ksn_<identificador del idioma>.txt que contiene la Declaración de Kaspersky Security Network se incluye en el kit de distribución de la aplicación.

Para reducir la carga en los servidores KSN, Kaspersky puede lanzar bases de datos antivirus de la aplicación que temporalmente inhabiliten o restrinjan en forma parcial solicitudes a Kaspersky Security Network. En este caso, el estado de la conexión con KSN aparece como *Permitido con restricciones*.

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 Proxy de KSN coloca en la memoria caché los datos procesados y, por lo tanto, reduce la carga en la conexión de la red externa y acelera la recepción de información solicitada por el equipo del usuario.

Para obtener más información sobre el servicio Proxy de KSN, consulte la *Guía de ayuda de Kaspersky Security Center*.

Los parámetros del servicio del Proxy de KSN se pueden configurar en las propiedades de la directiva de *Kaspersky Security Center*.

El uso de Kaspersky Security Network es voluntario. La aplicación invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios pueden iniciar o discontinuar su participación en KSN en cualquier momento.

Habilitación y deshabilitación del uso de Kaspersky Security Network

Para habilitar o deshabilitar el uso de Kaspersky Security Network:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione la subsección **Configuración de KSN**.

   La configuración de Kaspersky Security Network se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:

   - Si quiere activar el uso de Kaspersky Security Network, seleccione la casilla **Acepto la Declaración de KSN y las condiciones de participación**.
   - Si quiere desactivar el uso de Kaspersky Security Network, desmarque la casilla **Acepto la Declaración de KSN y las condiciones de participación**.
4. Para guardar los cambios, haga clic en el botón **Guardar**.

Verificación de la conexión con Kaspersky Security Network

Para verificar la conexión con Kaspersky Security Network:

1. Abra la ventana principal de la aplicación.
2. En la parte superior de la ventana, haga clic en el botón **Kaspersky Security Network**.

   Se abre la ventana **Kaspersky Security Network**.

   La parte izquierda de la ventana **Kaspersky Security Network** muestra el modo de conexión a Kaspersky Security Network en un botón **KSN** circular:

   - Si Kaspersky Endpoint Security no está conectado a Kaspersky Security Network, el botón **KSN** es de color gris. Debajo del botón **KSN** puede leerse el estado *Desactivado.*
   - Si Kaspersky Endpoint Security está conectado a Kaspersky Security Network y los servidores de KSN están disponibles, el botón **KSN** es de color verde. La siguiente información aparece debajo del botón **KSN**: estado *Activado*, tipo de KSN en uso (**KSN privada** o **KSN global**) y la fecha y hora de la última sincronización con los servidores de KSN. En la parte derecha de la ventana se muestran estadísticas sobre la reputación de los archivos, los recursos web y el software.

Kaspersky Endpoint Security recopila datos estadísticos sobre el uso de KSN cuando usted abre la ventana **Kaspersky Security Network**. Las estadísticas no se actualizan en tiempo real.

- Si Kaspersky Endpoint Security está conectado a Kaspersky Security Network pero los servidores de KSN no están disponibles, el botón **KSN** es de color rojo. Debajo del botón **KSN** puede leerse el estado *Activado*.

  Si la hora de la última sincronización con los servidores de KSN supera los 15 minutos o tiene estado *Desconocido*, KSN no está disponible. En dicha situación, le recomendamos que se ponga en contacto con el Servicio de soporte técnico o con su proveedor de servicios.

  La conexión con los servidores de Kaspersky Security Network puede perderse por los siguientes motivos:

  - El equipo no está conectado a Internet.
  - No se activó la aplicación o la licencia caducó.
  - Se han detectado problemas relacionados con la clave (por ejemplo, la clave se ha puesto en una lista negra).

Comprobación de la reputación de un archivo en Kaspersky Security Network

El servicio de KSN le permite recuperar información sobre las aplicaciones que se incluyen en las bases de datos de reputación de Kaspersky. Esto permite implementar una administración flexible de las directivas de inicio de aplicaciones al nivel de la empresa, evitando así el inicio de adware y otros programas que los delincuentes pueden utilizar para dañar su equipo o sus datos personales.

Para comprobar la reputación de un archivo en Kaspersky Security Network:

1. Haga clic con el botón derecho del mouse para abrir el menú contextual del archivo cuya reputación quiera comprobar.
2. Seleccione la opción **Revisar la reputación en KSN**.

   Esta opción está disponible si ha aceptado los términos de la Declaración de Kaspersky Security Network.

   Se abrirá la ventana **<Nombre del archivo> - Reputación en KSN**. En la ventana **<Nombre del archivo> - Reputación en KSN** se muestra la siguiente información sobre el archivo que se está comprobando:

   - **Ruta**. La ruta en la cual el archivo se guarda en el disco.
   - **Versión**. La versión de la aplicación (la información solo se muestra para archivos ejecutables).
   - **Firma digital**. Presencia de una firma digital con el archivo.
   - **Firmado**. La fecha en la cual se firmó el certificado con una firma digital.
   - **Creado**. Fecha de creación del archivo.

- **Modificado**. Fecha de la última modificación del archivo.
- **Tamaño**. Espacio de disco que ocupa el archivo.
- Información sobre la cantidad de usuarios que confían en el archivo o lo bloquean.

Mejor protección con Kaspersky Security Network

Kaspersky ofrece una capa adicional de protección a los usuarios a través de Kaspersky Security Network. Este método de protección está diseñado para combatir las persistentes amenazas avanzadas y los ataques del día cero. Las tecnologías en la nube integradas y la experiencia de los analistas de virus de Kaspersky hacen que Kaspersky Endpoint Security sea la elección insuperable para la protección contra las amenazas de red más sofisticadas.

Encontrará detalles sobre la protección mejorada de Kaspersky Endpoint Security en el sitio web de Kaspersky.

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.

La página de Kaspersky Endpoint Security de la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico.

En la página de Kaspersky Endpoint Security de la Base de conocimientos, encontrará artículos con información útil, recomendaciones y respuestas a las dudas más frecuentes sobre la compra, la instalación y el uso de la aplicación.

Los artículos de la Base de conocimientos pueden contestar preguntas que se relacionan no solo con Kaspersky Endpoint Security, sino también con otras aplicaciones de Kaspersky. Los artículos también pueden contener novedades del 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.

En esta comunidad, puede ver los temas existentes, dejar comentarios y crear nuevos temas de discusión.

Contacto con el Servicio de soporte técnico

En esta sección, se describen las maneras de obtener Servicio de soporte técnico y los términos de acuerdo con los cuales está disponible.

Cómo obtener Servicio de soporte técnico

Si no puede encontrar una solución a su problema en la documentación de la aplicación o en ninguna de las fuentes de información sobre la aplicación, le recomendamos que se ponga en contacto con el Servicio de soporte técnico. Los especialistas del Servicio de soporte técnico responderán sus preguntas acerca de la instalación y el uso de la aplicación.

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:

- Llamando por teléfono al Servicio de soporte técnico
- Enviando una solicitud al Servicio de soporte técnico de Kaspersky por medio del portal de Kaspersky CompanyAccount.

Consultas por teléfono al Servicio de soporte técnico

Puede llamar a representantes del Servicio de soporte técnico desde la mayoría de las regiones de todo el mundo. Puede hallar información sobre las maneras en que puede recibir soporte técnico en su región y los contactos del Servicio de soporte técnico en el sitio web del Servicio de soporte técnico de Kaspersky.

Antes de ponerse en contacto con el Servicio de soporte técnico, lea las reglas del soporte técnico.

Servicio de soporte técnico mediante Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para empresas que usan aplicaciones de Kaspersky. El portal de Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los expertos de Kaspersky a través de solicitudes electrónicas. Puede usar el portal de Kaspersky CompanyAccount para seguir el estado de sus solicitudes electrónicas y guardar un historial de esas solicitudes.

Puede registrar a todos los empleados de su organización en una única cuenta en Kaspersky CompanyAccount. Una única cuenta le permite gestionar de manera centralizada las solicitudes electrónicas de los empleados registrados en Kaspersky y también administrar los privilegios de estos empleados a través de Kaspersky CompanyAccount.

El portal de Kaspersky CompanyAccount está disponible en los siguientes idiomas:

- Inglés
- Español

- Italiano
- Alemán
- Polaco
- Portugués
- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del Servicio de soporte técnico.

Recopilación de información para el Servicio de soporte técnico

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 y los volcados de bloqueo de las aplicaciones.

Puede obtener la información necesaria con la ayuda de Kaspersky Endpoint Security. La información recopilada se puede guardar en el disco duro y cargarse más adelante cuando le resulte más conveniente.

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 y la transmisión de información de diagnóstico.
- Configurar la intercepción y el registro del tráfico de red.

Los expertos del Servicio de soporte técnico proporcionarán toda la información necesaria 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.) e informarle sobre el alcance de los datos recopilados con fines de depuración. La información de diagnóstico extendida recopilada se guarda en el equipo del usuario. Los datos recopilados no se transmiten a Kaspersky de manera automática.

La configuración que se utiliza para determinar la dirección del servidor de volcado para enviar archivos de volcado a Kaspersky se almacena en el equipo del usuario. Si es necesario, los valores de estos parámetros se pueden modificar en la clave del registro del sistema operativo `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

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.

Creación de un archivo de seguimiento de la aplicación

El *Seguimiento de la aplicación* es un registro detallado de las acciones que realiza la aplicación y de los mensajes acerca de los eventos que se producen durante el funcionamiento de la aplicación.

Para crear un archivo de seguimiento de la aplicación:

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

   Se abre la ventana **Soporte**.

2. En la ventana **Soporte**, haga clic en el botón **Seguimiento del sistema**.

   Se abre la ventana **Información para Soporte Técnico**.

3. Para iniciar el proceso de seguimiento, en la lista desplegable **Seguimiento de la aplicación**, elija uno de estos elementos:

   - **está habilitado**

     Seleccione este elemento para activar el seguimiento.

   - **con rotación**.

     Seleccione este elemento para activar el seguimiento y limitar el número máximo de archivos de seguimiento y el tamaño máximo de cada uno de ellos. Si el número máximo de archivos de seguimiento del tamaño máximo se escribe, el archivo de seguimiento más viejo se elimina de modo que un archivo de seguimiento nuevo se pueda escribir.

     Si se ha seleccionado este elemento, puede especificar un valor para los siguientes campos:

     - **Cantidad máxima de archivos para la rotación**

       En este campo, puede especificar el número máximo de archivos de rastreo escritos.

     - **Tamaño máximo de cada archivo**

       En este campo, puede especificar el tamaño máximo de cada archivo de seguimiento escrito.

4. En la lista desplegable **Nivel**, seleccione el nivel de rastreo.

   Se recomienda consultar a un especialista del Servicio de soporte técnico cuál es el nivel de seguimiento indicado. Si no cuenta con instrucciones del Servicio de soporte técnico, establezca el nivel de seguimiento en **Normal (500)**.

5. Reinicie Kaspersky Endpoint Security.

6. Para detener el proceso de seguimiento, regrese a la ventana **Información para Soporte Técnico** y seleccione **Deshabilitado** en la lista desplegable **Seguimiento de la aplicación**.

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.

Contenido y almacenamiento de archivos de rastreo

El usuario tiene la responsabilidad personal de garantizar la seguridad de los datos almacenados en su equipo, en particular de controlar y restringir el acceso a estos hasta que se los 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 rastreo se almacenan en la carpeta ProgramData\Kaspersky Lab.

El archivo de rastreo tiene el siguiente formato de nombre: `KES<número de versión_fechaXX.XX_horaXX.XX_pidXXX.><tipo de archivo de rastreo>.log`.

El archivo de rastreo del Agente de autenticación se almacena en la carpeta Información de Volumen del Sistema y tiene el siguiente nombre: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

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.

- 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 tráfico se registra en los archivos de rastreo sólo desde trafmon2.ppl.
- 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.

Contenido de los archivos de rastreo HST.log, BL.log, Dumpwriter.log, WD.log, 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 proveedor de protección para 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 se almacenan en el equipo en el que Kaspersky Security Center 11 Web Console se ha instalado, dentro de la carpeta
Archivos de programa\Kaspersky Lab\Kaspersky Security Center 11 Web Console\logs. Web Console comienza a guardar información en cuanto concluye su instalación. Los archivos de seguimiento se eliminan cuando Web Console se desinstala.

El nombre de los archivos de seguimiento de Kaspersky Endpoint Security se rige por este formato: `logs-kes_windows-<tipo de archivo de seguimiento>.DESKTOP-<fecha de actualización del archivo>.log`.

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

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.

Activación o desactivación de la transmisión de archivos de rastreo y de volcado a Kaspersky

Para activar o desactivar la transmisión de archivos de rastreo y de volcado a Kaspersky:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.

   La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.

3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.

   Se abre la ventana **Modo de funcionamiento**.

4. En la ventana **Modo de funcionamiento**, seleccione la casilla **Habilitar escritura en archivos de volcado** para permitir que la aplicación escriba archivos de volcado de la aplicación.

5. Realice una de las siguientes acciones:

   - Seleccione la casilla **Enviar archivos de volcado y de seguimiento a Kaspersky** si quiere que la aplicación muestre un cuadro de solicitud en la ventana **Transferir los datos para el Soporte Técnico al servidor** para enviar los archivos de volcado y rastreo a Kaspersky para analizar los motivos de la falla de la aplicación la próxima vez que se inicie la aplicación.

   - De lo contario, desmarque la casilla **Enviar archivos de volcado y de seguimiento a Kaspersky**.

6. Haga clic en **Aceptar** en la ventana **Modo de funcionamiento**.

7. Para guardar los cambios, haga clic en el botón **Guardar** de la ventana principal de la aplicación.

Envío de archivos al servidor del Servicio de soporte técnico

Los archivos que contienen información sobre el sistema operativo, los archivos de rastreo y los de volcado se deben enviar a los expertos del Servicio de soporte técnico de Kaspersky.

Para enviar archivos al servidor del Servicio de soporte técnico:

1. Reinicie Kaspersky Endpoint Security luego de cualquier falla en su funcionamiento.

   Se abrirá la ventana **Error durante el inicio anterior de la aplicación**.

   La ventana **Error durante el inicio anterior de la aplicación** se abrirá cada vez que se inicie Kaspersky Endpoint Security (incluso después de reiniciar el equipo) hasta que envíe los archivos de volcado o de rastreo al Soporte técnico o hasta que haga clic en el botón **No enviar**.

2. En la ventana **Error durante el inicio anterior de la aplicación**, abra la lista de archivos generados; para ello, haga clic **aquí**.

3. Seleccione las casillas adyacentes a los archivos que quiera enviar al Servicio de soporte técnico.

4. Haga clic en el botón **Mostrar texto de la declaración**.

   Se abre la ventana **Declaración de provisión de datos**.

5. Lea el texto de la Declaración de la provisión de datos y haga clic en el botón **Cerrar**.

6. En la ventana **Error durante el inicio anterior de la aplicación**, marque la casilla **Acepto la Declaración de provisión de datos**.

7. Haga clic en el botón **Enviar**.

   Se abrirá la ventana **Solicitar número**.

8. En la ventana **Solicitar número**, especifique el número que se asignó a su solicitud cuando se puso en contacto con el Servicio de soporte técnico a través de Kaspersky CompanyAccount.

9. Haga clic en **Aceptar**.

Los archivos de datos seleccionados se comprimen y envían al servidor del Servicio de soporte técnico.

Activación y desactivación de la protección de los archivos de volcado y de rastreo

Los archivos de volcado y los de rastreo contienen información sobre el sistema operativo, además de datos confidenciales del usuario. Para evitar el acceso no autorizado a dichos datos, puede activar 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 activar y desactivar la protección de los archivos de volcado y de rastreo:

1. Abra la ventana de configuración de la aplicación.
2. Seleccione la sección **Configuración avanzada** de la izquierda.

   La configuración de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.

   Se abre la ventana **Modo de funcionamiento**.
4. Realice una de las siguientes acciones:
   - Seleccione la casilla **Habilitar la protección de los archivos de volcado y de seguimiento** si quiere activar la protección.
   - Desmarque la casilla **Habilitar la protección de los archivos de volcado y de seguimiento** si quiere desactivar la protección.
5. Haga clic en **Aceptar** en la ventana **Modo de funcionamiento**.
6. Para guardar los cambios, haga clic en el botón **Guardar** de la ventana principal de la aplicación.

Los archivos de volcado y de rastreo que se escribieron con la protección activa permanecen protegidos incluso luego de desactivar esta función.

Glosario

Actualización

Procedimiento de reemplazo o incorporación de archivos nuevos (bases de datos o módulos de la aplicación) recuperados de los servidores de actualización de Kaspersky.

Administrador de archivos portátil

Esta es una aplicación que proporciona una interfaz para funcionar con archivos cifrados en discos extraíbles cuando no hay ninguna funcionalidad de cifrado disponible 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 antivirus 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.

Análisis de firmas

Una tecnología de detección de amenazas que utiliza las bases de datos de Kaspersky Endpoint Security, que contienen descripciones de amenazas conocidas y métodos para erradicarlas. La protección que usa el análisis de firmas proporciona un nivel de seguridad mínimamente aceptable. De acuerdo con las recomendaciones de los expertos de Kaspersky, este método 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.

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.

Archivo probablemente infectado

Archivo que contiene código modificado de un virus conocido o código que se asemeja a un virus, pero que Kaspersky no conoce todavía. Los archivos probablemente infectados son detectados mediante el Analizador heurístico.

Asunto del certificado

El titular de una clave privada vinculado a un certificado. Puede ser un usuario, una aplicación, cualquier objeto virtual, un equipo o un servicio.

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

Documento electrónico que contiene la clave privada e información sobre el titular y el alcance de la clave, y que confirma que la clave pública pertenece al titular. El certificado debe estar firmado por el centro de certificación que lo emitió.

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.

Conector del agente de red

Funcionalidad de la aplicación que conecta la aplicación con el agente de red. El agente de red permite la administración remota de la aplicación a través de Kaspersky Security Center.

Configuración de la aplicación

Configuración de la aplicación común para todos los tipos de tareas y rige la operación de la aplicación en conjunto, como la configuración del rendimiento de la aplicación, la configuración de los informes y la configuración de la copia de seguridad.

Configuración de tarea

Configuración de la aplicación específica para cada tipo de tareas.

Copia de seguridad

Almacenamiento especial para copias de seguridad de archivos que se crean antes de intentar una desinfección o eliminación.

Cuarentena

Kaspersky Endpoint Security coloca los archivos probablemente infectados en esta carpeta. Los archivos en cuarentena se almacenan en formato cifrado.

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 HTTP, 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 protección antivirus, 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.

Huella digital del certificado

Información utilizada para identificar una clave de certificado. Se crea una huella digital al aplicar una función de hash criptográfica al valor de la clave.

Lista negra de direcciones

Una lista de las direcciones de correo electrónico cuyos mensajes entrantes son bloqueados por la aplicación de Kaspersky, independientemente del contenido del mensaje.

Máscara de archivo

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:

- *****: reemplaza de cero a varios caracteres (cualesquiera).
- **?** ?: reemplaza un carácter (cualquiera).

Observe que el nombre del archivo y la extensión se separan siempre con un punto.

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.

Módulos de la aplicación

Archivos incluidos en el archivo de instalación de la aplicación, que implementan la funcionalidad básica de la aplicación. A cada tipo de tarea realizada por la aplicación le corresponde un módulo ejecutable en particular (Protección en tiempo real, Análisis a pedido y Actualización). Cuando se inicia un análisis completo del equipo desde la ventana principal de la aplicación, usted inicia el módulo de esta tarea.

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.

Parche

Una pequeña incorporación a la aplicación que repara errores descubiertos durante el funcionamiento de la aplicación, o que instala actualizaciones.

Phishing

Un tipo de fraude en Internet en el que se envían mensajes de correo electrónico con el propósito de robar datos confidenciales, más frecuentemente datos financieros.

Poner archivos en cuarentena

Método de manejo de un archivo probablemente infectado por el cual se bloquea el acceso al archivo y se lo mueve de su ubicación original a la carpeta de la Cuarentena, donde se mantiene en su forma cifrada para descartar la amenaza de infección.

Puntos vulnerables

Código de programa que usa algún tipo de vulnerabilidad en el sistema o software. Los exploits se usan a menudo para instalar malware en el equipo sin el conocimiento del usuario.

Servicio de red

Conjunto de parámetros que define la actividad de la red. Para esta actividad de la red, puede crear una regla de red que regule el funcionamiento del firewall.

Servidor de administración

Componente de Kaspersky Security Center que almacena centralmente información sobre todas las aplicaciones de Kaspersky que están instaladas dentro de la red corporativa. También se puede utilizar para administrar estas aplicaciones.

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.

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 comerciales y las marcas de servicio son propiedad de sus respectivos propietarios.

Adobe, Acrobat y Shockwave son marcas comerciales o marcas registradas de Adobe Systems Incorporated en los Estados Unidos de América y en otros países.

Mac y FireWire 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. o sus filiales/empresas afiliadas en los Estados Unidos y en otros países.

La marca denominativa Bluetooth y sus logotipos son propiedad de Bluetooth SIG, Inc.

Borland es una marca comercial o una marca registrada de Borland Software Corporation en los Estados Unidos y en otros países.

Citrix y Citrix Provisioning Services son marcas comerciales de Citrix Systems, Inc. o sus filiales registradas en la oficina de patentes de los Estados Unidos y en otros países.

dBase es una marca comercial de dataBased Intelligence, Inc.

EMC y SecurID son marcas comerciales de EMC Corporation o marcas comerciales registradas de EMC Corporation en EE. UU. o en otros países.

ICQ es una marca registrada y/o una marca de servicio de ICQ LLC.

Intel y Pentium son marcas comerciales de Intel Corporation registradas en Estados Unidos y en otros países.

Logitech es una marca comercial registrada o marca comercial de Logitech Company registrada en EE. UU. y en otros países.

Mail.ru es una marca comercial registrada de Mail.Ru LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell y Surface son marcas comerciales de Microsoft Corporation registradas en Estados Unidos de América y en otros países.

Mozilla y Thunderbird son marcas registradas de Mozilla Foundation.

Novell es una marca comercial de Novell Inc., registrada en EE. UU. y en otros países.

Java y JavaScript son marcas registradas de Oracle Corporation o sus empresas afiliadas.

SafeNet es la marca comercial registrada de SafeNet, Inc.

UNIX es una marca comercial registrada en EE. UU. y en otros países, y se utiliza con la licencia de X/Open Company Limited.